Digital Threats to Democracy:
Investigating the Complexities of Election Interference by Non-State Information Operations Actors and its Connection to Data Colonialism in the Global South

July 2023

University of Glasgow: 2316275B
Dublin City University: 21109231
Charles University: 47022204

Presented in partial fulfilment of the requirements for the Degree of
International Master in Security, Intelligence and Strategic Studies

Word count: 20,018
Supervisor: Dr. Petr Špelda
Date of Submission: 25/07/2023

Abstract

The integration of data-driven microtargeting techniques in political campaigning has transformed modern domestic and global politics. Contemporary elections cycles are witnessing a surge in attack advertisements, fake news, and data manipulation, fuelled by the emergence of political consulting firms like Cambridge Analytica. These firms, as non-state information operations actors (IOAs), have emerged as influential players with considerable sway over democratic stability worldwide. This dissertation aims to explore the role of such actors in Kenya's Presidential Elections of 2013 and 2017, combining existing research with the concept of 'Data Colonialism'. The study seeks to understand how non-state IOAs engage in digital election interference and potentially contribute to data colonial practices, paving the way for more effective regulation and protection of democratic processes in the Global South. This dissertation used qualitative data from investigations and news reports to thematically analyse the actions of non-state IOAs in the 2013 and 2017 Kenyan Presidential Elections. The findings were then interpreted in accordance with a data colonialism framework to understand the potential implications of digital election interference in the Global South. Through this approach, the study reveals how data-driven campaigns by non-state IOAs can be considered predatory and extractive, causing division and destabilising the democratic process. The findings raise questions about the nature of data-driven political campaigning and its impact, emphasising the need for robust data protection regulations and technical infrastructure to safeguard democratic politics in the Global South.

Keywords: Non-state information operations actors, data colonialism, digital election interference, disinformation, Global South, online political campaigns, thematic analysis.

<u>Acknowledgements</u>

Table of Contents

List of Figures and Tables

1. <u>Introduction</u>

Attack advertisements and fake news fuelled by data manipulation and psychographic targeting are becoming the norm in contemporary election cycles. Political consulting firms, like the infamous Cambridge Analytica, have become important players in global politics, offering prospective candidates a suite of tools to gain electoral success. The use of propaganda and disinformation, especially during elections, is not a new phenomenon. However, it has increased exponentially due to social media. There has been a proliferation of non-state information operations actors (IOAs) who use marketing techniques combined with insights from social media, unregulated by international law, to influence elections. This has led to disinformation being identified as a significant threat to democratic processes today (Maweu, 2019, 65). In a new digitised world, the work of political consulting firms and the impact of disinformation on elections has become a central issue for democratic stability. Of particular concern is the effect this phenomenon is having on political discourse, causing seemingly irreparable division amongst opposing sides of the political spectrum.

Existing research recognises disinformation's critical role in contemporary global politics (Bakir, 2020, 4; Bulckaert, 2018; DCMS Committee, 2019). Several studies have found that a global shift towards digital communication means that the Internet now plays a central role in our lives, transforming the way that politics is conducted (Mäkinen and Kuira, 2008, 333; Persily, 2017, 74; Schia and Gjesvik, 2020, 415). This has led to what has been dubbed the 'Analytics Turn', the increased use of experimental data science methods to analyse large-scale collections of personal data to influence elections (Chadwick and Stromer-Galley, 2016, 284). Crain and Nadler (2019) argue that traditional digital advertising techniques have become weaponised to the extent that consumer data shapes political attitudes. The quantity of personal data made available by social media has now made it increasingly simple for non-state IOAs to monitor and develop detailed voter profiles that can be used to deliver strategic messaging.

Scholarship on digital election interference focuses on democracies as the main targets of cyber information warfare (Chambers, 2021; Dowling, 2022, 233; Gorton, 2016; Maweu, 2019). Political candidates increasingly use non-state IOAs, political consultancy firms, to campaign for them. Due to the proliferation of these actors, electoral politics has now become fully integrated into "a growing, global commercial digital media and marketing ecosystem" (Chester and Montgomery, 2017, 2).

Debate continues as to the efficacy of such techniques within election campaigning. Some argue that this form of targeting may be beneficial, amplifying relevant information for voters (Borgesius, Möller, Kruikemeier, Fathaigh, Irion, Dobber, Bodo and de Vreese, 2018, 83). Others argue that it has a limited impact on the outcomes of elections, with any success being overstated (Allcott and Gentzkow, 2017; Benkler, Faris and Roberts, 2018). The consensus, however, is that the power of such techniques, combined with disinformation, derives from their demobilising qualities, erecting barriers to informed political decision-making (Persily, 2017, 69). Ultimately, these online political campaigns harm democracy by skewing the ability of voters to make informed choices based on fair and balanced information (Bakir, 2020, 5; Dowling, 2022, 233; Maweu, 2019, 66).

Although extensive investigation has been carried out regarding the use of targeted disinformation during foreign elections, there are still considerable gaps in the research landscape. First, much of the current work takes a state-centric approach, focusing on election interference from one state to another. Despite the increasing involvement of non-state IOAs in global elections, there remains a paucity of evidence that evaluates this. Adding to this, there have been few attempts to shed light on their involvement specifically in the Global South. A review of the literature found only a handful of studies that examine how political campaigning techniques used by non-state IOAs impact elections where democracy is tenuous. While some research has been carried out on Cambridge Analytica's involvement in African elections (Ekdale and Tully, 2019), little is known about the processes by which political consulting firms operate in such contexts and the impact of this.

For this reason, much uncertainty still exists about the work of political consulting firms, not just in the Global South but more generally. What is less clear is the nature of such work and how it could have potentially detrimental consequences for democratic stability. Data privacy laws in the Global South are currently not comprehensive enough to protect citizens from predatory foreign actors. This indicates a need to understand better non-state IOAs' role in digital election interference to produce better mitigation and protection strategies.

This dissertation aims to investigate online political campaigning in elections in the Global South by non-state IOAs, asking how does the involvement of non-state IOAs influence elections in the Global South? There are three primary objectives of this research; 1) to assess the use of disinformation in the 2013 and 2017 Kenyan Presidential Elections, exploring how it was used, whom it was used by and what it contained; 2) to develop an understanding of the motivations of non-state IOAs in interfering in these elections and the methods used to do so and 3) to explore these findings with reference to the theoretical concept of data colonialism.

Understanding the link between the involvement of such actors in foreign elections and neo-colonial power imbalances will help to fill gaps in the literature mentioned above. The research will address election interference by non-state IOAs as one form of data colonialism. It acknowledges multiple manifestations of data colonialism in the contemporary political sphere, many of which are more aggressive and less visible. The visibility of this case is what allows its exploration here; by analysing this form of online political campaigning in a data colonial context, we can further develop our understanding of this theory and aim to address other, more potent, manifestations of data colonialism in the future.

A complete discussion of foreign election interference by non-state actors involving multiple cases is beyond the scope of this study. Due to practical constraints, the analysis presented here is based solely on two instances from one case. The secretive nature of this phenomenon puts considerable limitations

on the available information. Thus, further in-depth research would need to be undertaken to gain evidence on less-publicised cases.

The dissertation is composed of six main chapters. It will begin with a thorough review of the current literature regarding disinformation, Big Data, non-state IOAs and data colonialism. This review will explore definitions and primary debates surrounding these essential components of digital election interference. In particular, it will address the efficacy of such techniques and how they threaten modern democratic practices.

The second section will overview the main conceptual framework. It will highlight critical linkages between the topics discussed in the literature review and explore how data colonialism can be used to assess election interference in the Global South. It will then outline the research design and methodological framework used for this study. To do this, it will give an account of the work undertaken by multiple political consulting firms in the 2013 and 2017 Kenyan Presidential Elections, using qualitative data from investigations and news reports to thematically analyse several research areas. NVivo will be used to conduct this analysis, allowing a comprehensive investigation that answers the above research question and aims.

The following sections will constitute the analytical body of the dissertation. Split into five sub-sections: case history, motivation, methods, content, and impact, it will look at how political consulting firms operated in Kenya during 2013 and 2017 to provide a new perspective on their work there, particularly the effect of this.

The penultimate chapter will address the above analysis in relation to the data colonial framework outlined in Chapter 3, bringing cohesion between the theory and empirics. It will show how data colonial practices are enabled through electoral interference and non-state IOAs' role in perpetuating this. The final chapter will conclude with the policy implications of these findings, research limitations, and an indication of future research directions.

2. <u>Literature Review</u>

Presently, a well-developed body of literature focuses on targeted disinformation in elections and its impact on the democratic process. Alongside this, a developing body of work investigates the theory of data colonialism and how this is currently impacting technological freedoms in the Global South. To date, only a limited number of studies have combined these two approaches to build a comprehensive view of how technological advancement impacts global politics, taking into account historical power asymmetries and relations.

This review will summarise the existing body of knowledge whilst highlighting current gaps that will be addressed. It will first overview the literature on disinformation and social media before looking at Big Data and what scholars call the 'Analytics Turn'. The following section will explore the literature surrounding microtargeting and psychometric profiling within political campaigning, followed by an assessment of the current academia on non-state IOAs. Finally, the review will address the decolonial turn in information studies to overview current theories of data colonialism.

2.1. <u>Defining Disinformation</u>

The United Kingdom's Digital, Culture, Media, and Sport Committee (2019) has described disinformation as an inherent part of modern political life. It has been central to several high-profile political events, such as the 2017 French Presidential Elections (Bulckaert, 2018) and the 2019 European Parliament Elections (Bendiek and Schulze, 2019). For this reason, a considerable amount of literature has been published on disinformation. These studies focus on its growing use and the impact of this on international politics.

Several definitions of disinformation have been proposed. These generally contain three main components. Firstly, disinformation consists of false, inaccurate, or manipulated information (DCMS Committee, 2019; Maweu, 2019, 65; Wardle and Derakhshan, 2017, 6). This can be composed of a mixture of fact and fabricated content, manipulated images and videos or false

information sources (Bennett and Livingston, 2018; McKay and Tenove, 2021, 704). Secondly, this information is knowingly and intentionally shared (Bennett and Livingston, 2018; DCMS Committee, 2019; Maweu, 2019, 65; Wardle and Derakhshan, 2017, 6; Weedon, Nuland and Stamos, 2017, 5). Finally, disinformation is shared to advance specific aims or goals. It is often intentionally spread to arouse passion, attract viewership, and deceive readers, all to achieve a political purpose (Bennett and Livingston, 2018; Maweu, 2019, 65; Weedon et al., 2017, 5). The DCMS Committee (2019) claims that disinformation is spread to cause harm or political gain. These campaigns often seek to amplify social divisions and distrust (McKay and Tenove, 2021, 704). It is important to note that disinformation is widely regarded as a long-observed tactic deployed during election campaigns throughout history (Bakir, 2022, 4; Chambers, 2020, 149; Grigsby, 2017; Maweu, 2020, 63). However, disinformation has become more prevalent because of the digitisation of democracy and the advent of social media (Alcott, Gentzkow and Yu, 2019, 1; Berghel, 2018; Maweu, 2020, 63). These views are consistent with those of Grigsby (2017), who notes that the ever-increasing use of digital technologies has made disinformation highly prominent in today's international arena.

There has been a global shift towards digital communication, so much so that daily life has become 'digitised'. Social media has unlocked new ways for citizens to share their views, with Persily (2017, 74) noting that social media platforms "are the new intermediary institutions for our present politics". According to Schia and Gjesvik (2020), the Internet has several key features that have changed how information is shared. These include the removal of geographic boundaries, the ability to share information anonymously and the ability to reach larger audiences, bypassing the gatekeeper role of the traditional media (Schia and Gjesvik, 2020, 415). This shift has resulted in improvements in freedom of speech and expression but has also allowed the rapid spread of disinformation facilitated by technological advancements in social media platforms.

Social media has the perfect design for allowing the spread of disinformation. Scholars argue that online disinformation campaigns exploit vulnerabilities in

the structures of such platforms (McKay and Tenove, 2021, 708). Several perspectives support this argument; messages and posts can be sent and received almost instantly, meaning that disinformation can spread quickly throughout the online world (Lion, Kropotov and Yarochkin, 2017, 4). Persily (2017, 70) has found that deception spreads much quicker than truth on social media, and Allcott and Gentzkow (2017, 221) note that the low cost of such campaigns means that anyone can conduct them and gain considerable profit. The biggest reason put forward for the efficiency of disinformation on social media is the use of algorithms and selective bias. Social media networks are often ideologically segregated; thus, people are likelier to read or share articles that align with their ideological position (Allcott and Gentzkow, 2017, 221; Maweu, 2020, 67). Further, there is often an automatic selection of content with which users interact (Schia and Gjesvik, 2020, 415), meaning that viewers generally have no choice in what they interact with, restricting them to their ideological segregation.

Social media's effectiveness in supporting disinformation spread has resulted in widespread concern for the implications on democracies and electoral processes. Several global institutions have stated that they are worried about the proliferation of disinformation online. For instance, the World Economic Forum has listed digital misinformation as one of the main threats to our society (Howell, 2013). This is supported by many scholars, calling disinformation "the defining political communication topic of our time" (Freelon and Wells, 2020, 145), "a social vulnerability" (Schia and Gjesvik, 2020, 414) and a "critical issue facing contemporary digital society" (Howard and Bradshaw, 2018). Adding to this fear, commentators have argued that efforts to fight disinformation are not working to the extent that it is becoming unstoppable (Ghosh and Scott, 2018; Levin, 2017).

2.2. Big Data and The 'Analytics Turn'

Disinformation on social media exists as a considerable threat on its own. However, the latest advancements in data analysis have exacerbated this threat considerably. The rise in disinformation online has coincided with and been

amplified by the datafication of daily life. More recent attention has focused on how social media has created extensive collections of aggregated personal data (Ekdale and Tully, 2019; Solove, 2004; Tenove, Buffie, McKay and Moscrop, 2018, 19). Because social media plays a central role in users' daily lives, it can collect mass amounts of information (Chester and Montgomery, 2017, 3). These platforms can acquire data via likes, posts, profile information, connections, data from photographs and videos and user login information (Crain and Nadler, 2019, 377). Data's pervasive role in today's information ecosystem has changed the nature of social life as we know it. Rosenberger (2020, 204) describes this change, stating that as the amount of data about us grows, it is being collected and fed into a digital information ecosystem that invisibly shapes our information reality. This change has been caused by a growing range of analytical tools, which have enhanced the ability of actors to gain valuable insight from generated data points (Chester and Montgomery, 2017, 3). Many businesses now see data as a valuable by-product of their work, a recent Harvard Business Review article titled "To Get More Value from your Data, Sell It" (2016) discusses the benefits of collecting and selling data for businesses who want to increase profits. This represents a shift in thinking towards seeing data as a profit-producing resource that can be extracted from individuals.

This shift has had a knock-on effect in the realm of electoral interference. Dowling (2021, 385) has identified that because of the widespread availability of personal data, the target pool of information campaigns has increased significantly; now, anyone can be targeted by malicious cyber actors. It is relatively cost-effective and straightforward to acquire intelligence on citizens of a particular state, process this using machine learning and create valuable insights used to manipulate (Dowling, 2021, 385). To date, several studies have investigated this phenomenon; Grassegger and Krogerus (2017) explored how Cambridge Analytica used data in their campaigning; Crain and Nadler (2019) analysed the weaponisation of the digital advertising infrastructure, and Tufekci (2018) concluded that advertisers and political campaigners use data to create profiles of 'desirable' audiences and target political messaging. Taken together, these studies support the notion that the rise of social media and the data that it produces has become instrumental in changing the efficacy of electoral

interference. Further, this data has allowed for the more targeted dispersal of disinformation, making it even more potent.

Chadwick and Stromer-Galley (2016) have proposed the 'Analytics Turn'. This is the increased usage of experimental data science methods to analyse large-scale collections of personal data to influence key segments of the electorate to act a certain way (Chadwick and Stromer-Galley, 2016, 284). Gorton (2016, 62) makes a similar point in his study of political campaigning firms, stating that technological advancements in the behavioural science community combined with marketing techniques developed for selling consumer products produce the power to manipulate.

Following these conclusions, several studies have begun to examine advancements in consumer marketing techniques, attributing the Analytics Turn to their co-option by the political consulting community (Chester and Montgomery, 2017, 4; Tenove et al., 2018, 5). Tufecki (2014) demonstrated that the commercial sector first developed and deployed many of the digital strategies used in the 2016 US Presidential Election. Additionally, Crain and Nadler (2019, 376) theorise that the digital advertising infrastructure provides three interlocking communication capacities. First, the capacity to use consumer monitoring to develop detailed consumer profiles. Second, the ability to target highly segmented audiences with strategic messaging across devices and contexts. Finally, the capacity to automate and optimise tactical elements of influence campaigns (Crain and Nadler, 2019, 376). Importantly, they also argue that there have been relatively few attempts to understand the linkages between manipulation campaigns and the digital advertising systems where they originate (Crain and Nadler, 2019, 370). They suggest that data-driven digital advertising has played a vital role in facilitating political manipulation online because of its current design and management (Crain and Nadler, 2019, 372). This design has become weaponised, so consumer data is now being used to shape and modify political behaviours and attitudes (Crain and Nadler, 2019, 370). These studies, therefore, clearly indicate a relationship between consumer marketing techniques and the increased use of targeting within political campaigns to manipulate potential voters.

Political campaigners are increasingly deploying these tools to conduct influence activities, often for coercive and deceptive purposes (Bakir, 2022, 3). So much so that it is widely argued that electoral politics has become integrated into a global commercial digital media and marketing ecosystem (Chester and Montgomery, 2017, 2; Gorton, 2016, 68). Much of the literature on this subject pays particular attention to the phenomenon of 'online political microtargeting'. In this literature, the term is used to refer to a type of personalised communication that involves collecting information about people and using this to target political advertisements (Heawood, 2018, 429; Tenove et al., 2018, 19; Borgesius et al., 2018, 82). This involves taking the plethora of publicly available data described above and creating finely honed messaging (Gorton, 2016, 68; Tenove et al., 2018, 20; Borgesius et al., 2018, 83). During elections, this technique is used to identify voters likely to vote for a specific party or concerned with a particular policy issue and target them with mobilising messaging (Borgesius et al., 2018, 83). Several studies have shown that microtargeting is effective and can be easily deployed (Crain and Nadler, 2019; Isaak and Hanna, 2018). In 2017, leaked documents revealed that Facebook claimed the ability to predict its teenage users' emotional states to give advertisers the means to reach those who feel 'worthless,' 'insecure,' and 'anxious' (Crain and Nadler, 2019, 378). The studies presented thus far provide evidence that suggests microtargeting is both commonly used and increasing in effectiveness.

This concept is similar to that of psychological profiling. This has been described by the European General Data Protection Regulation (2016) as a form of automated processing of personal data to analyse or predict aspects relating to that person's preferences, interests, and behaviour. This is consistent with the CEO of Cambridge Analytica's claim that this technique allowed campaigners to know what persuasive messages need to be delivered, on what issues, to what personality types and to what groups of people before the messages are even created (Bakir, 2022, 2). In some cases, it has been shown that advertisers have tried to develop underlying psychological profiles to create influence campaigns customised to psychological dispositions (Crain and Nadler, 2019, 377). As

these methods have advanced, advertisers can design campaigns around traits that may not even be disclosed by the individual (Crain and Nadler, 2019, 378). Such inferences have made it possible to target or exclude politically sensitive groups for these campaigns (Crain and Nadler, 2019, 378). Supporting this view, Hinds, Williams and Joinson (2020, 2) found that advertisements psychologically tailored towards an individual's socio-demographics and preferences were more effective than non-tailored advertisements. This literature aligns with that described above, allowing us to infer that microtargeting and psychological profiling are two sides of the same coin: using personal data to manipulate thought intentionally.

Considering all this evidence, it is clear that this is a problematic use of people's data and presents significant implications, especially during election periods. Much of the current literature on microtargeting pays particular attention to the problems with these techniques and explains how they have led to the potency of modern-day disinformation. Previous research has established that microtargeting manipulates individuals' opinions through corroding and inhibiting public dialogue by shielding viewers from information that may challenge their beliefs (Gorton, 2016, 69; Tenove et al., 2018, 21). Along the same lines, microtargeting is seen as harmful because it exploits personal data non-consensually in a way that conceals the true nature of the information (Heawood, 2018, 431). A broadly similar point has also been made that disinformation actors can target messages in a way that avoids detection by more critical publics, allowing the avoidance of questioning or critique (McKay and Tenove, 2021, 706; Tenove et al., 2018, 21). Data-driven advertising is designed "like a one-way mirror" where campaigners and tech platforms can "see the public, but the public cannot see them" (Ravel, Woolley and Sridharan, 2019). Crain and Nadler (2019, 706) further this point stating that social media companies have not yet released all the data necessary to offer a fully detailed picture of manipulation campaigns. Those using such techniques can often not even say themselves why a particular voter is considered 'friendly' or not; the data analysis is far too subtle and complicated to be understood by the human mind (Gorton, 2016, 69). Gorton's work is complemented by McKay and Tenove (2021, 705), who propose that algorithmic curation is opaque in that

most users do not understand how their individual information feeds are moderated, and most researchers do not have the appropriate data to analyse this.

Other writers have argued that this targeting could be positive because it can amplify the effects of campaigns on citizens, enabling politicians to engage audiences through more relevant advertising (Borgesius et al., 2018, 85). However, the precise nature of this targeting is often highlighted as one of the main problems with microtargeting. More specifically, how messages can be personalised to specific audiences and devised to exploit cognitive dispositions and information deficits (Tenove et al., 2018, 21). Microtargeting can even target messaging designed to incite citizens by playing on biases and psychological states (Tenove et al., 2018, 21). Gorton's (2016) work furthers this by showing that with the use of psychographic profiles, potential non-voters may be encouraged to abstain. He quotes an anonymous political activist who notes, "The data let you target. Who would want to target non-voters, for example? Big waste of time" (Gorton, 2016, 70). This highlights an issue with microtargeting in political campaigns where potential voters' behaviour is controlled to achieve a particular outcome. Young et al. (2018, 3) call this 'stealth media', a media system that allows deliberate operations of political campaigns with undisclosed identities, clandestine messaging on divisive issues and imperceptible targeting. Along the same lines, Gorton (2016) proposes four ways that such techniques enable manipulation:

1) They produce more precise predictive power.
2) The experimentation itself alters the behaviour of voters without their awareness.
3) The use of these methods, especially in conjunction with each other, serves to undermine a healthy public sphere by individualising, distorting and isolating information.
4) Many of these techniques are grounded in models of unconscious processes of the mind (Gorton, 2016, 63).

16

The DCMS Committee (2018, 3) has ultimately concluded that the "relentless targeting of hyper-partisan views, which plays to the fears and prejudices of people, in order to alter their voting plans", is arguably "more invasive than obviously false information" and is a "democratic crisis". An important theme arises from the literature described above; microtargeting harms public debate, personal freedoms, and democratic integrity as a whole.

2.3. Non-State Information Operation Actors

So far, this paper has focused on the rise of disinformation and microtargeting, specifically during elections. The following section will discuss the actors involved in such manipulations and their role in the broader political campaigning sphere.

Digitisation has enabled non-state IOAs to interfere in elections and democratic processes through the means of microtargeting and disinformation at an unprecedented level (Dowling, 2022, 230). Political consulting firms such as Cambridge Analytica gained infamy as one of the first non-state IOAs to digitally interfere in elections (Dowling, 2022, 231). Morgan (2018, 40) highlights the role of foreign actors and how this is changing, arguing that manipulation efforts across geographic boundaries occur not only in state-sponsored efforts but also through motivated actors wishing to promote a particular worldview. It is now well-established that political candidates are using political consulting firms to do this work for them. Couldry and Mejias (2019, 340) describe such actors as "data analysis brokerages", a largely unregulated part of the economy that specialises in collecting information from data so that individuals can be categorised through algorithms. However, this definition only details one part of the process, failing to account for the broader definition of non-state IOAs. Although extensive research has been carried out on disinformation campaigns, few studies define the actors involved in these. This section will piece together such a definition from what is available in the literature.

One of the most prominent features of the modern political system is the rise in the number and importance of non-state entities (Geeraerts, 1995). In 1995, Geeraerts noted that the study of non-state actors was still relatively new. Thus, much of the terminology for classifying them was unclear and contradictory; the same could be said for contemporary efforts to understand non-state IOAs. A non-state actor is an entity that has significant political influence and is visible and active on the international stage but is not directly tied to a state (Buchan and Tsagourias, 2016, 377; Gross, 2016, 112). These actors do not exercise formal power over a given population but may have formal membership in the form of bases, employees, and sympathisers (Wijninja, Oosterveld, Galdiga and Marten, 2014, 144). As a result, non-state actors can sometimes be very influential and, in some ways, even more powerful than the state itself (Wijninja et al., 2014, 144). It is now well established that non-state actors take many forms, from ideological extremist groups and anti-vax advocates to political campaigning firms (Mavriki and Karyda, 2019). The literature argues that non-state actors are gradually assuming more responsibility under international law (Wijninja et al., 2014, 144). However, this generally only applies to non-state actors involved in physical conflict, those in the cyber sphere have yet to be adequately understood in international law.

Several definitions of information operations have been proposed. Fecteau (2022) defines them as campaigns dedicated to obtaining a decisive advantage in the information environment. According to Facebook Security, they are actions taken by organised actors to distort domestic or foreign political sentiment, most frequently to achieve a strategic outcome (Fecteau, 2022). RAND Corporation (n.d.) writes that information operations are the collection of tactical information about an adversary and the dissemination of propaganda to pursue a competitive advantage over an opponent. This definition is close to that of Crain and Nadler (2019, 374), who define them as deceptive communication strategies that use data-driven advertising to target vulnerabilities in attempts to shape discourse or change behaviour.

By combining the above literature, we can define non-state IOAs as actors not tied to a particular state but with significant political influence that conduct

campaigns dedicated to obtaining decisive advantages in the information environment. Surveillance technology companies and political microtargeting firms can be considered part of this definition. These companies profit from their services and often do so to promote an ideology (Cadwalladr, 2017; Privacy International, 2017a). Social media companies can also be considered non-state IOAs as they pursue their own corporate and ideological global interests (Fuchs 2017; Gillespie 2010). Both groups interfere in elections to the extent that they shape people's contributions to public debate and create vulnerabilities in the information environment (Tenove et al., 2018, 19).

Several studies have begun to examine how these information operations actors operate. Many focus solely on state or state-sponsored actors, neglecting to analyse the increase in the involvement of non-state IOAs, such as political consulting firms, in global politics. Tenove et al. (2018, 1) suggest four principles foreign actors use in elections: hacking attacks, mass misinformation and propaganda campaigns, microtargeted manipulation, and trolling operations. This study will focus on two of these, mass misinformation and microtargeting. Tenove et al. (2018, 2) argue that these actors sometimes promote particular candidates, policies, or ideologies through these mechanisms. They may also seek to undermine government legitimacy, exacerbate social tensions, or erode democratic trust (Tenove et al., 2018, 2). This particular research describes foreign state actors but can easily apply to non-state IOAs, who share a similar modus operandi. They concluded that foreign entities now have significantly greater access to personal data making it easier for information operations to occur (Tenove et al. 2018, 19). A similar point has also recently been made by Nadler, Crain and Donovan (2018), who identify a "digital influence machine" consisting of various surveillance and data analysis tools utilised by influencing actors to mobilise supporters and divide opponents via behavioural science. Companies like Google, Facebook and Cambridge Analytica now play a central role in this digital influence machine, offering a full spectrum of commercial digital marketing tools and techniques designed for political use (Bond, 2017). For example, Facebook has created an 'identity-based' targeting platform that enables political campaigns to access its customers and target them by age, gender, and interests (Chester

and Montgomery, 2017, 4). Further, the business models of social media companies depend on the circulation and sharing of attention-garnering content rather than accurate or high-quality information (Tenove et al., 2018, 40). The infrastructure available for microtargeting and manipulation did not come into being naturally; it was created and is now controlled by these non-state IOAs, allowing them to act largely unregulated outside state control.

The above relates to a significant issue with the increasing use of political consulting firms during elections; these entities are under-studied in academia and international law. The lack of regulation or guidelines for these operations has created a loophole for outside groups to run political advertisements on popular digital platforms concealing their true nature (Young et al., 2018, 3). Furthermore, because these operations generally take place below the radar, they are not fully understood by the public (Chester and Montgomery, 2017, 2). This limited understanding of how they operate makes them all the more dangerous, limiting effective responses to their actions.

Having defined what is meant by non-state IOAs, I will now discuss the literature surrounding the effectiveness of their campaigns. A large and growing body of literature has investigated the impact of the techniques outlined above. A few of these studies propose that disinformation, microtargeting and interference have a smaller impact than feared. Several researchers have criticised the idea that disinformation can effectively alter perceptions (Benkler, Faris, and Roberts, 2018). This is consistent with arguments put forward by Allcott and Gentzkow (2017, 22), who question the claim that fake news swayed the 2016 US Presidential Election, noting that even the most widely circulated stories were only seen by a small fraction of Americans. They found that Television remained the most dominant news source and calculated that for fake news to change the election outcome, a single article would have needed the same persuasive effect as 36 TV campaigns (Allcott and Gentzkow, 2017, 22). Similarly, Grassegger and Krogerus (2017) maintain that it is hard to know exactly how much of the American population was targeted via microtargeting because of the personalised nature of such campaigns. Data about disinformation is often inconsistent as many of these activities take place

secretly, and thus painting an accurate picture of the use of disinformation is hard (Bradshaw and Howard, 2018). Tenove et al. (2018, 26) support the above, stating that solid evidence about the effects of meddling is limited and that they did not find conclusive proof that foreign interference using microtargeting changed the outcome of an election from one candidate to another. These arguments show scepticism of the efficacy of microtargeted disinformation campaigns by non-state IOAs, especially for their ability to change the popular vote drastically.

Other authors would refute these claims, however. Persily (2017, 69) notes that the power of fake news and disinformation does not derive from changed attitudes but from how it demobilises, causes confusion, and erects barriers to informed political decision-making by hiding genuine information. Dowling (2022, 231) supports this argument, pointing to the undermining of democratic decision-making processes. These studies highlight a crucial point; whilst being unable to change who is elected directly, targeted disinformation can have more profound, more widespread consequences.

Evidence suggests that foreign actors can use digital techniques to undermine citizens' political participation in various ways. Disinformation can be used to discourage voters from going to the polls (Eordogh, 2016). Existing research suggests that advertisements can be more effective at increasing or depressing voter turnout and influencing whether people will vote for lesser-known candidates (Holtz-Bacha, Just, Ridout and Holland, 2017; Krupnikov, 2014). Further, it can lead to a weaker understanding of public issues and a disagreement on facts, potentially leading to belief in dangerous conspiracy theories (Martin, 2017; Marwick and Lewis, 2017; Peters, 2017). This could create division and distrust in society, especially during unstable election periods. This view is supported by the widely acknowledged notion that disinformation can be created, disseminated, and targeted in ways that amplify existing divides to drive wedges between allies and undermine shared norms of democratic debate (Canadian Security Intelligence Service, 2017; King, 2016). Lastly, various studies have shown that social media negatively affects decision-making, information sharing and personal expression. It may lead to an increase

in exposure to ideological heterogeneous information (Eady, Nagler, Guess, Zilinsky and Tucker, 2019, 2); online messages may influence a variety of offline behaviours (Bond, Fariss, Jones, Kramer, Marlow, Settle, and Fowler, 2012, 298), and users tend to select and share content related to a specific narrative and ignore the rest (Del Vicario, Bessi, Zollo, Petroni, Scala, Caldarelli, Stanley, and Quattrociocchi, 2016, 558). Together these studies provide important insights into the impact of information campaigns by political consulting firms. Whilst there is doubt about their ability to change electoral outcomes, there is consensus that they can affect society on a deeper level, harming decision-making and political dialogue.

2.4. Data Colonialism

So far, this review has focused on disinformation, microtargeting, and political consulting firms in general terms. The following section will discuss the current debate on data colonialism and how this relates more broadly to the discussions outlined above. The research to date has tended to focus overwhelmingly on digital politics in the Global North rather than the impact of non-state IOAs in the Global South. In relation to digital election interference, the focus has primarily resided on Brexit and the 2016 US Presidential Election (Nyabola, 2019; Young, 2019). Even though the impact of such interferences is often hardest felt in less-developed countries where authoritarianism is a constant threat (Nyabola, 2019). Young (2019) notes that discussions tend to be more instrumental and one-dimensional when the focus shifts to the Global South. Often digital participation is implicitly assumed to be beneficial in instrumental ways, such as enabling economic advances or providing access to better services (Young, 2019). Debates fail to take a critical approach to digital innovation in the Global South, especially that which is promoted by Western corporations. It has been argued that there is currently inadequate theory to examine how the local context is impacted by digital technologies (De, Pal, Sethi, Reddy, and Chitre, 2018). This may explain why the current debate surrounding this area is often one-sided.

Researchers are now calling for greater attention to the colonial implications of technological engagement (Young, 2019). Avila Pinto (2018) has described Big Tech's relations with countries in the Global South in terms of the dependency their tools create; Zuboff (2019) discusses the era of surveillance capitalism in which platforms are susceptible to surveillance processes, and Nhemachena, Hlabangane, and Kaundjua (2020) call for African data sovereignty in response to renewed threats of colonisation. Collectively, these studies outline a critical need for continued exploration of this subject matter so that appropriate theoretical standpoints can be produced to deal with the current realities.

In the last three decades, there has emerged a "decolonial turn" in the field of data studies (Couldry and Mejias, 2023, 786). This turn has provided a theory of data extractivism that can articulate practices that impact human life and freedom globally (Couldry and Mejias, 2023, 794). There are a growing number of theorists who propose the idea of data colonialism in response to the West's technological advancements in the Global South (Couldry and Mejias, 2019; Ekdale and Tully, 2019; Kwet, 2019). This concept has been used as a metaphor to understand the shifting terrain of data's role in society. It has the advantage of highlighting the power asymmetries inherent in data commodification (Thatcher, O'Sullivan and Mahmoudi, 2016, 992).

Several definitions of data colonialism have been proposed. Couldry and Mejias (2023, 297) have divided these into three main categories. The first is 'digital colonialism', used mainly by Kwet (2019). He defines digital colonialism as a structural form of domination exercised through the centralised ownership and control of the digital ecosystem's three core pillars: software, hardware, and network connectivity (Kwet, 2019). In this theory, digital colonialists build communication infrastructure for harvesting data, storing this as raw material, and creating profit (Coleman, 2019, 422). In this view, data and technology practices in the Global South are directly continuous with earlier economic imperialism (Couldry and Mejias, 2023, 789). This form of decolonial thought considers data practices to sustain themselves in inherited imperialism (Couldry and Mejias, 2023, 795). The second category falls under 'technocolonialism', a theory that appears least within the literature. This posits that data practices

take a specific form of neo-colonial setting because of the distinctive social and economic power characteristics of these settings (Madianou, 2019). Madianou (2019, 2) argues that data-powered humanitarian organisations enact a technocolonialism that reinvigorates and reworks colonial relationships of dependency. Lastly, there is 'data colonialism', the most commonly used term. This is the belief that practices of data appropriation and processing are themselves a distinctive new type of resource extraction, representing a new phase of colonialism (Couldry and Mejias, 2019). It involves new modalities of oppression that may be less outwardly disruptive and unfold in different ways but still have fundamental impacts (Couldry and Mejias, 2023, 797). This theory argues that what is happening with data constitutes a new state of colonialism that combines the predatory extractive practices of historical colonialism with Big Data technologies (Couldry and Mejias, 2019, 337; Couldry and Mejias, 2023, 787). This final definition will be predominantly used in this research as it most adequately describes this phenomena's connection to history whilst acknowledging the impact of technological advancement.

There are some key tenants of the data colonial perspectives. The social quantification sector is considered the principal actor in data colonialism, and Big Data is the central component (Couldry and Mejias, 2019, 340; Kwet, 2019). Historically, corporations played a pivotal role in colonialism through the "pathological pursuit of profit and power" (Coleman, 2019, 420). In the modern context, Big Tech corporations are considered the primary actors of data colonialism, possessing monopolies over digital infrastructures (Magalhães and Couldry, 2021). Many functions are dominated by a handful of predominantly American multinational corporations; search engines (Google), web browsers (Google Chrome), smartphones (Apple and Android) and so on (Kwet, 2019). Colonial conquest typically entailed the dispossession of valuable resources from indigenous groups to the control of colonial powers (Kwet, 2019). Under data colonialism, the same thing happens; foreign powers use their infrastructure to extract personal data and use this for profit. This is worsened by the idea that Africa is an "untapped data market" (Coleman 2019, 425, 431). Hendricks, Vestergaard and Marker (2018) argue that this structure has four principal actors:

1) Western tech companies that create and provide the technology and infrastructure that harvest the data for advertising, targeting and distribution.

2) Advertising and consulting firms that use this technology to target various groups with highly personalised advertisements and messages.

3) Local companies, parties and organisations who pay 2) to help them impose their agenda.

4) The citizens who knowingly or unknowingly act as data sources for 1) and targets for 2) and 3) (Hendricks, Vestergaard and Marker, 2018).

Collectively, these studies outline the critical role of corporations in both historical and present-day colonial activities. They highlight how predominantly Western, big tech firms are now the main perpetrators of data colonialism and how the infrastructures created by these actors are the main enabling tools.

Kwet (2019) considers Big Data to be the central component of digital colonialism. The WEF (2011, 5) claims that personal data will be the new "oil", a valuable resource of the 21st century. Coleman (2019, 424) states that data has become a new currency wherein access to it is now the most valuable asset available to nation-states and corporations. Social life has become an open resource for extraction for profitable gain (Couldry and Mejias, 2019, 337). This idea that data is a natural resource has been criticised as problematic in itself, causing a blurring metaphorically that suggests data is merely an exhaust of people's lives and thus incapable of being owned by anyone (Couldry and Mejias, 2019, 340). A broadly similar point has also been made by Fraser (2019, 193), who argues that what makes the process of data accumulation colonial is not so much that it involves foreign powers subjugating and controlling indigenous populations but the way that digital subjects are dispossessed and alienated from the very data they create. Several studies have problematised this extraction of personal data for profit (Couldry and Mejias, 2019, 11; Tait, Peron

& Suárez, 2022; Thatcher et al., 2016). It has been stated that a parallel can be drawn between the dimensions of violence and expropriation of historical colonialism and new forms of exploitation that characterise the processing of personal data (Tait et al., 2022, 11). Adding to this, Thatcher et al. (2016, 994) argue that the process in which our data is converted into a useful resource is part of an asymmetrical relationship between data producers and data collectors. They demonstrate that as technology users enter into data license agreements, they are dispossessed of the right to control their own data (Thatcher et al., 2016, 994). This aligns with Golumbia's (2009) view that only "big money and big power" can reap the benefits of data.

At the very centre of historic colonialism was the economic agenda to provide maximum financial benefit at a minimal price; this is the same situation here (Coleman, 2019, 420). The extraction of value through data represents a new form of resource appropriation on par with the land grab that started historical colonialism (Couldry and Mejias, 2023, 788). Thus, if we combine the two aspects discussed here – corporations and Big Data – we create a situation where the most extensive sets of valuable data are dominated by a handful of (Western) corporations (Kwet, 2019). It is important to note that although this research will focus on Western intervention in the Global South, it has been argued that data colonialism can exist both externally, on a global scale, and internally toward home populations (Couldry and Mejias, 2019, 337).

There have been some criticisms of this theoretical concept. The most notable of which comes from Casilli (2017), who accepts a "digital decolonial turn" but rejects other less coherent interpretations of contemporary data practices as 'colonial'. He argues that the usage of the term 'colonial' falls prey to the "neocolonialism pitfall", which assumes that any form of international power relation can be conflated with neo-colonial dynamics (Casilli, 2017, 3945). This, he states, removes agency from the Global South and paints them as victims of external power, a dynamic which is not necessarily accurate for contemporary politics (Casilli, 2017, 3946). This is an important perspective; however, it fails to acknowledge situations where political elites and local actors are involved in accepting the "colonisers" into their home state. Further

criticisms warn against assuming that datafication plays out the same way everywhere and ignoring the struggles over data extractivism in various contexts (Couldry and Mejias, 2023, 793). A final notable criticism comes from Segura and Waisbord (2019, 417), who claim that methods of datafication are not 'colonial' because they are not inherently violent. This appears to be a significant point of departure between historical and contemporary data colonialism (Couldry and Mejias, 2019). An alternative to this argument is that as social relations have developed, physical violence as a method of colonialism has been replaced by other ways, including symbolic forms of violence such as data dispossession (Jasanoff, 2006). Together these criticisms provide essential insights into the development of this theory. They warn against assuming homogeneity in cases of data colonialism and the denial of agency of actors involved; these are important points to consider.

In terms of empirical research, there is some intersection between theory and practice. Only in the past few years have studies of data colonialism directly addressed its impact on the Global South. In relation to the African continent, academics have criticised the monopoly that predominantly Western companies have over the technology infrastructure in the area (Coleman, 2019; Nyabola, 2018a). Limited work has been completed regarding the relationship between data colonialism and the involvement of non-state IOAs in elections. Despite the end of colonial rule, many foreign states have continued to meddle in African development and democratisation (Bates, 2008). Ekdale and Tully (2019) are some of the only authors to have synthesised the theory of data colonialism with cases of digital election interference in Kenya and Nigeria. They present three core issues with this form of election interference: data privacy and protection, unethical campaigning on social media, and foreign involvement in emerging democracies (2019, 28). This is some of the only research that addresses both the innovation of microtargeting voters during elections and the relation this has with data colonialism. It is influential research for this study.

2.5. Literature Gap: Connecting Data Colonialism with the Wider Discourse

There remain several aspects about the intersection between data colonialism and non-state IOAs, of which relatively little is known. There is, thus far, little cooperation between the two fields of study, both of which could benefit from each other. This is the gap that this dissertation aims to address.

Research on interference in elections by IOAs is relatively well developed, despite it mainly focusing on state actors. There are discernible definitions of disinformation and microtargeting which can be applied to the work of non-state IOAs. Taken together, these studies also support the notion that the Analytics Turn in election campaigning presents a considerable threat to democratic integrity. However, this literature has tended to focus on instances of Western victimhood, failing to address the consequences in states with much lower levels of democratic stability and Internet protections. This is problematic neglect, especially as the consequences in these states can often be much worse.

Similarly, the literature on data colonialism is in a nascent theoretical stage. Opinions, criteria, and categorisations are just being operationalised, and thus there are few instances where theory is applied to empirical examples. Notwithstanding this, there is a clear definition of data colonialism within the literature and an evolving debate surrounding it. This is an essential first stage in the theory's development and will be aided by interaction with the broader digital election campaigning literature.

Digital election interference by non-state IOAs, particularly in the Global South, fulfils many of the theoretical criteria of data colonialism. First, it involves the extraction and manipulation of citizens' data, often without their knowledge or consent. Secondly, the principal actors of this are large corporations with a monopoly over the digital infrastructure creating a power imbalance that often results in destabilisation. For this reason, I believe this phenomenon presents an interesting empirical case to be applied to data colonialism to help us understand the concept further. The only research to do this is presented above – Ekdale and Tully (2019) – this work will expand on theirs, addressing further the

linkages between digital election interference by non-state IOAs and the concept of data colonialism.

3. <u>**Conceptual Framework and Methodology**</u>

Before proceeding to the analysis section of this work, it is important to rigorously lay out and define the conceptual framework and research design that will be utilised. This section will outline key concepts used throughout and link them to an overall methodology to answer the research question. This dissertation takes the shape of a qualitative study that ultimately aims to describe and explain a pattern of relationships; this can only be done with a set of conceptually specified categories (Mishler, 1990, 431). Therefore, it is necessary first to define the concepts that will be used to explore the empirical case.

3.1. Conceptual Framework

Miles and Huberman (1994, 440) state that a conceptual framework "lays out the key factors, constructs, or variables, and presumes relationships among them". The following section will outline fundamental concepts and theories used within the research, connecting them to create a cohesive conceptual framework that aligns with the research aims. As a reminder, this dissertation seeks to explore the involvement of non-state IOAs in elections in the Global South. It has three critical guiding objectives: to assess the use of disinformation in the 2013 and 2017 Kenyan Presidential Elections, to develop an understanding of the motivation of non-state IOAs in interfering in these elections and the methods used to do so, and to explore these findings with reference to the concept of data colonialism.

The theory of data colonialism will be used as a lens through which to view the involvement of non-state IOAs in elections in the Global South. According to this theory, practices of data appropriation, extraction and processing represent a new form of colonialism informed by the practices of historical colonialism (Couldry and Mejias, 2019). This is worsened by the monopoly held by Western tech companies over technology infrastructures leading to a state of dependency through resource extraction. This is a highly nuanced theoretical concept that is

still in the nascent stages of development, and thus this research uses a much-simplified version to explore the empirics adequately.

The theory of data colonialism used in this research has three fundamentals:

1) *The social quantification sector is the principal actor* (Couldry & Mejias, 2019, 340). Just as corporations were the main actors of historical colonialism, so too are they the principal actors in this new stage. They possess a monopoly over technology infrastructure and are motivated primarily by profit and power. They are not necessarily always of Western origin, but this does represent a majority of corporations.

2) *Data and Big Data analysis are the tools which facilitate and enable data colonialism* (Kwet, 2019). During historical colonialism, raw materials were seen as resources to be extracted; data constitutes this raw material within data colonial theory.

3) *Profit and power remain the motivation.* The extraction and manipulation of personal data for profit drives and fuels data colonialism. This results in corporations providing limited or no investment back into the country where they operate (Nyabola, 2018c, 200).

These fundamentals provide a helpful framework for identifying cases of potential data colonialism and a baseline to judge such interactions. I will now address how this theoretical concept links to election interference by non-state IOAs.

The most straightforward connection between the two is that non-state IOAs, specifically political consulting firms, are some of the corporations considered principal actors in data colonial practices. In this research, non-state IOAs are defined as actors not tied to a specific state but with significant political influence that conduct campaigns dedicated to obtaining decisive advantages in the information environment. Political consulting firms and Big Tech

corporations are considered part of this categorisation. In their framework, Hendricks et al. (2018) outline four principal actors of data colonialism. They argue that advertising and consulting firms that use technology to target groups with personalised advertisements are the second main actor involved (Hendricks et al., 2018). Social Media companies such as Facebook and Twitter and political consulting firms like Cambridge Analytica play a central role in the contemporary information sphere, offering a range of commercial marketing tools that can be used for political influence operations (Bond, 2017). In this view, political consulting firms are seen as participants in data colonial practices; they are the creators, users and distributors of data analysis marketing techniques that allow for the manipulation of information online.

The second fundamental of data colonialism is that data is the central means of its existence. This is comparable to how data fuels political consulting practices, enabling microtargeting and profiling to spread political advertisements and disinformation. In the literature review, I discussed the notion that social media is aiding the rapid spread of disinformation. This has been aggravated by the Analytics Turn, which has resulted in an increased use of digital marketing techniques within political campaigning (Chadwick and Stromer-Galley, 2016). All of these advancements can be attributed to the rise in the importance of data in our daily lives. Without obtaining vast collections of personal data, political consulting firms would be unable to target advertisements so effectively; without data, these techniques would cease to exist.

Microtargeting is used to increase the efficiency of targeted political advertisements and campaigns and ultimately increase overall profits from such endeavours. This links to the third tenant of data colonialism; it is motivated by profit and power maximisation with little consideration for the consequences. Evidence has suggested that Cambridge Analytica viewed its involvement in some Kenyan and Nigerian elections as a test for its tactics that could be exported to even more lucrative markets (Cadwalladr, 2018a). This aligns with the data colonialism concept that it is a form of foreign exploitation for profit and power without local investment or regard for domestic consequences (Nyabola, 2018c).

As identified in the literature review, there currently exists a gap in the literature between scholarly explorations into data colonialism and empirical studies of political campaigning by non-state IOAs. By filling this gap, we can develop a better understanding of this phenomenon and further both theoretical development and potential response creation. This section has outlined key concepts in a framework that guides the overall research. By simplifying the theory of data colonialism, we can see how it relates to the actions of non-state IOAs in political campaigning. This outline will help inform the research design and methodology described in the subsequent paragraphs.

3.2. Methodology

Having discussed the conceptual framework and theoretical underpinnings of this dissertation, the following section will outline the fundamental research beliefs of this work and the methodology that will be used to answer the research question; how does the involvement of non-state information operations actors influence elections in the Global South? A qualitative case study approach involving a thematic analysis will be used to investigate this.

3.2.1. Ontology and Epistemology

Before any research can be undertaken, the researcher must be clear on the ontological and epistemological beliefs that inform their approach. Methodology, ontology, and epistemology are essential for establishing why, how and for what purpose research is undertaken (Lamont, 2015, 24). Ontology is the study of being or the nature of social entities (Lamont 2015, 25). It refers to what exists in the human world that we can acquire knowledge about, whether there is only one true reality or multiple experiences of this. Epistemology, on the other hand, investigates what knowledge we should acquire and how knowledge is produced (Lamont 2015, 25). It questions whether there is an objective 'truth' or if knowledge is produced by how we engage with the world. This research will follow the interpretivist or constructivist approach to research. This is a reflexive approach that rejects the application of natural science methods to the social world and instead investigates ideas, beliefs and norms that underlie international politics (Lamont, 2015, 18). Ontologically

speaking, this is the belief that there are multiple interpretations of reality that are informed by personal experience. Epistemologically, it means that knowledge is constructed by the researcher and is steeped in this researcher's personal experiences, histories, and values. Interpretivists argue that the researcher and the research subject are mutually constituted through intersubjective understanding. Thus, the object of research does not have its own existence outside of this relationship (Klotz and Lynch, 2007, 12). Burr (1995) lists four premises of social constructivist approaches that will be kept in mind throughout this research:

1) *A critical approach to taken-for-granted knowledge.* Our knowledge of the world should not be taken as objective truth. Reality is a product of how we categorise the world.

2) *Historical and cultural specificity.* How we understand the world is historically and culturally specific and contingent.

3) *The link between knowledge and social processes.* Our ways of understanding the world are created and maintained by social processes (Burr, 1995, 4; Gergen, 1985, 268).

4) *The link between knowledge and social action.* Different social understandings of the world lead to different social actions; the construction of knowledge has social consequences.

These four premises will be essential for guiding this interpretivist approach. When taking a decolonial stance, it is important to be reflexive about where ideas, concepts and thoughts arise. Thus, it is important to acknowledge that the researcher approaches their work with a perspective informed by their life experience.

3.2.2. A Qualitative Thematic Analysis

A qualitative methodology is employed in this study. Qualitative methods refer broadly to data collection and analysis strategies that rely upon the collection and analysis of non-numerical data (Lamont, 2015, 78). They require us to focus on the meanings and processes that make up international politics (Lamont,

2015, 78). Qualitative methods offer an effective way of collecting in-depth information on a specific topic from a relatively small number of cases (Burnham, Lutz, Grant and Layton-Henry, 2008, 40). A singular case study will be used as this allows researchers to focus on a single research area and study this in-depth over an extended period (Burnham et al., 2008, 64; Gerring, 2004, 348). Furthermore, this approach allows a relatively complete account of the phenomenon, enabling the researcher to argue convincingly about relationships between variables and causal explanations for events and processes (Burnham et al., 2008, 66). These explanations are limited to the particular case; nevertheless, a wealth of information is collected which is specific to this (Burnham et al., 2008, 66). Adding to this, to have a broader impact, a robust theoretical dimension must be incorporated into the research design (Burnham et al., 2008, 64). Here, data colonial theory is used to guide the analysis to ensure a detailed and rich investigation occurs. This methodological approach was instrumental in this research, where instances of election interference are unique and individualised, and thus generalisations are difficult to make. Such complex cases require and deserve an in-depth investigation to understand them further.

This dissertation utilised thematic analysis of a single case study to explore the research question. Thematic analysis was chosen because it is a qualitative method that can be widely used across a range of epistemologies and questions (Nowell, Norris, White and Moules, 2017). According to Braun and Clarke (2006), thematic analysis is a method for identifying, analysing, organising, and reporting themes found within collected data via data coding. One advantage of thematic analysis is that it is theoretically flexible, allowing it to work cohesively with the research's conceptual framework.

Braun and Clarke (2006) and Nowell et al. (2017) set out six phases of thematic analysis. These six phases cover the entirety of the process, giving a detailed account of how the investigation should be carried out. Phase one involves familiarising oneself with the data through initial readings of the data set. In phase two, the researcher must begin to generate initial codes, moving from unstructured data to the development of ideas about themes and issues (Morse and Richards, 2002). Boyatzis (1998) suggests that a 'good code' captures the

qualitative richness of the phenomenon. Phase three relates to this, requiring the search for themes, defined as "an abstract entity that brings meaning and identity to a recurrent experience and its variant manifestations" (DeSantis and Ugarriza, 2000, 362). Following this, the researcher reviews these themes in phase four to understand if they create a coherent pattern (Braun and Clarke, 2006). At the end of this stage, the research should have a good idea of the different themes, how they relate to each other and the overall story this tells (Braun and Clarke, 2006). The penultimate phase involves defining and naming the finalised themes. In this stage, a detailed analysis of each theme will be written, identifying a story for each (Braun and Clarke, 2006). Finally, phase 6 is the production of the final report. This begins once the researcher has established the themes and is ready to start the final analysis (Braun and Clarke, 2006). In this final phase, the researcher should aim to articulate what each theme means as well as the assumptions that underpin them and the implications of this (Braun and Clarke, 2006).

This study used one case across two time periods, the 2013 and 2017 Kenyan Presidential Elections, to investigate how non-state IOAs use targeted disinformation in election campaigns in the Global South. The events of these two elections were widely reported, becoming the subject of multiple journalistic and governmental investigations. These include whistle-blower statements, eyewitness accounts, and examples of disinformation used at the time. The most prominent of these investigations is The Guardian's 'The Cambridge Analytica Files', a yearlong investigation into Facebook, data and influencing elections (n.d.), and a series of investigative reports by Channel 4 News titled 'Data, Democracy and Dirty Tricks' (2018). Evidence from these two sources was used in conjunction with newspaper articles from the time. These were analysed to identify common themes and sentiments used throughout the period. This helped to show what kind of manipulation was used by these firms during the elections so that a broader understanding of their operating practices could be gained.

NVivo 12 is a qualitative data analysis software that allows researchers to store, analyse and visualise qualitative data (NVivo, 2022). For this reason, it was

chosen to assist in the analysis of the data collected. With this software, a multitude of data sources could be analysed by coding 'nodes'. These nodes helped highlight themes throughout the dataset, ultimately helping to find observations and patterns (NVivo, 2022). Following the above structure, laid out by Braun and Clarke (2006), initial nodes were formed via data familiarisation, followed by a process of review and adjustment, until themes were considered finalised. NVivo allows the researcher to count how many references within each node exist; this was the primary analysis function used in this research. This enabled inferences to be made as to the commonality of a specific theme within a broader category.

The data set included thirty-six newspaper articles, eight investigative reports and two web pages. These were chosen primarily due to their relevance to the topic, in content and temporality. The newspaper reports were predominantly part of The Guardian and Channel 4's investigative series; additional newspaper sources from both election periods were included to supplement these. Care was taken to include sources from 'The Daily Nation' and 'The Star', two of the most popular Kenyan news sites, to portray local sentiments accurately. Investigative reports included key evidence from the UK Parliament's Digital, Culture, Media, and Sport Committee, which took a lead role in investigating the Cambridge Analytica scandal and further investigations by prominent non-governmental organisations. These were chosen because of their prominence to the case and valuable insider information, such as eyewitness testimonies and evidence they could provide. Finally, the two web pages included in the analysis were screen captures of one political consulting firm, BTP Advisers' website. These were included as they offered direct insight into the case, describing the organisation's work in Kenya.

From this data set, five parent nodes were created, considered to be categories of investigation. These five categorisations contained multiple sub-nodes that reflected themes found within the data that related to their parent node; the final node structure is depicted below in Figure One. Items were coded into a sub-node due to their perceived relevance to a particular theme; this occurred during multiple read-throughs of each data source. Data could be coded into more than

one node at a time, and in this research, there was an overlap between specific themes and issues that arose. It is important to note here that in the production of the final analysis, it was decided that the 'Relationships' node would be included in the 'Case History' section rather than having its own. It was felt that the conclusions made from this analysis would be better suited to the initial explanatory section, allowing the reader an overview of the key players in the Kenyan elections and the relationship between them before moving on to the main analysis.
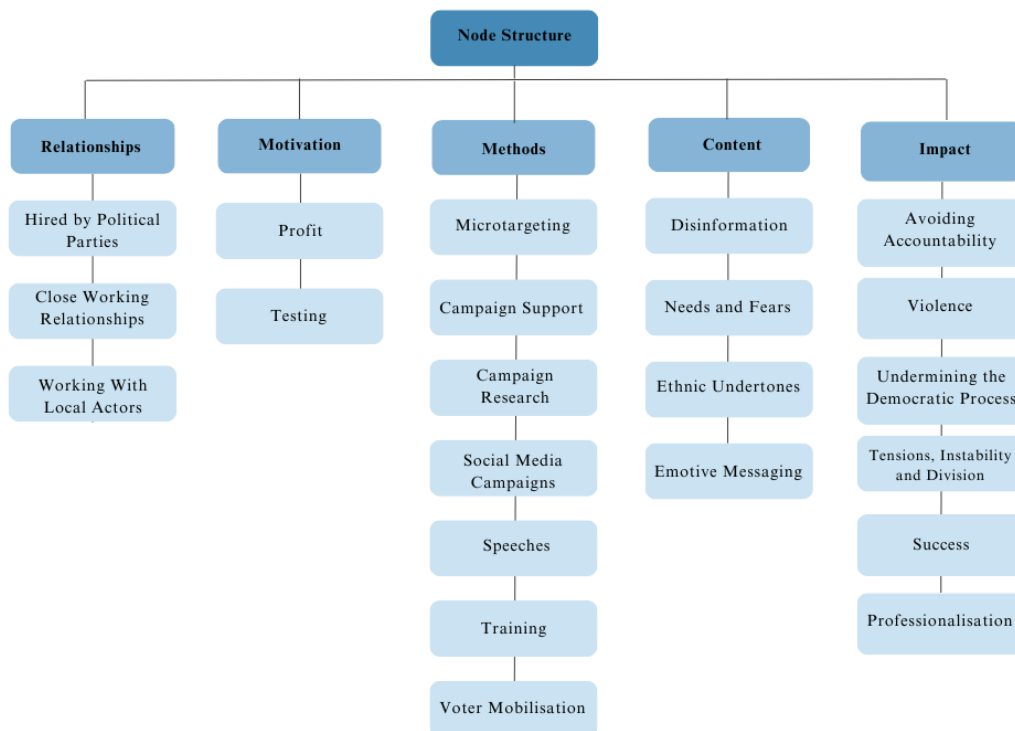
Figure 1. Node Structure of the Thematic Analysis

3.2.3. Limitations, Reliability and Justifications

Whilst all care has been taken to ensure this research design can fully answer the research question, it is acknowledged that this is not possible without flaws and limitations. Whilst this single case will attempt to explain the features of this phenomenon, a cautious approach must be taken. Single-case research design often falls short in its representativeness of a more extensive set of cases and thus cannot be wholly generalised (Gerring, 2014, 348). Particularly in this context where digital election interference often occurs via multiple actors in multiple ways and, thus, each case is slightly different. Further, one key

methodological challenge of thematic analysis is its abstract and interpretative approach which proves challenging for analytical credibility (Graneheim, Lindgren, and Lundman, 2017). Whilst the flexibility of thematic analysis is beneficial, this flexibility can lead to inconsistency and a lack of coherence when developing themes (Holloway and Todres, 2003). These limitations were taken into consideration when conducting the analysis. It does not aim to generalise findings about this phenomenon, only to provide a deeper understanding of the specific case and help to link theory to empirical data. Further, the inclusion of the six phases of thematic analysis (Braun and Clarke, 2006; Nowell et al., 2017) were used to bring a degree of rigidity to the research design, reducing inconsistencies and lack of coherence.

Another source of uncertainty is the covert nature of such operations and the consequent difficulty in collecting sufficient data on them. It is acknowledged that the chosen case occurred five years ago, limiting the newness of the sources. However, due to this covert nature, finding suitable evidence from more recent examples would be difficult. This case was, therefore, selected due to its public nature and availability of information. Further, primary source collection directly from social media sources was not possible with the available resources and time limitations. Thus, the research relies on those pre-collected by investigative journalists in the sources mentioned above. This resulted in a small data set. Nevertheless, White and Marsh (2006) argue that the size of qualitative data sets will always be limited due to the qualitative approach's unique investigation of data which is carried out with more nuance. The sample in a qualitative research design must be purposeful in the researcher's intention of analysing a phenomenon and thus is not required to meet a minimum threshold if the question can be adequately addressed with what is available (White and Marsh, 2006, 35). Therefore, this should not diminish the study's usefulness, but further investigation could benefit from primary source collection.

The overall value of this approach is that a rigorous thematic analysis can produce trustworthy and insightful findings (Braun and Clarke, 2006). Because of its theoretical freedom, a thematic analysis-based research design provides a highly flexible approach that can be modified for the needs of the particular

study, providing a complex and detailed account of data (Braun & Clarke, 2006; King, 2004). It, notably, allowed for the rich and detailed analysis of themes combined with a theoretical framework that evaluates this issue's social, political, and historical background.

4. A Thematic Analysis of the Work of Political Consulting Firms in the 2013 and 2017 Kenyan Presidential Elections

4.1. Case History

The Kenyan political landscape is complex, marred by a long history of authoritarianism and malfunctioning democracy. The 2013 and 2017 elections were an opportunity for the country to take considerable steps towards a peaceful democratic transition. The 2013 Kenyan Presidential Election was a battle between Uhuru Kenyatta of the National Alliance and Raila Odinga of the Orange Democratic Movement (ODM). In 2013 Kenyatta won the election with just over 50% of the vote share. The 2017 election was between now President Uhuru Kenyatta for the Jubilee Party and Raila Odinga for the ODM. This election was controversial, with the Kenyan Supreme Court denouncing the August results and calling for a re-run in October, where Kenyatta won with over 98% of the vote. Turnout during this re-run was exceptionally low, with only 38% of the population participating and Raila Odinga refusing to partake because he felt the re-run was rigged. Both elections were highly competitive, surrounded by energetic political discourse online and in person.

There has been a proliferation of social media usage for political discourse in Kenya. In 2013 politics was paid far greater attention on the Internet than previously; this reached its peak in 2017 (Nyabola, 2019). Since 2013, digital tools have been extensively used in Kenyan politics as major political parties spend considerable amounts on foreign PR and IT consultants attempting to win more votes (Imende, 2017; Nyabola, 2018c). The high internet and social media penetration experienced by Kenya fuels this investment into the digital campaign strategy. Kenyans are some of Africa's most active social media users (Bright, 2017). In 2017, 67% of Kenyans were internet users, compared to the average of 18% in Africa (Crabtree, 2018). Mobile phone users rose from 8 million in 2007 to 30 million in 2013, and the number of Facebook users grew from 4 million in 2013 to 7 million in 2017 (Bright, 2017; Crabtree, 2018). It is clear from these figures that in 2013 and 2017, Kenya had a considerable online

sphere, with many citizens having access to social media in some form or another. It is widely agreed that social media now plays a crucial role in Kenya's political discourse, fundamentally changing how citizens communicate and share information about politics. This rapidly evolving and increasing use of social media has made Kenya a fertile environment for online political campaigning, opening the door for non-state IOAs to conduct interference during election periods.

In 2013, two main non-state IOAs were operating in Kenya, Cambridge Analytica and BTP Advisers. Both were hired to work for the Kenyatta campaign. In 2017, the political consulting firms operating in Kenya expanded. There was Cambridge Analytica, Aggregate IQ/SCL Elections, Harris Media Ltd., and Aristotle Inc.; all but Aristotle Inc., employed for the Raila campaign, worked for Kenyatta and the Jubilee party. This list only includes those revealed to be operating in Kenya at the time, there may have been others working covertly, but this is difficult to ascertain.

Part of the analysis mapped the relationships between the critical actors in these campaigns. It found that, generally, these firms were hired by interested political parties who held close working relations with them. Additionally, there were close links between firms operating in the region and with local actors. Employees of Cambridge Analytica and BTP Advisers reportedly had access to the campaign's website, direct links to key personnel, and were given offices in the Jubilee Party Headquarters in 2017 (Githae, 2019; Imende, 2017; Miriello, Gilbert and Steers, 2018). This information adds an important contextual layer to the analysis; non-state IOAs are often invited to assist in election campaigning by concerned political actors. They are given access to local knowledge about customs and language that is indispensable in complex socio-political environments such as Kenya.

This thematic analysis will examine the 2013 and 2017 Kenyan elections, using newspaper articles, publications, and investigative reports from these periods to answer the research question. The following section will discuss the results of the thematic analysis, which will focus on four key areas: motivation, methods,

content, and consequences. This will be followed by a discussion that will tie the analysis to data colonialism, showing how this theoretical view can allow us to analyse and critique the actions of non-state IOAs in interfering in foreign elections. Whilst data colonial theory is a current that runs throughout this section, the final part will allow for the full exploration of its applicability here.

4.2. Motivation of Non-State IOAs in the 2013/17 Kenyan Elections

Table 1. Thematic Analysis of the Motives Behind the Involvement of Non-State IOAs in the 2013 and 2017 Kenyan Presidential Elections

Node Name	Number of References
Motivation	62
Profit	42
Testing	20

The analysis found that, regarding motivation, themes of testing and profit recurred throughout the dataset. Within the data, profit was a considerable driver for why firms undertook political consulting work in Kenya during 2013 and 2017, with 42 references compared to 20. A standard view amongst the sources was that a high level of money is available in Kenyan politics, particularly from political parties looking to secure an advantage in the electoral race. On average, a Kenyan presidential candidate spends $5 million on their campaign (Nyabola, 2018a). Thus, Kenya is a highly lucrative market for prospective political consulting firms wanting to profit relatively quickly. There is no published evidence on the cost of Cambridge Analytica's work in the 2013 election, but it was widely reported that in 2017, the company was paid $6 million for their three-month project there (Privacy International, 2017a). Alongside this, political consultant and British MP Alexandra Philips was revealed to have been secretly working for Kenyatta on a contract of £300,000 per month (Nation Team, 2019). The 2017 election was one of the most expensive in African history (Nyabola, 2018a). These figures are backed up by anecdotal evidence from ex-employees who commented that, "They'll work for pretty much anyone who pays" (Cadwalladr, 2018b) and "They care about their business…they care about their bottom line" (Channel 4 News, 2018). From this data, we can see

that profit was a clear motivation for firms' involvement in the Kenyan elections, with the companies being offered considerably large amounts of money to aid the campaign.

Further analysis revealed another motivation for non-state IOAs interfering in elections, testing. Operating in Kenya allowed political consulting firms to refine their techniques before taking them to 'more significant' elections. Cambridge Analytica's work in Kenya in 2013 was one of the earliest examples of a non-state IOA working as a political consultancy to help a foreign politician win their election. They advertised this success on their website, boasting of their achievement in securing Kenyatta's victory (Cambridge Analytica, n.d.). Evidence provided by whistle-blowers highlighted why the company was undertaking election work before 2016, "Everything the company did after the Mercers got involved was about refining a set of techniques that they would go on to use in the US elections" (Cadwalladr, 2018a). This excerpt refers to the Mercer family, wealthy Americans with ties to the Republican Party who invested in Cambridge Analytica to develop influence capabilities that could be used in the US. Through experience, the company was, therefore, able to continuously develop data harvesting and weaponisation techniques (Cadwalladr, 2018a). Researchers have pointed out similarities between initial tactics used in Kenya in 2013 and those used in the 2016 Trump and Brexit campaigns; "Many of the same characters, some of the same tactics…a campaign that now seems eerily prefigure to what happened in the US" (Cadwalladr, 2018a). These findings may further indicate the incentive to test data mining and profiling procedures in an environment where elections face much less publicity and scrutiny than in the West.

The data suggest Kenya was considered an ideal testing ground due to its high internet and social media penetration and a lack of data protection regulation. This allowed non-state IOAs to operate with relative freedom, testing microtargeting, data manipulation and campaign strategies. One ex-employee told The Guardian, "We were just doing it to win elections in the kind of developing countries that don't have many rules," and that they would fly around the world, working with presidents, getting "to do all sorts of crazy sh*t"

(Cadwalladr, 2017). These findings are particularly troubling, highlighting the ability of non-state IOAs to operate relatively free of scrutiny in Kenya with a lack of concern for the consequences.

Together these results suggest that profit and testing were substantial motives for firms involved in these elections. In this case, political consulting firms were offered large sums of money to work for short periods of time in Kenya. They were able to use this work to test and refine their techniques, ensuring that they would become the most influential actors with the most cutting-edge technological processes in the political consulting market.

4.3. Methods used by Non-State IOAs in the 2013/17 Kenyan Elections

Table 2. Thematic Analysis of the Methods Used by Non-State IOAs in the 2013 and 2017 Kenyan Presidential Elections

Node Name	Number of References
Methods	185
Microtargeting	97
Campaign Support	34
Campaign Research	25
Surveys	15
Social Media Campaigns	14
Positive and Negative Advertisements	40
Image and Messaging	25
Speeches	8
Training	4
Voter mobilisation	3

The thematic analysis found that non-state IOAs used multiple methods to influence the 2013 and 2017 Kenyan elections. Seven fundamental techniques were discovered: campaign research, campaign support, microtargeting, social media campaigns, speeches, training, and voter mobilisation. Ex-Managing Director of Cambridge Analytica, Mark Turnbull, highlights this, stating,

> We have rebranded the entire party twice, written their manifesto, done two rounds of 50,000 surveys and then we'd write all the speeches and stage the whole thing so just about every element of his campaign (Channel 4 News, 2018).

This shows the widespread nature of political consulting firms' role in elections and the interlinked nature of their methodology. This analysis is supported by evidence found on the BTP Advisers website that, in 2013, they helped establish and manage a modern political campaign machine, offering both strategic campaign advice and hands-on, day-to-day support (BTP Advisers, n.d.). According to an ex-employee, this type of campaigning was the company's "bread and butter" (Cadwalladr, 2018a). It could be inferred from this, therefore, that these methods are most commonly used during election interference by non-state IOAs and that they are often heavily involved in the election process.

First, the political consulting firms would conduct campaign research. For Cambridge Analytica, this involved what it describes as "the largest political research project ever conducted in East Africa" (Crabtree, 2018). They surveyed over 47,000 Kenyans in 2013, allowing them "to do all the data, all the analytics, all the targeting" (The Guardian, 2018). This allowed the company to create a profile of the Kenyan electorate. Cambridge Analytica used OCEAN psychological analysis to identify issues people might support and how to best position arguments to them (DCMS Committee, 2018). Working at the same time was BTP Advisers, who, according to their website, monitored media, especially social media, with an interest in gathering information on Raila Odinga (BTP Advisers, n.d.). This research allowed the firms to identify issues that resonated most with each voter group, allowing them to assess voting behaviour and how citizens consumed political information (Nyabola, 2018a). This gave the campaign a considerable advantage when designing its communication strategy. With the data gathered, the companies could use microtargeting to implement their social media campaigns, allowing them to operate effectively, targeting emotive advertisements to the right people to gain support.

The firms would use the information gathered to create their social media campaigns. These would focus on changing image perception via messaging, using a mix of positive and negative advertisements to do so. In 2013 and 2017, the focal point was an online social media campaign to generate a substantial active following (Nyabola, 2018a). In 2013 specifically, this was aimed at mobilising the younger generation of voters. Cambridge Analytica's work highlighted that the Kenyan youth were an underutilised party asset that could be highly influential if mobilised (Cambridge Analytica, n.d.).

In 2013, BTP Advisers conducted work on image perception, developing a "compelling political narrative that would allow Kenyatta to build an electoral majority" (BTP Advisers, n.d.). This meant centring the narrative around the ongoing International Criminal Court (ICC) controversy, which saw Kenyatta under investigation for inciting violence in the 2007 elections. BTP aimed to deflect adverse reports arising from the ICC process and play up issues that favoured Kenyatta (Mathenge, 2013). This PR spin portrayed Kenyatta as a victim of a Western plot to persecute African politicians (Nyabola, 2018c). This involved using what has been described as "aggressive propaganda tactics" that cast the ICC as racist and supporters of the process as "puppets of the West" (Warah, 2019). BTP Advisers ultimately helped to develop a set of messages that turned Kenyatta's image around, allowing him to be elected whilst under scrutiny by the international community.

These tactics were again used in 2017 when attention turned to the reputation of opposition candidate Odinga. This time the focus was on giving Kenyatta a more youthful and technocratic image, whereas Odinga was portrayed as a "dangerous, racist, xenophobe" (Mathenge, 2013; Privacy International, 2017a). This occurred through a mixture of positive and negative advertising. "Uhuru for US" was a site showcasing President Kenyatta's achievements, illustrated in Figure Two. This was used to target searches where positive praise for Kenyatta could occur. However, as has been widely researched, the algorithm generally prioritises negative stories (DCMS Committee, 2019). And thus, attack advertisements, such as "The Real Raila", similar to those used in the US in 2016, were utilised in the 2017 election. The Real Raila advertisement

relied on Google ad words and targeted advertising on various social media platforms (Privacy International, 2018). For instance, paid ads for the campaign emerged above Google search results for election-related queries, such as "Kenyan election date" (Privacy International, 2018). This can be seen in Figure Two, which depicts four instances of ad targeting online during the 2017 election.
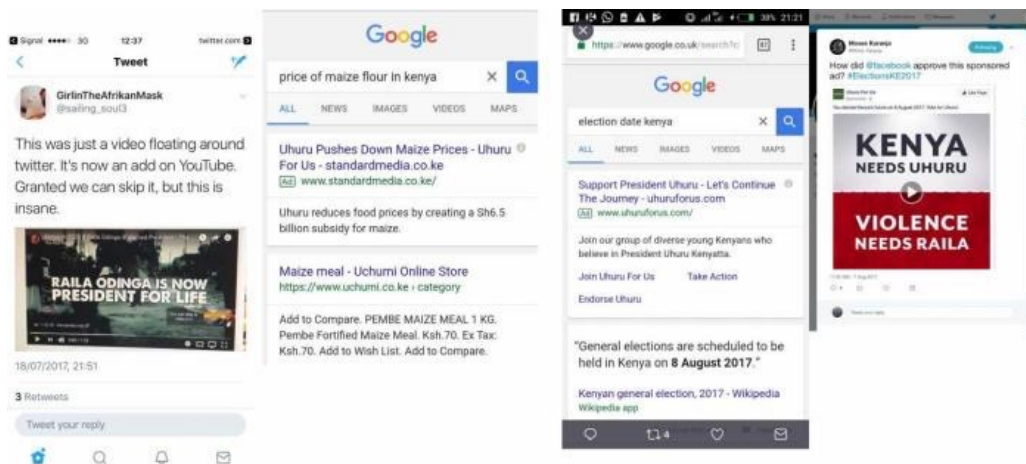
Figure 2. Examples of Targeted Online Advertisements During the 2017 Kenyan Presidential Election. Source: Privacy International (2018)

These findings reveal valuable insight into the nature of the work conducted by non-state IOAs in elections. Firms in both the 2013 and 2017 elections were heavily involved in all aspects of campaign support. They conducted campaign research in the form of surveys, which informed the creation of social media campaigns that targeted negative and positive advertisements to influence the image of specific candidates and, ultimately, mobilise certain voters. Alongside this, firms would write Kenyatta's speeches and train Kenyan staff to operate using such techniques. This complex methodology allowed the companies to target individuals who could be persuaded to vote a certain way. These findings thus identify seven key methods political consulting firms use to interfere in elections, highlighting their interlinked nature and the level of sophistication needed to undergo such work.

4.4. Content of Online Political Campaigns during the 2013/17 Kenyan Elections

Table 3. Thematic Analysis of the Online Content Shared by Political Campaigns During the 2013 and 2017 Kenyan Presidential Elections

Node Name	Number of References
Content	119
Disinformation	59
Needs and Fears	23
Ethnic undertones	21
Emotive Messaging	16

The next section of the investigation is related to the content of these campaigns. The analysis found four key areas: disinformation, needs and fears, ethnic undertones, and emotive messaging. A note of caution is due here since these categorisations are mainly dependent on the availability of evidence; there may have been more advertisements, no longer viewable, that could alter the dataset.

One of the key themes in the available content was emotive messaging. Turnbull states, "It's no good fighting an election on the facts because it's actually just about emotion" (Nyabola, 2018a). The 2013 campaign against the ICC did just this; it used emotive language referencing Western imperialism to persuade voters to vote for Kenyatta. It framed the election as a choice between political autonomy or Western control, playing on people's fears of Western subjugation. This emotive content relates to the second theme within the data, needs and fears. According to Cambridge Analytica, political research allowed them to identify the Kenyan electorate's needs and fears, which were jobs and tribal violence, respectively (Cambridge Analytica, n.d.). The campaign thus ran on a deliberate narrative of fear, playing on Kenya's violent past and concerns for future violence (Miriello et al., 2018). Fake polls and other manipulated content, which often tapped into ethnic or other grievances, were prevalent in the 2017 election (McKay, 2022). According to whistle-blower Christopher Wylie, this type of emotionally charged content was what companies like Cambridge Analytica were built on (Channel 4 News, 2018).

The following paragraphs will focus specifically on an example of this emotive content. The Real Raila advertisement sought to discredit the opposition by harnessing people's fears of violence and ethnic tension. This campaign, run by US firm Harris Media Ltd., argued that a vote for the opposition would lead Kenya to an apocalypse (Nyabola, 2018a). The video, which has 144k views on YouTube, runs like a film trailer, setting the scene in 2020, three years into an imaginary Odinga presidency. Slogans describing how Odinga has negatively impacted Kenya flash across the screen in front of black-and-white imagery of impoverished citizens, dirty streets, and outbreaks of violence. The video implies that Odinga would revoke the constitution, becoming a president for life. It then invokes images of violence under a Raila Presidency, suggesting that this violence will give way to martial law and that "whole tribes and communities are removed from their homes." This could be viewed as a reference to the fear of tribal violence identified by Cambridge Analytica.
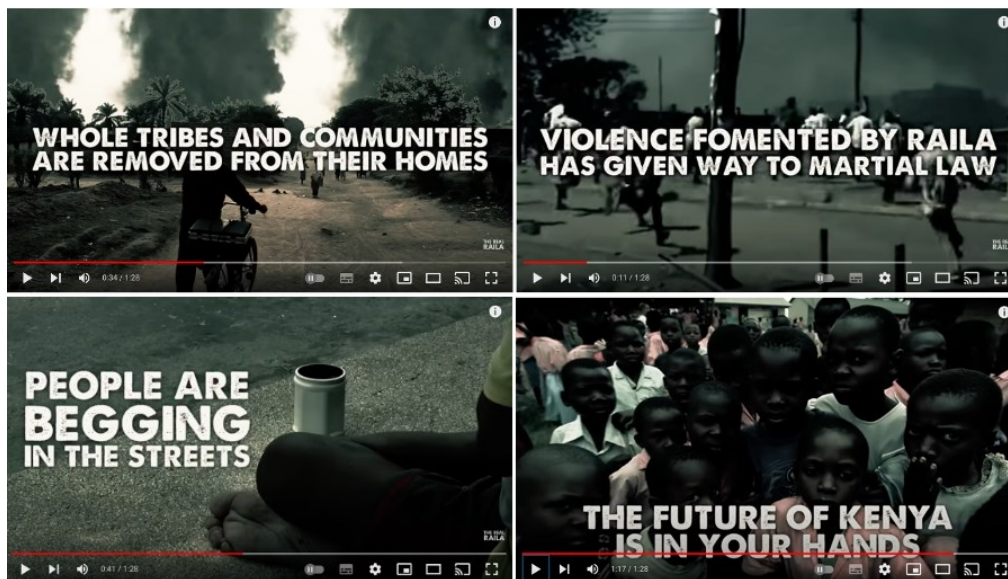
Figure 3. Screenshots from "Kenya in 2020 if Raila Odinga is elected President | The Real Raila" (2017). Source: YouTube

The advertisement then depicts the economic downfall that Kenya would experience under Odinga, with images of abandoned schools, crumbling infrastructure and people begging on the streets. This relates to the identified needs of Kenyan citizens, jobs, with the implication that under Odinga, everyone will become poorer and less economically secure. Finally, the video

ends with the phrase, "The future of Kenya is in your hands." This sentiment is similar to that of BTP Adviser's 2013 election campaign, which focused on taking back control from Western imperialism. Both campaigns rely on emotional imagery and powerful slogans on top of distressing images of Kenya to invoke a mix of patriotism and fear, persuading viewers to protect their country by voting for Kenyatta.

These findings are even more worrying when analysed in context with the final category of content found, ethnic undertones. Throughout the online political campaigns, there were ethnic and tribal undertones that had the potential to spread division. Whilst The Real Raila campaign avoids expressly ethnic references, it contains coded political language which indirectly references ethnicity (Privacy International, 2017a). According to one investigation, the communities who listen to such messages know precisely what is being said (Privacy International, 2017a). Throughout the election period in 2017, there were attempts by political actors online to stereotype one group in particular, the Luo, Odinga's ethnic group, as violent. Thus, advertisements tried to link the main opposition with the Luo community so that rifts between the Luo and Kenyatta's party would deepen further (Wangari, 2017). This type of campaigning has been argued to have promoted and strengthened ethnic divisions throughout Kenya (Madung, 2022; Zimmerman, 2020). In a country where ethnic tensions have resulted in violence and death in the past, playing to these prejudices can have dangerous consequences, as will be discussed in the following section.

This was an election that was run on disinformation which played on people's worst emotions and deepest fears. 90% of Kenyans surveyed suspected of having seen or heard false information regarding the election online (Portland, n.d.). According to the ex-CEO of Cambridge Analytica, "These things don't necessarily need to be true as long as they are believed" (Channel 4 News, 2018). Most striking from this revelation is the lack of concern for fact, highlighting the problematic nature of running campaigns on emotional manipulation rather than objective truth.

4.5. Impact of Online Political Campaigning by Non-State IOAs in the 2013/17 Kenyan Elections

Table 4. Thematic Analysis of the Impact of Involvement of Non-State IOAs in the 2013 and 2017 Kenyan Presidential Elections

Node Name	Number of References
Impact	168
Avoiding Accountability	70
Unethical Behaviour	25
Lack of transparency	20
Violence	38
Undermining the Democratic Process	22
Tension, Instability and Division	22
Success	11
Limits on Success	15
Professionalisation	5

The final area of analysis was the impact of these firms' involvement on the electoral process. It is important to remember here that this study aims to look at the perceived influence of these campaigns and the discourse they promoted. It does not claim direct links between the work of non-state IOAs and the elections' aftermath. Instead, it aims to explore the potential links between the two variables. The analysis yielded six main consequences: avoiding accountability, violence, undermining the democratic process, tension and instability, success and professionalisation.

One consequence of the involvement of political consulting firms in these elections was the professionalisation of the Kenyatta campaign. Five references discussed the improvements made by non-state IOAs on Kenyatta's campaign, arguing that it was more professional, more visible, slicker, and very clean (Mathenge, 2013; Miriello et al., 2018). This supports the idea that non-state IOAs can not only help political parties gain an edge over their opponents but help them get their message across much clearer. This professionalisation is highlighted in the success of Kenyatta's campaigns in 2013 and 2017. In both

elections, Kenyatta and his party secured victory. Kenya is seen as Cambridge Analytica's greatest success story (Nyabola, 2018c) and BTP Advisers boast on their website that they took Kenyatta from 16% in the polls to "outright victory" (BTP Advisers, n.d.). Hiring experienced firms that had conducted such operations previously allowed the Kenyatta campaign the opportunity to streamline its campaign and ultimately gain success. Whether this can directly be attributed to the assistance of political consulting firms is unclear; Kenya is a very complex political terrain where microtargeting may not have as significant an influence as is generally argued (Bright, 2017; Miriri, 2018). In Kenya, traditional media still plays a prominent role in the diffusion of political information, and thus social media campaigning may have less success than boasted (Nyabola, 2018a). It is difficult to attribute the success of an election victory to any specific component. However, it can still be said that these firms did play a prominent role in Kenyatta's campaigns, improving their overall strategy and appearance.

The analysis also found significant negative consequences of the involvement of non-state IOAs in the Kenyan elections. One of the most concerning is the impact on the democratic process. McKay argues that Kenyan elections have suffered considerably over the last decade from domestic and foreign interference (McKay, 2022). Cambridge Analytica has been accused of hijacking Kenya's democracy (Madowo, 2018). Strategies were put in place based on data-mined information, meaning certain groups were favoured in political advertising and others were not. Twenty-two sources referenced the detrimental impact that these firms' involvement had on Kenyan democracy. They highlight the subversion of people's will (BBC News, 2018); the cementation of a culture of impunity (Zimmerman, 2020); skewing political behaviour contributing to one of the most virulent campaigns in Kenyan history (Nyabola, 2019) and undermining faith in the democratic process (Privacy International, 2017a). These statements are reflected in the fact that 35% of people surveyed by Portland felt they were unable to make an informed voting decision (Portland, n.d.). These results present worrying evidence about the impact that interference by non-state IOAs can have on the democratic process, linking to Persily's argument that the power of such campaigns lies in their

ability to demobilise, confuse, and hinder informed political decision-making (2017,69).

The analysis also found that there was an increase in tension, instability, and division. The firms have been accused of sowing divisions that will "take many generations to heal" by exploiting tribal tensions to ensure victory for Kenyatta (Miriello et al., 2018). The 2013 and 2017 elections are considered to be some of the "darkest and most vicious campaigns" in Kenyan history (Madowo, 2018). The prevalence of disinformation spread online, controversial campaigning that aimed to undermine opponents, and biased political information contributed to this. The whole Cambridge Analytica controversy fed into the popular belief amongst Kenyans that the ruling party had mobilised state resources in an attempt to rig the election (Privacy International, 2017b). This will only serve to undermine not only the legitimacy of the state but any future elections. Adding to this, during the controversial 2017 election, when Kenyatta was eventually announced as the winner, a string of protests arose in Nairobi and Kisumu (Nyabola, 2017). Government forces brutally suppressed these in some areas. The days and months surrounding the two elections have been described as tense, as anxious voters waited to discover the outcome amidst the disinformation spread online (Nyabola, 2017). The flawed election disenfranchised many voters; between the nullified August poll and the October rerun, voter turnout dropped from 79% to 38% (Nyabola, 2018b). The DCMS Committee includes a telling quote from those involved with Cambridge Analytica's exploits, discussing how they "created bushfires and then put a big fan on them and made the fan blow" (DCMS Committee, 2019). This suggests the purposeful use of divisive tactics to increase tension during the electoral period. Using methods discussed previously, and content that plays on people's fears and emotions, non-state IOAs can cause considerable instability within online political discourse that can quickly spread into the physical world.

This tension and instability can easily turn into violence if not properly managed, representing the final theme. Both elections were marred with various violent instances that only served to undermine the democratic process further. Kenya has a troubled past with electoral violence; in 2007, over 1,000 people

died after widespread dissatisfaction over the election result erupted into violence (Privacy International, 2017a). This is a point of considerable apprehension for Kenyan citizens who fear the return of such instability. In 2017, violent clashes erupted over accusations of vote rigging. According to the Kenya National Commission on Human Rights, at least 25 people were killed between the 8th and 12th of August (Crabtree, 2018). Later that month, over 100 were injured. From the 1st of September to October 25th, a further 25 people died (Crabtree, 2018). In addition to these public clashes of violence, there were some high-profile killings and kidnappings, including the Independent Electoral and Boundaries Commission's ITC Director and two American and Canadian citizens who were political consultants for the opposition party (Nyabola, 2017, 2018a). In the analysis, violence was the second most referenced impact, presenting a worrying insight into the consequences of sowing division online. Of course, it cannot be directly attributed to the work of political consulting firms, but it is a consideration to be made. Elections in Kenya are already fraught with difficulty and tension, often having difficult pasts with electoral violence. Adding data mining, profiling and disinformation to the mix only serves to exacerbate existing tensions.

The final analysis highlighted one pertinent theme regarding the work that non-state IOAs undertake during elections; these campaigns operate in a shroud of secrecy, allowing them to engage in unethical practices whilst almost always avoiding accountability. Seventy references were made to the secretive nature of such operations, with Channel 4's investigation revealing the extent of this. Executives were filmed stating, "We're used to operating through different vehicles, in the shadows…" and describing how the organisation could set up front companies to conceal the true nature of their work (Channel 4 News, 2018). When asked about this secrecy, Turnbull said, "It has to happen without anyone thinking, 'that's propaganda', because the moment you think that's propaganda, the next question is 'who put that out?'" (Channel 4 News, 2018). This lack of transparency leads to uncertainty and many unanswered questions. No one is certain of what work was undertaken in Kenya, what data was used and how this was obtained. This lack of transparency means that, for both

researchers and policymakers, there is no ability to check what campaigns were undertaken by non-state IOAs (DCMS Committee, 2019). Therefore, limiting how to respond to and mitigate them.

Thus far, the firms involved in 2013 and 2017 have taken no accountability for their actions nor faced retribution. Initially, the involved firms and political parties denied any involvement; this soon evolved into partial acceptance, with a Kenyatta spokesperson stating, "They were basically branding and all that, but not directly" (BBC News, 2018). Cambridge Analytica has continued to deny any wrongdoing and unlawful behaviour throughout the investigations. There has been no investigation into the work these firms conducted in Kenya; those supposed to challenge these things were most likely the ones who directly benefited from the work undertaken (Madowo, 2018). This lack of acceptance, coupled with a lack of transparency, has led to an overall lack of accountability.

5. <u>Connections to Data Colonialism</u>

The previous section has analysed the involvement of non-state IOAs in the 2013 and 2017 Kenyan Presidential Elections through a data colonial framework. It has sought to examine the practices of non-state IOAs in these elections to aid understanding of the broader phenomenon and problematise some of the ways that Big Data analytics have influenced democracy and political practices. This final section will provide an overview of the analysed data with reference to the conceptual framework set out in the introduction, taking a de-colonial view to question the findings.

As put forward in the conceptual framework, there are three fundamental components of data colonialism; the social quantification sector is the principal actor, data and Big Data facilitate and enable data colonialism, and profit and power remain the primary motive. By applying a de-colonial critical lens, these three tenants can be applied to the above analysis of the 2013 and 2017 Kenyan elections.

5.1. The Pursuit of Profit and Power by Political Consulting Firms

The most apparent connection between data colonial practices and the involvement of political consulting firms in Kenya's recent elections is the motivation of profit and power. The third key component of data colonialism mirrors the motivations found in the thematic analysis; testing and profit. The work undertaken by non-state IOAs in these elections earned them considerable amounts of money in relatively short periods of time. As detailed above, companies like Cambridge Analytica were afforded lucrative contracts to orchestrate Kenyatta's political campaign, aiming to gain the maximum economic benefit at a minimal price, similar to historical colonialism (Coleman 2019, 420). Furthermore, their work in Kenya allowed them to test and refine their microtargeting and profiling techniques, as described by an ex-employee in the evidence (Cadwalladr 2018).

This testing was seen mainly in 2013 when the company conducted surveys to obtain data on thousands of Kenyan citizens. Similar research was conducted in the US and UK in 2016 for the Trump and Brexit campaigns. Non-state IOAs used this campaign research to determine which citizens to target; in Kenya, it was youth voters. This was also a method in the Brexit Referendum, found in a proposal by Cambridge Analytica to the 'Leave.EU' campaign (DCMS Committee, n.d.). It shows the varying criteria that could be used to segment and message the population, including priority issues (national security), partisanship and persuadablity.

A similar methodology was also utilised when it came to the use of Google Ad targeting. As was seen in the Kenyan elections, ads were placed under related search queries to bring attention to specific campaigns. This technique was also used in the 2016 Trump campaign, depicted in the image below, taken from a Cambridge Analytica overview of their work on the 2016 US Election (Lewis and Hilder, 2018).
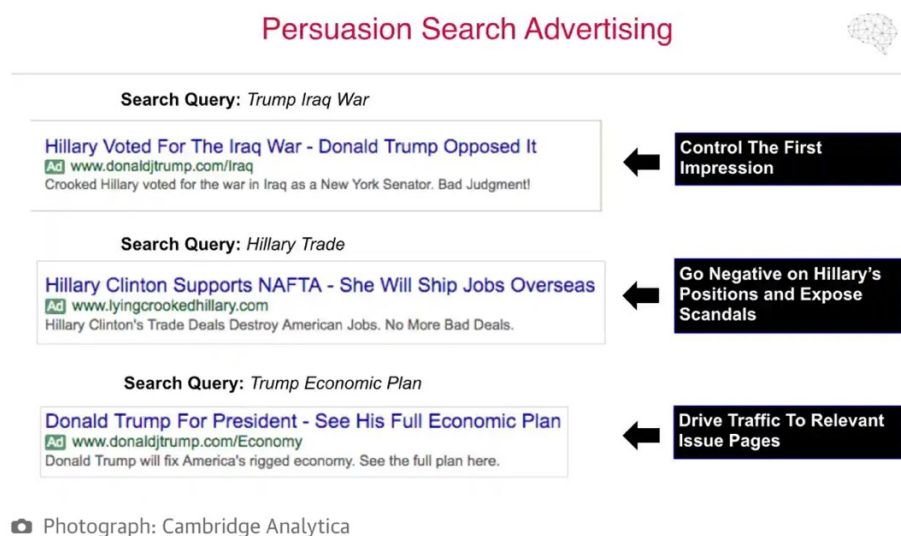
Figure 4. Examples Taken From a Cambridge Analytica Presentation of Targeted Online Advertising in the 2016 US Election. Source: Lewis and Hilder (2018)

This comparison should be interpreted with caution. These techniques could merely be standard methods used by political consulting firms; it does not necessarily imply that data colonialism has taken place. However, it does indicate the kinds of methodology used by non-state IOAs and helps to further

understanding that these firms have a modus operandi, regardless of the state they are operating in.

Corporations played a pivotal role in historic colonialism through the pathological pursuit of profit and power (Kwet, 2019). A similar phenomenon is witnessed here, where political consulting firms are the main perpetrators of extractive and predatory practices in the Global South. As explored in the literature review, data is a new form of currency, wherein access to data is now the most valuable asset available to corporations (Coleman, 2019, 424). Because of this value, it has become extensively commodified, leading to the endless pursuit of 'bigger' data, driven by intense profit-seeking competition within capitalist markets (Thatcher et al., 2016, 992). The principle aim of this extraction is to gain knowledge from data via analysis; to enhance profit-making and efficiency (Thatcher et al., 2016, 992). This process occurs within the extraction itself but also within the aftermath; data is a never-ending source of information for corporations. In this case, data extracted through campaign research was instrumental in informing messaging strategy. However, it also allowed non-state IOAs such as Cambridge Analytica to test and refine their techniques to improve their strategy for future elections. In this sense, corporations can continue maximising profit and gain corporate power by enhancing and refining their techniques.

An extension of data colonialism's profit and power thesis is the lack of investment in the environment where these corporations operate. Similar to previous manifestations of colonialism, data colonialism extracts profit but invests nothing back into the country (Nyabola, 2018a, 200). The focus for non-state IOAs in the 2013 and 2017 elections was on collecting and weaponising data to gain electoral success for a specific candidate. There was little concern for how this would impact the overall democratic process, political dialogue, and societal stability in Kenya. This is particularly troubling when these firms are operating in emerging democracies, where such political stability is tenuous and easily manipulated. Again, this links to profit and power-seeking, where the primary aim of expanding and improving business practices obscures real-world implications.

By involving themselves in high-paying elections, non-state IOAs stand to gain considerable profits and the opportunity to test their methods to further their power in data analytics and political consulting. Wylie has ultimately coined this "post-colonial blowback", describing a situation where, "The West found a way of firehosing disinformation into weak and vulnerable democracies. And now this has been turned back on us" (Cadwalladr, 2018a). This provides an interesting perspective; that data colonial practices impact not just the Global South or the West but everyone.

5.2. Extractive and Predatory Methods of Political Consulting Firms

The three core tenants of data colonialism are also found within the methods used by non-state IOAs in the Kenyan elections. Data was what facilitated these campaigns; firms surveyed and researched the Kenyan population to gain invaluable insight, which allowed them to target advertisements and focus on specific demographics. The analysis found that microtargeting was the key method used by political consulting firms in Kenya, allowing them to utilise various other methods, such as social media campaigns which sought to control image perception through a combination of positive and negative advertising. These methods are inherently extractive and predatory, touched on above and in the literature review. The manipulation of personal data to target specific audiences with specific messaging leads to a degradation of political discourse and understanding (Martin, 2017; Marwick and Lewis, 2017; Persily, 2017). This can be problematised further when addressed in the context of a Global North versus Global South power imbalance, where a Western non-state IOA has used data manipulation techniques to sow discord in a democratically fragile state. A parallel can thus be made between the dimensions of violence and expropriation of historical colonialism and new forms of exploitation that are indicative of political microtargeting practices (Tait, dos Reis Peron and Suárez, 2022, 11).

Throughout both elections, multiple political consulting firms were involved in the campaigns of Kenyan political parties. This finding is consistent with that

of Hendricks et al. (2018), who show that consulting firms are the second principal actor of data colonialism. They also argue that the third main actor is local companies, parties and organisations who pay Western technology companies to work for them (Hendricks et al., 2018). This was seen in the close links held between the firms and political parties that hired them. This presents the argument that political parties and local actors are often complicit in enabling data colonialism in their home country. This adds an important layer to the analysis, allowing for differing levels of agency within data colonialism. Consulting firms and political parties actively work together to influence political discourse, which then impacts principal actor number four, the citizens who unknowingly act as data sources (Hendricks et al. 2018). In this instance, Kenyan politicians were not passive participants in data colonialism but active enablers, and Kenyan citizens were (un)knowing providers of data sources that helped run these campaigns.

The analysis also highlighted the lack of rules in Kenya that made this extraction possible. One ex-employee said, "We were just doing it to win elections in the kind of developing countries that don't have many rules" (Cadwalladr, 2017). Other articles pointed out the lack of data protection regulation, meaning that Kenyan citizens will remain vulnerable to manipulation whilst firms avoid accountability (Ngila and Sheik, 2022; Nyabola, 2019; Tsalikis, 2019). This links to the asymmetrical relationship discussed by Thatcher et al. (2016, 994), who argue that the processes of data extraction and weaponisation create a power imbalance between the data collector and the data creator. All known firms operating in Kenya during 2013 and 2017 were of Western origin, adding to this power imbalance. According to Kwet (2019), in data colonialism, we have a situation where the largest sets of data are dominated by a handful of Western corporations. This was precisely the case in the 2013 and 2017 Kenyan elections, where a handful of Western firms were operating using data only they could access.

5.3. Exploiting Needs and Fears Through Strategic Messaging

As depicted in the analysis, the online political advertising conducted throughout the 2013 and 2017 Kenyan elections focused on four primary areas; disinformation, needs and fears, ethnic undertones, and emotive messaging. All of which combined to create a toxic electoral environment. When viewing these campaigns through a de-colonial lens, we can see aspects of data colonialism throughout. Disinformation reaffirms existing prejudices that reflect current social and political divisions in society (Mutahi and Kimari 2020, 12). This was certainly the case in Kenya, where advertising focused on the needs and fears of the electorate, such as ethnic violence, economic stability, and state sovereignty, playing up political issues with emotive messaging.

The 2013 Kenyan campaign revolved around the rhetoric of 'taking back control' from Western interventionism. Several sources outlined the contradiction of Kenyatta's 2013 campaign, which made a case against neo-colonial interference whilst paying a British company millions of dollars to spread this message (Madowo, 2018; Nyabola, 2018c). BTP Advisers, who conducted this campaign, state on their website, "We made the election a choice about whether Kenyans would decide their own future or have it dictated to them by others" (BTP Advisers, n.d.). The irony of this statement is evident here, with this firm playing a considerable role in manipulating political thought and narrative in the 2013 election.

Interestingly, this was seen again in both the 2016 Brexit and Trump campaigns, which included similar sentiments. In the UK, the Vote Leave Campaign was based around the slogan 'Take Back Control', and in the US, Trump's campaign focused on statements such as 'Make America Great Again' and 'America First'. This is an intriguing similarity, pointing to the emotive language used in such campaigns that play on people's needs and fears, which may not vary drastically from society to society. It further links to the testing aspect of these campaigns, as discussed above.

A significant component of these campaigns was ethnicity. The Real Raila video, although not explicitly, sowed seeds of ethnic unrest, insinuating that a vote for Odinga would result in the oppression of certain groups and the "removal of whole tribes". The exploitation of ethnicity to achieve colonial goals is not a new phenomenon, linking directly back to the historic colonialism of the late 19ᵗʰ century. Colonial rulers created ethnographic states that divided colonised peoples into communal categories to make them controllable (Dirks, 2001; Lange, Jeong and Amasyall, 2021, 481; Mamdani, 2012). Kenya was under British colonial control, which followed a 'divide and rule' system. In this system, the British maintained control by cultivating factional rivalries among different ethnic groups, generally by promoting the minority to governmental positions (Blanton, Mason and Athow, 2001, 480). After decolonisation, this system continued, where the goal of ethnic competition was to maintain control over the state machinery and subsequently avoid marginalisation (Blanton et al., 2001, 481). Ethnicity thus became a mobilising tool in contemporary Kenyan politics, co-opted by politicians to gain support and create rivalries against the opposition. The use of ethnic messaging in the 2013 and 2017 elections could be considered a consequence of historical colonialism, something that has become entrenched in Kenyan political society. This historical tactic of division to gain power has combined with new data practices, advancing the ability to divide even further.

5.4. Unravelling the Consequences: How Data Colonial Practices Impacted Kenyan Democracy

Lastly, the thematic analysis of the impact of online political campaigning in Kenya points to several issues relating to data colonialism. The findings highlighted the impact these interventions had on the overall democratic process, limiting people's access to reliable and trustworthy sources of information. Whilst an active online social sphere can be good for democratic conversation, it can also harm electoral integrity (Maweu, 2019, 66). This integrity depends on a competitive process, credible electoral institutions, and informed participation; strategic deployment of disinformation has been shown to undermine this (Maweu, 2019, 66). Whilst no direct links between these

election campaigns and democratic backslide can be claimed here, it is evident that such campaigning and its perceived effects potentially threaten democracy. Technological expansion into the Global South is often seen as inherently positive, offering better access to services and economic improvement (Young, 2019). One of the purposes of data colonial theory is to problematise this. The analysis shows that despite technological advancement often being seen as an enabler of democracy and free speech, microtargeted political campaigns in Kenya have inhibited this. This further links to the abovementioned argument that data colonial practices extract but offer nothing in return (Nyabola, 2018a). In this case, non-state IOAs were heavily involved in the 2013 and 2017 elections in Kenya and stood to gain considerable profits from this; but put nothing back into the country to the extent that their work there was largely detrimental to democratic stability.

Tensions, instability, and violence were all consequences of online disinformation spread by political campaigns in Kenya during 2013 and 2017. This, combined with a lack of transparency and avoidance of accountability, created a scenario where Western corporations had interfered secretively in a foreign election, facing no consequences. Due to the globalised nature of the online sphere, data mining and profiling is available from anywhere to anywhere, meaning that non-state IOAs can easily operate in another state and avoid any potential consequences for this. A lack of data protection regulation partially fuels the lack of accountability. In Kenya, there is little to no regulation on data practices and no legal mechanism to regulate and control potential malicious non-state IOAs. Because of this, there is nothing in place that safeguards citizens' digital rights, nothing to track what data is used and nothing to stop firms from continuing to do this in the future. This helps to fuel the continuation of data colonial practices. Many also point to the reluctance and inability of the Kenyan government to push data protection regulation through parliament and the lack of understanding of the importance of such protections (Bright, 2017). This highlights the complex nature of this issue and the difficulties faced when trying to tackle data regulation in a society which is so reliant on it. The overall lack of accountability for actions that caused considerable disruption further confirms the inherent power imbalances and

extractive nature of the work conducted by non-state IOAs in Kenya. Ultimately, Nyabola asks, What does accountability for political misinformation look like when a British company uses an American platform to influence political discourse in a Kenyan election?" (Madung, 2022), highlighting the complex and intertwined nature of data colonial practices in contemporary global politics.

6. **Conclusion**

Data derived from our social media is undoubtedly changing how modern life functions, specifically domestic and global politics. The integration of political campaigning with data-driven microtargeting techniques has resulted in a transformation in how elections are run and the skewing of the political sphere. The principal actors in this, political consulting firms, represent a new form of non-state IOAs that now hold considerable influence over the stability of democracy globally.

This dissertation has aimed to answer the research question: how does the involvement of non-state IOAs influence elections in the Global South? It set out to assess the use of disinformation in the 2013 and 2017 Kenyan elections, to develop an understanding of the motivations and methods of non-state IOAs in these campaigns and to explore these findings in relation to data colonialism. It was necessary first to conceptualise the topic at hand, exploring notions of datafication, online disinformation campaigns and theoretical perspectives of data colonialism in the literature review. Next, the methodology and conceptual framework laid out the thematic analysis approach that would be taken to analyse the available data.

The resulting analysis identified central themes within four key areas of investigation, motivations, methods, content, and impact. It found that within each area, a range of significant themes related to the theoretical conceptualisation of data colonialism explored in the literature review and conceptual framework. In these elections, non-state IOAs were primarily motivated by profit and the opportunity to test their methods. This is linked to a key tenant of the data colonial thesis, that profit and power are drivers. During these elections, political consulting firms mainly used data-driven techniques that enabled the operationalisation of targeted online campaigns based on the needs and fears of the Kenyan electorate. The investigation found that these methods, and the content they produced, could be considered predatory and extractive in nature, seeking to sow division and cause tension between

opposing sides. The findings also addressed the influence of such activities on the two election periods, revealing the destabilising nature of such interventions and detrimental effects on the overall democratic process.

Ultimately, the thematic analysis confirmed that by utilising a data colonial lens, the involvement of political consulting firms during elections and the impact of this could be problematised. These findings have significant implications for the understanding of how non-state IOAs operate in the Global South, showing how interactions between Western corporations and local actors remained imbued with power imbalances. Further, this investigation raises important questions about the nature of data-driven political campaigning and the impact of this, not just in the Global South but worldwide.

Research conducted before this study provided a depth of information regarding data, disinformation, and the changing nature of electoral politics. However, this literature was often heavily Western-focused and lacked theoretical exploration. The contribution of this dissertation has been to widen the scope to provide a deeper insight into the impact of datafication in the Global South. The empirical findings provide a new understanding of the impact of data-driven political campaigns by non-state IOAs by investigating the phenomenon through a data-colonial lens. This new perspective will prove helpful in not only expanding the theoretical applications of data colonialism but the overall understanding of how these operations are conducted and their fundamentally destabilising nature on the democratic process.

This dissertation is not without its limitations. The most important of which lies in the fact that the secretive nature of such operations makes them hard to investigate, significantly limiting the available data sources. This necessitated a secondary research approach; further primary research should be undertaken to obtain more data on the specifics of these campaigns. Secondly, the scope of this study was limited to one case study across two temporal periods, impacting the generalisability of the findings. Although this restricts the applicability of the research, the individuality of election interference by non-state IOAs means that these cases are often unique in the first place. Thus, generalisability may

only be possible sometimes. A final limitation of this dissertation lies within its qualitative nature. The thematic analysis, whilst allowing for a deep exploration of the phenomenon at hand, means it was not possible to assess the direct impact of such interventions, instead addressing sentiments and feelings portrayed throughout the data sources. Despite its exploratory nature, this study did offer some insight into the perceived impact of data-driven political campaigns by non-state IOAs, specifically with regard to data colonialism.

This would be a fruitful area for further work. If the debate surrounding data colonialism and political campaigning firms is to be moved forward, further research could usefully explore this phenomenon in other states. There are multiple documented instances of such occurrences in various other places, such as Mexico, St Kitts and Nevis and Romania (DCMS Committee, n.d.). Such investigation would help improve understanding and increase the generalisability of the findings. A greater focus on the relationships between political consulting firms and those who hire them could produce interesting results that account more for the practicalities of data colonialism and how it is perpetrated. In this vein, research on data protection regulations within international law would be an essential next step in addressing the legality of such interferences, something that could not be addressed in the current study.

The findings of this dissertation also have several practical implications. The most significant of these is that greater efforts are needed to protect citizens' data from potential manipulation by non-state IOAs. Governments must ensure that comprehensive data protection regulation is implemented to guarantee that corporations looking to utilise data do not go unregulated and consequently un-punished. Unless governments adopt such policies, non-state IOAs, like the political consulting firms discussed in this dissertation, will continue to harvest and use citizens' data to target and manipulate political messaging. Solid legal frameworks would help address this issue and ultimately protect democratic politics. Continued efforts are also needed to develop the technological capabilities of the Global South so that technological reliance, as perpetrated by data colonialism, does not continue. Having a technical infrastructure built by corporations in the Global South that understands the needs and specificities of

the Global South will be instrumental in ensuring the reduction of online disinformation and, ultimately, the protection of citizens.

7. <u>Bibliography</u>

Allcott, H. and Gentzkow, M. (2017) 'Social Media and Fake News in the 2016 Election,' *Journal of Economic Perspectives,* 31 (2), pp. 211–236.

Allcott, H., Gentzkow, M and Yu, C. (2019) 'Trends in the Diffusion of Misinformation on Social Media,' *Research & Politics,* 6(2), pp. 1–8.

Auchard, E. (2018) 'Cambridge Analytica stage-managed Kenyan president's campaigns: UK TV,' *Reuters*, 19 March. Available at: https://www.reuters.com/article/us-facebook-cambridge-analytica-kenya-idUSKBN1GV300 (Accessed: 8 June 2023).

Avila Pinto, R. (2018) 'Digital sovereignty or digital colonialism?' *SUR*, 27.

Bakir, V. (2020) 'Psychological Operations in Digital Political Campaigns: Assessing Cambridge Analytica's Psychographic Profiling and Targeting,' *Frontiers in Communication,* 5.

Bastos, M.T. and Mercea, D. (2019) 'The Brexit Botnet and User-Generated Hyperpartisan News,' *Social Science Computer Review*, 37(1), pp. 38–54.

Bates, R. H. (2008) *When Things Fell Apart: State Failure in Late-Century Africa*. Cambridge, MA: Harvard University Press.

BBC News (2018) 'Cambridge Analytica's Kenya election role "must be investigated",' *BBC News*, 20 March. Available at: https://www.bbc.co.uk/news/world-africa-43471707 (Accessed 24 July 2023).

Bendiek, A., and Schulze, M. (2019) 'Disinformation and Elections to the European Parliament. SWP Comment,' *Stiftung Wissenschaft und Politik*.

Benkler, Y., Faris, R. and Roberts, H. (2018) *Network Propaganda*. New York: Oxford University Press.

Bennett, W. L., and Livingston, S. (2018) 'The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions,' *European Journal of Communication,* 33 (2), pp. 122–139.

Berghel, H. (2018) 'Malice Domestic: The Cambridge Analytica Dystopia,' *Computer,* 51 (5), pp. 84–89.

Blanton, R., Mason, T.D. and Athow, B. (2001) 'Colonial Style and Post-Colonial Ethnic Conflict in Africa,' *Journal of Peace Research*, 38(4), pp. 473–491.

Bode, L. and Vraga, E.K. (2015) 'In Related News, That Was Wrong: The Correction of Misinformation Through Related Stories Functionality in Social Media,' *Journal of Communication*, 65(4), pp. 619–638.

Bond, R. M., Fariss, C. J., Jones, J. J., Kramer, A. D., Marlow, C., Settle, J. E., and Fowler, J. H. (2012) 'A 61-million-person experiment in social influence and political mobilization,' *Nature*, *489*(7415), pp. 295–298.

Bond, S. (2017) 'Google and Facebook build digital ad duopoly,' *Financial Times,* 14 March. Available at https://www.ft.com/content/30c81d12-08c8-11e7-97d1-5e720a26771b (Accessed 12 June 2023).

Borgesius, F. Z., Möller, J., Kruikemeier, S., Fathaigh, R., Irion, K., Dobber, T., Bodo, B. and de Vreese, C.H. (2018) 'Online Political Microtargeting: Promises and Threats for Democracy,' *Utrecht Law Review,* 14 (1), pp. 82–96.

Boyatzis R. (1998) *Transforming qualitative information: Thematic analysis and code development,* Thousand Oaks, CA: Sage.

Bradshaw, S. and Howard, P.N. (2018) 'The Global Organization of Social Media Disinformation Campaigns,' *Journal of International Affairs,* 71(1.5), pp. 23–32.

Braun, V. and Clarke, V. (2006) 'Using thematic analysis in psychology,' *Qualitative Research in Psychology,* 3, pp. 77–101.

Bright, S. (2017) 'After Trump, "big data" firm Cambridge Analytica is now working in Kenya,' *BBC News*, 3 August.

BTP Advisers (no date) *I believe in Uhuru*, *BTP Advisers*.

Buchan, R. and Tsagourias, N. (2016) 'Special Issue: Non-State Actors and Responsibility in Cyberspace: State Responsibility, Individual Criminal Responsibility and Issues of Evidence,' *Journal of Conflict and Security Law,* 21(3), pp. 377–81.

Bulckaert, N. (2018) 'How France Successfully Countered Russian Interference During the Presidential Election,' *Euractiv.fr*. 17 June.

Burnham, P., Lutz, K.G., Grant, W. and Layton-Henry, Z. (2008) *Research Methods in Politics,* London: Palgrave Macmillan.

Burr, V. (1995) *An Introduction to Social Constructionism,* Taylor & Frances/Routledge.

Cadwalladr, C. (2017) 'The great British Brexit robbery: how our democracy was hijacked,' *The Guardian*, 7 March. Available at: https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robbery-hijacked-democracy (Accessed 24 July 2023)

Cadwalladr, C. (2018a) 'Cambridge Analytica's Ruthless Bid to Sway the Vote in Nigeria,' *The Guardian*, 21 March. Available at: https://www.theguardian.com/uk-news/2018/mar/21/cambridge-analyticas-ruthless-bid-to-sway-the-vote-in-nigeria#:~:text=They%20said%20the%20hackers%20offered,provide%20free%20and%20fair%20elections. (Accessed 24 July 2023)

Cadwalladr, C. (2018b) '"I made Steve Bannon's psychological warfare tool": meet the data war whistleblower,' *The Guardian*, 18 March. Available at: https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump (Accessed 24 July 2023).

Cadwalladr, C. and Graham-Harrison, E. (2018) 'Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach,' *The Guardian*, 17 March. Available at: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (Accessed 24 July 2023).

Cambridge Analytica. (n.d.) 'Case Study: Kenya," *CA Political.*

Canadian Security Intelligence Service. (2017) *Russian World-Views: Domestic Power Play and Foreign Behaviour*. Government of Canada.

Casilli, A. (2017) 'Digital labor studies go global: Towards a digital decolonial turn,' International Journal of Communication, 11, pp. 3934–3954.

Chadwick, A. and Stromer-Galley, J. (2016) 'Digital Media, Power, and Democracy in Parties and Election Campaigns: Party Decline or Party Renewal?' *International Journal of Press/Politics*.

Chambers, S. (2020) 'Truth, Deliberative Democracy, and the Virtues of Accuracy: Is Fake News Destroying the Public Sphere?' *Political Studies,* 69 (1), pp. 147–163.

Channel 4 News. (2018) 'Data, Democracy and Dirty Tricks,' Channel 4 (19 Mar). Available at: https://www.channel4.com/news/data-democracy-and-dirty-tricks-cambridge-analytica-uncovered-investigation-expose. (Accessed 14 June 2023)

Chege, N. (2018) 'Your guide to Cambridge Analytica Kenya election scandal,' *Daily Nation*, 21 March.

Chester, J., and Montgomery, K.C. (2017) 'The Role of Digital Marketing in Political Campaigns,' *Internet Policy Review,* 6 (4), pp. 1–20.

Coleman, D. (2019) 'Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws,' *Michigan Journal of Race & Law*, 24 (2).

Couldry, N. and Mejias, U.A. (2019) 'Data Colonialism: Rethinking Big Data's Relation to the Contemporary Subject,' *Television and New Media,* 20 (4), pp. 336-349.

Couldry, N. and Mejias, U.A. (2023) 'The decolonial turn in data and technology research: what is at stake and where is it heading?' *Information, Communication & Society*, 26(4), pp. 786–802.

Crabtree, J. (2018) 'Here's how Cambridge Analytica played a dominant role in Kenya's chaotic 2017 elections,' *CNBC*, 23 March. Available at: https://www.cnbc.com/2018/03/23/cambridge-analytica-and-its-role-in-kenya-2017-elections.html (Accessed: 8 June 2023).

Crain, M. and Nadler, A. (2019) 'Political Manipulation and Internet Advertising Infrastructure,' *Journal of Information Policy*, 9, pp. 370–410.

De, R., Pal, A., Sethi, R., Reddy, S.K. and Chitre, C. (2018) 'ICT4D research: a call for a strong critical approach,' *Information Technology for Development,* 24(1), pp. 63-94.

Del Vicario, M., Bessi, A., Zollo, F., Petroni, F., Scala, A., Caldarelli, G., Stanley, H. E., and Quattrociocchi, W. (2016) 'The spreading of misinformation online,' *Proceedings of the National Academy of Sciences of the United States of America*, *113*(3), pp. 554–559.

DeSantis, L. and Ugarriza, D. (2000) 'The concept of theme as used in qualitative nursing research,' *Western Journal of Nursing Research,* 22, pp. 351–372.

Dirks N (2001) *Castes of Mind: Colonialism and the Making of Modern India*. Princeton, NJ: Princeton University Press.

Dowling, M. (2021) 'Democracy Under Siege: Foreign Interference in a Digital Era,' *Australian Journal of International Affairs,* 75 (4), pp. 383–387.

Dowling, M. (2022) 'Cyber Information Operations: Cambridge Analytica's Challenge to Democratic Legitimacy,' *Journal of Cyber Policy,* 7 (2), pp. 230–48.

Eady, G., Nagler, Guess, Zilinsky and Tucker. (2019) 'How Many People Live in Political Bubbles on Social Media? Evidence From Linked Survey and Twitter Data,' *SAGE Open* 9(1).

Ekdale, B. and Tully, M. (2019) 'African Elections as a Testing Ground: Comparing Coverage of Cambridge Analytica in Nigerian and Kenyan Newspapers,' *African Journalism Studies,* 40 (4), pp. 27-43.

Eordogh, F. (2016) 'Pro-Trump Trolls Want You To Vote For Hillary Via Text (You Can't),' *Forbes*. Available at: https://www.forbes.com/sites/fruzsinaeordogh/2016/11/03/pro-trump-trolls-want-you-to-vote-for-hillary-via-text-you-cant/ (Accessed 20 July 2023).

European General Data Protection Regulation. (2016) *Regulation 2016/679.*

Fecteau, M.J. (2022) 'Understanding Information Operations & Information Warfare: The Muddled Meaning of IO (and IW),' *Global Security Review.* Available at: https://globalsecurityreview.com/understanding-information-operations-information-warfare/ (Accessed 20 July 2023).

Fraser, A. (2019) 'Curating digital geographies in an era of data colonialism,' *Geoforum*, 104, pp. 193–200.

Freelon, D. and Wells, C. (2020) 'Disinformation as Political Communication,' *Political Communication,* 37 (2), pp. 145–56.

Fuchs, Christian. (2017) *Social Media: A Critical Introduction*. 2nd ed. London: SAGE Publications.

Geeraerts, G. (1995) 'Analyzing Non-State Actors in World Politics,' *Pole Paper Series,* 1(4).

Gergen, K. J. (1985) 'The social constructionist movement in modern psychology,' *American Psychologist, 40*(3), pp. 266–275.

Gerring, J. (2014) 'What Is a Case Study and What Is It Good For?' *The American Political Science Review,* 98 (2), pp. 341-5.

Ghosh, D. and Scott, B. (2018) 'Disinformation is becoming unstoppable,' *Time.*

Gillespie, Tarleton. (2010) 'The Politics of 'Platforms,' *New Media & Society,* 12(3), pp. 347–64.

Githae, W. (2019) 'Jubilee e-mail leaks unmask quiet power of Nancy Gitau,' The Nation, 20 July. Available at: https://nation.africa/kenya/news/politics/jubilee-e-mail-leaks-unmask-quiet-power-of-nancy-gitau-187928 (Accessed 24 July 2023).

Golumbia, D. (2009) *The Cultural Logic of Computation*, Cambridge, MA: Harvard University Press.

Gorton, W. A. (2016) 'Manipulating Citizens: How Political Campaigns' Use of Behavioral Social Science Harms Democracy,' *New Political Science,* 38 (1), pp. 61–80.

Graneheim, U.H., Lindgren, B.M., and Lundman, B. (2017) 'Methodological challenges in qualitative content analysis: A discussion paper,' *Nurse Education Today*, 56, pp. 29-34.

Grassegger, H. and Krogerus, M. (2017) 'The Data That Turned the World Upside Down,' *Vice*, 28 January.

Grigsby, A. (2017) 'The End of Cyber Norms,' *Survival,* 59 (6), pp. 109–122.

Gross, J. (2016) 'Hack and Be Hacked: A Framework for the United States to Respond to Non-State Actors in Cyberspace,' *California Western International Law Journal,* 46 (2).

Halpern Sue (2021) 'Facebook and the Normalization of Deviance,' *The New Yorker*, 2 May. Available at: https://www.newyorker.com/news/daily-comment/facebook-and-the-normalization-of-deviance (Accessed: 8 June 2023).

Hanson, F. et al. (2019) 'Policy Brief: Hacking democracies: Cataloguing cyber-enabled attacks on elections,' *Australian Strategic Policy Institute.* Available at: https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-05/Hacking%20democracies.pdf (Accessed 24 July 2023).

Heawood, J. (2018) 'Pseudo-Public Political Speech: Democratic Implications of the Cambridge Analytica Scandal,' *Information Polity,* 23 (4), pp. 429–434.

Hendricks, V.F., Vestergaard, M. and Marker, S. (2018) 'Digital colonialism on the African continent,' *IOL Business Report.*

Henschke, A., Sussex, M. and O'Connor, C. (2020) 'Countering Foreign Interference: Election Integrity Lessons for Liberal Democracies,' *Journal of Cyber Policy,* 5 (2), pp. 180–198.

Hinds, J., Williams, E.J. and Joinson, A.N. (2020) '"It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal,' *International Journal of Human-Computer Studies,* 143.

Holloway I. and Todres, L. (2003) 'The status of method: Flexibility, consistency and coherence,' *Qualitative Research,* 3, pp. 345–357.

Holtz-Bacha, C., Just, M.R., Ridout, T. and Holland, J.L. (2017) 'The Effects of Political Advertising.' In *Routledge Handbook of Political Advertising* (eds) New York: Routledge, pp. 61–71.

House of Commons. Digital, Culture, Media and Sport Committee –
(2018) 'Disinformation and 'Fake News: Interim Report' *UK Parliament.*
(2019) 'Disinformation and 'Fake News: Final Report' *UK Parliament.*
(n.d.) 'Chris Wylie Background Papers', *UK Parliament.* Available at: https://www.parliament.uk/globalassets/documents/commons-

committees/culture-media-and-sport/Chris-Wylie-Background-papers.pdf (Accessed 20 July 2023).

Howard, P. and Bradshaw, S. (2018) 'The Global Organization of Social Media Disinformation Campaigns,' *Journal of International Affairs* [Preprint].

Howell L. (2013) 'Digital wildfires in a hyperconnected world,' *WEF Report* 2013. Available at reports.weforum.org/global-risks-2013/risk-case-1/digital-wildfires-in-ahyperconnected-world. (Accessed 9 June 2023).

Hu, M. (2020) 'Cambridge Analytica's black box,' *Big Data & Society,* 7(2).

Hunt, J.S. (2021) 'Australian Journal of Defence and Strategic Studies Commentary Countering cyber-enabled disinformation: implications for national security,' *Australian Journal of Defence and Strategic Studies,* 3(1).

Imende, B. (2017) 'Uhuru, Raila teams take campaign wars online,' *The Star*, 6 June. Available at: https://www.the-star.co.ke/news/2017-06-06-uhuru-raila-teams-take-campaign-wars-online/ (Accessed: 8 June 2023).

Information Commissioner's Office. (2018) 'Investigation into the use of data analytics in political campaigns,' *Information Commissioner's Office*. 6 November. Available at: https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf (Accessed: 19 July 2023).

Isaak, J. and Hanna, M.J. (2018) 'User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection,' *Computer,* 51(8), pp. 56-59.

Jackson, M. and Lieber, P. (2020) 'Are We Our Own Worst Enemy?' *The Cyber Defense Review*, 5(2), pp. 45–56.

Jasanoff, S. (2006) 'Biotechnology and empire: The global power of seeds and science,' *Osiris,* 21(1), pp. 273–292.

Kanakia, H., Shenoy, G. and Shah, J. (2019) 'Cambridge Analytica: A Case Study,' *Indian Journal of Science and Technology*, 12(29), pp. 1–5.

Karlsen, G.H. (2019) 'Divide and rule: ten lessons about Russian political influence activities in Europe,' *Palgrave Communications*, 5(1), p. 19.

Kim, Y.M. et al. (2018) 'The Stealth Media? Groups and Targets behind Divisive Issue Campaigns on Facebook,' *Political Communication*, 35(4), pp. 515–541.

King N. (2004) 'Using templates in the thematic analysis of text.' In Cassell C., Symon G. (Eds.), *Essential guide to qualitative methods in organizational research* (257–270). London, UK: Sage.

King, E. (2016) 'Russian Hackers Targeting Germany: Intelligence Chief,' *Politico EU.* Available at: http:// www.politico.eu/article/german-intelligence-chief-russian-hackers-targeting-us-bruno-kahl-vladimir-putin/ (Accessed 20 June 2023).

Klots, A. and Lynch, C. (2007) *Strategies for Research in Constructivist International Relations.* Armonk, NY: M.E. Sharpe.

Krupnikov, Y. (2014) 'How Negativity Can Increase and Decrease Voter Turnout: The Effect of Timing,' *Political Communication,* 31(3), pp. 446–66.

Kwet, M. (2019) 'Digital Colonialism: US Empire and the New Imperialism in the Global South,' *Race & Class,* 60 (4), pp. 3–26.

Lamont, C.K. (2015) *Research methods in international relations,* SAGE Publications, London.

Lange, M., Jeong, T. and Amasyali, E. (2021) 'The colonial origins of ethnic warfare: Re-examining the impact of communalizing colonial policies in the British and French Empires,' *International Journal of Comparative Sociology*, 62(2), pp. 141–165.

Lee, G. (2018) 'Q&A on Cambridge Analytica: The allegations so far, explained,' *Channel 4 News.* Available at: https://www.channel4.com/news/factcheck/cambridge-analytica-the-allegations-so-far (Accessed 24 July 2023).

Leszczynski, A. (2012) 'Situating the geoweb in political economy,' *Progress in Human Geography*, 36(1), pp. 72–89.

Levin, S. (2017) 'Facebook promised to tackle fake news. But the evidence shows it's not working,' *The Guardian*. Available at: https://www.theguardian.com/technology/2017/may/16/facebook-fake-news-tools-not-working#:~:text=A%20Guardian%20review%20of%20false,to%20be%20having%20minimal%20impact. (Accessed 24 July 2023).

Lewis, A. and McKone, D. (2016) 'To Get More Value from Your Data, Sell It,' *Harvard Business Review*, 21 October.

Lewis, P. and Hilder, P. (2018) 'Leaked: Cambridge Analytica's blueprint for Trump victory,' *The Guardian* 23 March. Available at: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory (Accessed 20 June 2023).

Lion, G., Kropotov, V and Yarochkin, F. (2017) 'The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public,' *TrendMicro.* Available at:

https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf (Accessed 24 July 2023).

Madianou, M. (2019) 'Technocolonialism: Digital innovation and data practices in the humanitarian response to refugee crises,' *Social Media & Society*.

Madowo, L. (2018) 'How Cambridge Analytica poisoned Kenya's democracy,' *The Washington Post*, 20 March. Available at: https://www.washingtonpost.com/news/global-opinions/wp/2018/03/20/how-cambridge-analytica-poisoned-kenyas-democracy/ (Accessed: 8 June 2023).

Madung, O. (2022) 'Kenya's already fragile elections now face a dangerous new enemy: big tech platforms,' *The Guardian*, 7 April. Available at: https://www.theguardian.com/commentisfree/2022/apr/07/kenya-elections-2022-big-tech-platforms (Accessed: 8 June 2023).

Magalhães, J.C. and Couldry, N. (2021) 'Giving by Taking Away: Big Tech, Data Colonialism, and the Reconfiguration of Social Good, International Journal of Communication,' *International Journal of Communication*, 15.

Mäkinen, M. and Kuria, M.W. (2008) 'Social Media and Post-Election Crisis in Kenya,' *International Journal of Press/Politics,* 13 (3), pp. 328–335.

Martin, J. (2017) 'Dubious Vote-Fraud Claim Gets the Trump Seal of Approval,' *The New York Times*. Available at: https://www.nytimes.com/2017/01/27/us/politics/donald-trump-voter-fraud.html (Accessed 20 July 2023).

Marwick, A., and Lewis, R. (2017) 'Media Manipulation and Disinformation Online,' *New York: Data & Society Research Institute*.

Mathenge, O. (2013) 'Kenya: How British PR Firm Helped Jubilee Win,' *The Star*, 6 April.

Mavriki, P., and Karyda, M. (2019) 'Big Data Analytics: From Threatening Privacy to Challenging Democracy.' In *E-Democracy Safeguarding Democracy and Human Rights in the Digital Age,* edited by Katsikas, S. and Zorkadis, V., pp. 3–17. Cham: Springer.

Maweu, M. (2019) 'Fake Elections? Cyber Propaganda, Disinformation and the 2017 General Elections in Kenya,' *African Journalism Studies,* 40 (4), pp 62-76.

McKay, G. (2022) *Disinformation and Democratic Transition: A Kenyan Case Study*. Stimson Centre.

McKay, S., and Tenove, C. (2021) 'Disinformation as a Threat to Deliberative Democracy,' *Political Research Quarterly,* 74 (3), pp. 703–717.

Miles, M. B. and Huberman, A. M. (1994). *Qualitative data analysis: An expanded source book* (2nd ed.). Newbury Park, CA: Sage.

Miriello, N., Gilbert, D. and Steers, J. (2018) 'Kenyans face a fake news epidemic,' *Vice*. Available at: https://www.vice.com/en/article/43bdpm/kenyans-face-a-fake-news-epidemic-they-want-to-know-just-how-much-cambridge-analytica-and-facebook-are-to-blame (Accessed 24 July 2023).

Miriri, D. (2018) 'Kenya's ruling party says hired firm linked to data breach,' *Reuters*, 20 March. Available at: https://www.reuters.com/article/facebook-cambridgeanalytica-kenya-idUSL8N1R24G2 (Accessed 9 June 2023).

Mishler, E. G. (1990) 'Validation in inquiry-guided research: The role of exemplars in narrative studies,' *Harvard Educational Review,* 60, pp. 415–441.

Morgan, S. (2018) 'Fake news, disinformation, manipulation and online tactics to undermine democracy,' *Journal of Cyber Policy*, 3(1), pp. 39–43.

Morse J. and Richards, L. (2002) 'Coding.' In Morse J., Richards (Eds.), *Read me first for a user's guide to qualitative methods* (111–128). Thousand Oaks, CA: Sage.

Mozilla Foundation –
'Exporting Disinformation: How foreign groups peddle influence in Kenya through Twitter'. Available at: https://assets.mofoprod.net/network/documents/Exporting_Disinformation.pdf. (Accessed Nov 2022)
'From Dance App to Political Mercenary: How disinformation on TikTok gaslights political tensions in Kenya'. Available at: https://assets.mofoprod.net/network/documents/From_Dance_App_to_Political_Mercenary.pdf. (Accessed Nov 2022)
'Inside the Shadowy World of Disinformation for Hire in Kenya'. Available at: https://assets.mofoprod.net/network/documents/Report_Inside_the_shadowy_world_of_disinformation_for_hire_in_Kenya_5._hcc.pdf. (Accessed Nov 2022)

Mumford, D. (2022) 'Data colonialism: compelling and useful, but whither epistemes?' *Information, Communication & Society*, 25(10), pp. 1511–1516.

Nadler, A., Crain, M., and Donovan, J. (2018) 'Weaponizing the digital influence machine: the political perils of online ad tech,' *Data and Society*.

The Nation Team (2019) 'Agent in Jubilee's 2017 Jubilee poll victory opens up', *The Nation*, 16 July. Available at: https://nation.africa/kenya/news/politics/agent-in-jubilee-s-2017-jubilee-poll-victory-opens-up-186722 (Accessed 24 July 2023).

Ngila, F. (2020) 'When technology is used to run evil schemes, democracy suffers', *The Nation*, 12 September. Available at: https://nation.africa/kenya/blogs-opinion/opinion/when-technology-evil-schemes-democracy-1937310 (Accessed 24 July 2023).

Ngila, F. and Sheik, M. (2022) 'Africa's struggles in regulating Big Tech's data colonialism', *The Nation*, 3 April. Available at: https://nation.africa/kenya/blogs-opinion/blogs/-africa-s-struggles-in-regulating-big-tech-s-data-colonialism--3776636 (Accessed 24 July 2023).

Nhemachena, A., Hlabangane, N., and Kaundjua, M. (2020) 'Relationality or hospitality in twenty-first century research? Big data, internet of things, and the resilience of coloniality in Africa,' *Modern Africa: Politics, History and Society*, *8*(1), pp.105–139.

Nowell, L.S., Norris, J.M., White, D.E. and Moules, N.J. (2017) 'Thematic Analysis: Striving to meet the trustworthiness criteria,' *International Journal of Qualitative Methods,* 16 (1).

NVivo. (2022) 'Thematic analysis of interview data: 6 ways NVivo can help', Available at: https://lumivero.com/resources/thematic-analysis-of-interview-data-nvivo/ (Accessed 20 July 2023).

Nyabola, N. (2017) 'What Kenyan voters got for the $500m spent on elections,' *Al Jazeera*, 18 August. Available at: https://www.aljazeera.com/opinions/2017/8/18/what-kenyan-voters-got-for-the-500m-spent-on-elections (Accessed 24 July 2023).

Nyabola, N. (2018a) *Digital Dialogue, Analogue Politics: How the internet era is transforming politics in Kenta*. 1st edn. London: Zed Books.

Nyabola, N. (2018b) 'In Kenya, Election Manipulation Is a Matter of Life and Death,' *The Nation*, 28 March. Available at: https://www.thenation.com/article/archive/in-kenya-election-manipulation-is-a-matter-of-life-and-death/ (Accessed 24 July 2023).

Nyabola, N. (2018c) 'Politics in the digital age: Cambridge Analytica in Kenya,' *Al Jazeera*, 22 March. Available at: https://www.aljazeera.com/opinions/2018/3/22/politics-in-the-digital-age-cambridge-analytica-in-kenya (Accessed 24 July 2023).

Nyabola, N. (2019) 'Platform Governance of Political Speech,' *Centre for International Governance Innovation*, 28 October. Available at:

https://www.cigionline.org/articles/platform-governance-political-speech/ (Accessed: 8 June 2023).

Ochieng', J. (2020) 'ODM "refused" to work with "evil" Cambridge Analytica in 2017,' *The Nation*, 5 January. Available at: https://nation.africa/kenya/news/politics/odm-refused-to-work-with-evil-cambridge-analytica-in-2017--238180 (Accessed 24 July 2023).

Persily, N. (2017) 'Can Democracy Survive the Internet?' *Journal of Democracy,* 28(2), pp. 63–76.

Peters, J. W. (2017) 'A Pro-Trump Conspiracy Theorist, a False Tweet and a Runaway Story,' *The New York Times*. Available at: https://www.nytimes.com/2017/06/10/us/politics/comey-fake-newstwitter-posobiec.html (Accessed 20 July 2023).

Portland (no date) 'The Reality of Fake News in Kenya,' *Portland Communication*. Available at: https://portland-communications.com/pdf/The-Reality-of-Fake-News-in-Kenya.pdf (Accessed 24 July 2023).

Privacy International (2017a) 'Texas Media Company Hired By Trump Created Kenyan President's Viral 'Anonymous' Attack Campaign Against Rival, New Investigation Reveals,' *Privacy International*. Available at: https://privacyinternational.org/long-read/954/texas-media-company-hired-trump-created-kenyan-presidents-viral-anonymous-attack (Accessed: 8 June 2023).

Privacy International (2017b) 'Voter Profiling in the 2017 Kenyan Election,' *Privacy International*.

Privacy International (2018) 'Further questions on Cambridge Analytica's involvement in the 2017 Kenyan Elections and Privacy International's investigations,' *Privacy International*.

RAND Corporation (n.d.) 'Information Operations,' *RAND*. Available at https://www.rand.org/topics/information-operations.html (Accessed 20 July 2023).

Ravel, A. M., Woolley, S. C., and H. Sridharan. (2019) *Principles and Policies to Counter Deceptive Digital Politics*. Maplight; Institute for the Future, 2019.

Ray, A. (2021) 'Disinformation, Deepfakes and Democracies: The Need for Legislative Reform,' *University of New South Wales Law Journal*, 44(3).

Rosenberger, L. (2020) 'Disinformation Disorientation,' *Journal of Democracy*, 31(1), pp. 203–207.

Rosenberger, L. and Gorman, L. (2020) 'How Democracies Can Win the Information Contest,' *The Washington Quarterly*, 43(2), pp. 75–96.

Sadowski, J. (2019) 'When data is capital: Datafication, accumulation, and extraction,' *Big Data & Society*, 6(1).

Schia, N.N. and Gjesvik, L. (2020) 'Hacking democracy: managing influence campaigns and disinformation in the digital age,' *Journal of Cyber Policy*, 5(3), pp. 413–428.

Segura, M. S., and Waisbord, S. (2019) 'Between data capitalism and data citizenship,' *Television & New Media,* 20(4), pp. 412–419.

Sevenzo, F. (2017) 'Kenya election: Fake CNN, BBC reports target voters,' *CNN*, 1 August.

Solove, Daniel. (2004) *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.

Steensen, S. (2019) 'Journalism's epistemic crisis and its solution: Disinformation, datafication and source criticism,' *Journalism*, 20(1), pp. 185–189.

Tait, M.M., dos Reis Peron, A.E. and Suárez, M. (2022) 'Terrestrial politics and body-territory: two concepts to make sense of digital colonialism in Latin America,' *Tapuya: Latin American Science, Technology and Society*, 5(1).

Taylor, M.L. (2019) 'Combating disinformation and foreign interference in democracies: Lessons from Europe,' *Brookings*, 31 July.

Tenove, C.*,* Buffie, McKay and Moscrop. (2018) 'Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy,' *SSRN Electronic Journal* [Preprint].

Thatcher, J., O'Sullivan, D. and Mahmoudi, D. (2016) 'Data colonialism through accumulation by dispossession: New metaphors for daily data,' *Environment and Planning D: Society and Space*, 34(6), pp. 990–1006.

The Guardian. n.d. 'The Cambridge Analytica Files.' Accessed Nov 2022, https://www.theguardian.com/news/series/cambridge-analytica-files.

The Real Ralia. (2017) 'Kenya in 2020 if Raila Odinga is elected President | The Real Raila', *Youtube* 10 July. Available at: https://www.youtube.com/watch?v=o45NlqZXDXw (Accessed 20 July 2023).

Thompson, N. (2017) 'Canadian working with Kenya opposition party deported,' *The Canadian Press*, 5 August.

Tsalkilis, C. (2019) 'Nanjala Nyabola on the "Digital Colonialism" Transforming Kenya's Political Discourse,' *Centre for International Governance Innovation*, 5 November.

Tufekci, Z. (2018) 'Facebook's Surveillance Machine,' *New York Times*, March 19, 2018. Accessed Nov 2022, https://www.nytimes.com/2018/03/19/opinion/facebook-cambridge-analytica.html.

Vosoughi, S., Roy, D., and Aral, S. (2018) 'The spread of true and false news online,' *Science,* 359(6380).

Wangari, N. (2017) 'Data and Democracy: What Role Did Cambridge Analytica Play in Kenya's Elections?' *Global Voices*, 3 November.

Warah, R. (2019) 'Cambridge Analytica and the 2017 Elections: Why Has the Kenyan Media Remained Silent?' *The Elephant*, 19 August.

Wardle, C., and Derakhshan, H. (2018) 'Thinking about 'Information Disorder': Formats of misinformation, Disinformation and Mal Information.' In *Journalism, 'Fake News' & Disinformation: Handbook for Journalism Education and Training,* edited by C. Ireton and J. Posetti, 44–56. UNESCO.

Weedon J., Nuland W. and Stamos A. (2017) 'Information operations and Facebook.' *Facebook*, 27 April.

White, M.D., and Marsh, E.E. (2006) 'Content Analysis: A Flexible Methodology,' Library Trends, 55 (1), pp. 22-45.

Wijninga, P., Oosterveld, W.T., Galdiga, J.H. and Marten, P. (2014) 'State and Non-State Actors: Beyond the Dichotomy,' *Strategic Monitor*.

Woolley, S.C. (2016) 'Automating power: Social bot interference in global politics', *First Monday* [Preprint].

World Economic Forum. (2011) 'Personal Data: The Emergence of a New Asset Class', *WE Forum,* January. Available at: http://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf. (Accessed 20 July 2023).

Young, J.C. (2019) 'The new knowledge politics of digital colonialism,' *Environment and Planning A: Economy and Space*, 51(7), pp. 1424–1441.

Young, K.M., Hsu, J., Neiman, D., Kou, C., Bankston, L., Kim, S.Y., Heinrich, R., Baragwanath, R. and Raskutt, G. (2018) 'The Stealth Media? Groups and Targets Behind Divisive Issue Campaigns on Facebook.' *Political Communication,* 35 (4), pp. 515–541.

Zawacki, K. (2021) 'Breaking Bias: When Twitter's Negligence Harms Democracy,' *Mozilla*.

Zimmerman, R. (2020) 'Corporate Weaponization of Social Media Platforms Threatens Democracy [analysis],' *AllAfrica News*, 6 July.

Zuboff, S. (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York, NY: Polity Press.

8. __Appendices__

Appendix A: Full Results of the Thematic Analysis

Node Name	References
Relationships	75
Hired by Political Parties	35
Close Working Relationship	31
Working with Local Actors	8
Motivation	62
Profit	42
Testing	20
Methods	185
Microtargeting	97
Campaign Support	34
Campaign Research	25
Surveys	15
Social Media Campaigns	14
Positive and Negative Advertisements	40
Image and Messaging	25
Speeches	8
Training	4
Voter mobilisation	3
Content	119
Disinformation	59
Needs and Fears	23
Ethnic undertones	21
Emotive Messaging	16
Impact	168
Avoiding Accountability	70
Unethical Behaviour	25
Lack of transparency	20
Violence	38
Undermining the Democratic Process	22
Tension, Instability and Division	22
Success	11
Limits on Success	15
Professionalisation	5

Appendix B: Screencap of Relationship Node in Nvivo 12

Name			Files	References	
⌄ ◯ Relationships			28	75	
◯ Close Working Relation...			11	31	
◯ Hired by Political Parties			22	35	
◯ Working with local actors			6	8	

Appendix C: Screencap of Motivation Node in Nvivo 12

Name			Files	References	
⌄ ◯ Motivation			24	62	
◯ Testing			10	20	
◯ Profit			22	42	

Appendix D: Screencap of Methods Node in Nvivo 12

Name			Files	Refe... ⌄
⌄ ◯ Methods used by Non-sta...			38	185
◯ Microtargeting			26	97
◯ Campaign Support			18	34
⌄ ◯ Campaign Research			15	25
◯ Surveys			14	15
⌄ ◯ Social Media Campaigns			12	14
◯ Positive and Negativ...			14	40
◯ Image and Messaging			16	25
◯ Speeches			6	8
◯ Training			3	4
◯ Voter Mobilisation			3	3

Appendix E: Screencap of Content Mode in Nvivo 12

Name			Files	References
⌄ ● Content			31	119
● Emotional Messaging			9	16
● Ethnicity			11	21
● Fake News or disinform...			19	59
● Needs and fears			18	23

Appendix F: Screencap of Impact Node in Nvivo 12

Name			Files	References	
⌄ ● Impact			38	168	
⌄ ● Avoiding Accountability			22	70	
● Lack of transparency			12	20	
● unethical behaviour			15	25	
● Professionalisation			2	5	
⌄ ● Succcess			8	11	
● Limits on success of...			7	15	
● Tension, Instability and...			13	22	
● Undermining the Demo...			13	22	
● Violence			14	38	