



UNIVERSITY
OF
JOHANNESBURG

COPYRIGHT AND CITATION CONSIDERATIONS FOR THIS THESIS/ DISSERTATION

 creative
commons



- Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.
- NonCommercial — You may not use the material for commercial purposes.
- ShareAlike — If you remix, transform, or build upon the material, you must distribute your contributions under the same license as the original.

How to cite this thesis

Surname, Initial(s). (2012). Title of the thesis or dissertation (Doctoral Thesis / Master's Dissertation). Johannesburg: University of Johannesburg. Available from: <http://hdl.handle.net/102000/0002> (Accessed: 22 August 2017).

Computational Propaganda:
Exploring Mitigation Strategies for Political Parties in Online Brand Contexts.

by

Randy Robertson

200503883

Submitted in fulfilment of the requirements for the degree

MA Strategic Communication

in the

Strategic Communication Department

of the

Faculty of Humanities

at the

University of Johannesburg

supervised by

Dr. Corné Meintjes

31 January 2019

Acknowledgements

I would first like to thank Dr. Corné Meintjes of the University Of Johannesburg for her patience and belief that this project could be completed.

I would also like to thank the experts who were involved in this research, although you remain anonymous; I appreciate your valuable time, insights and perspective.

Finally, I must express my very profound gratitude to my mother Shireen Robertson who passed during the time this report was written, your fight gave me the will and courage and to continue when completion seemed nearly impossible. I appreciate all you've done to get me here.

To my wife Odile Robertson thank you for providing me with unfailing support and continuous encouragement throughout my years of study. This accomplishment would not have been possible you.

Thank you!



Abstract

This research delves into the phenomenon of computational propaganda on social media, and draws on social media specialists from some of South Africa's best performing brands to explore potential strategies political parties can employ to mitigate against crises that occur as a result of computational propaganda.

This research is of importance given that South Africa is entering its first ever National Elections since the identification of computational propaganda as a threat to electoral processes. To date, there is no research that explores this within the South African context.

The research entailed semi-structured interviews with eight social media managers, selected using the purposive non-probability sampling method. In addition to this, the research interviewed a communications head from South Africa's largest political party in order to assess what strategies are already in place. These two sets of data were consolidated resulting in four potential strategies to mitigate against the risk of computational propaganda. The four potential mitigation strategies are grouped into two approaches, the first approach relates to preventative measures political parties can take, namely protecting brand identity and aligning communications. The second approach related to defensive measures political party brands could take in the event of a computational propaganda event, namely online reputation management and integration of communication.

The research further uncovered contextual considerations political party brands must take into account before employing strategies to mitigate against crises that arise as a result of computational propaganda.

Table of Contents

	Page number
1.1 Introduction	1
1.1.1 Problem Statement.....	5
1.1.2 Purpose Statement.....	6
1.1.3 Research objectives	6
1.1.4 Theoretical Framework.....	7
1.1.5 Research Methods	8
1.1.6 Limitations of the study.....	8
1.1.7 Outline of the Report	10
1.1.8 Conclusion.....	10
2.1 Literature Review	11
2.1.1 Introduction.....	11
2.1.2 Political Parties as Brands.....	11
2.1.3 Web 2.0 and Social Media.....	13
2.1.4 Digital Brand Risk.....	16
2.1.5 Computational Propaganda.....	18
2.1.5.1 Algorithmic filtering	19
2.1.5.2 Automation.....	21
2.1.5.3 Curation	23
2.1.6 Online Reputation Management.....	24
2.1.7 Risk Mitigation Strategies.....	25
2.1.8 Conclusion.....	27
3.1 Research Methodology.....	28
3.1.1 Introduction.....	28
3.1.2 Research Approach.....	28
3.1.3 Sampling Strategy	29
3.1.3.1 Sample Population.....	29
3.1.3.2 The Sample	30
3.1.4 Data Collection	31
3.1.5 Data Analysis.....	32
3.1.6 Ethics.....	33
3.1.7 Trusworthiness	34
3.1.8 Limitations of the Study	35
4.1 Exploring mitigation strategies for computational propaganda.....	36
4.1.1 Introduction.....	36
4.1.2 Preventative Measures.....	40
4.1.2.1 Issues of brand identity.....	40
4.1.2.2 Communications Alignment	45
4.1.3 Defensive Measures.....	49
4.1.3.1 Online Reputation Management.....	49
4.1.3.2 Communication Integration.....	53
4.1.4 Contextual Considerations	56
4.1.4.1 Engagement and Algorithmic Filtering.....	56
4.1.4.2 Freedom of speech and censorship	58
4.1.4.3 Conclusion	59

5.1 Research Findings and Recommendations	60
5.1.1 Findings as they Relate to the Research Aims and Objectives.....	61
5.1.2 Recommendations for Future Research.....	64
5.1.3 Recommendations for Practice	64
5.1.4 Conclusion.....	65
5.2 References	66
5.3 Appendix A: Social Media Interview Question Guide	80
5.4 Appendix B: Political Party Interview Question Guide	80
5.5 Appendix C: Social Media Interview Transcript	80
5.6 Appendix D: Political Party Interview Transcript	103
5.7 Appendix E: Communication Misalignment	105



Introduction

1.1 Introduction

Sidi Bouzid, Tunisia, 17 December 2010 (Lageman, 2016) Mohammed Bouazizi, a 26 year old fruit vendor and breadwinner to a household of seven people (Abouzied, 2011), takes his fruit cart to the local souk to begin the day's trade. While making his way to the market, Bouazizi is approached by police officials, with whom he has a confrontational verbal exchange (Ryan, 2011b). Bouazizi later arrives at the market and is confronted again by police officials where the situation escalates quickly when Mohammed can only give \$7 for a \$10 fine. This act results in him being slapped in addition to the confiscation of his electronic scales and fruit cart (Abouzied, 2011). Frustrated that his livelihood had been taken away, Bouazizi later walks to the nearest government offices in his town to seek recourse to no avail. An hour after senior officials refuse to attend to his complaint, Bouazizi sets himself alight in frustration (Lageman, 2016). Shocked bystanders captured the spectacle and uploaded the content for distribution on Facebook, which was Tunisia's only uncensored platform at the time (Ryan, 2011a). This moment became a symbol of the frustration North African youth felt as a result of socio-economic inequality and disenfranchisement (Salih, 2013), and would be the spark to a fire that would be later known as the Arab Spring (Toko, 2012). Starting in Tunisia, the Arab Spring became a civilian revolutionary movement that engulfed Algeria, Jordan, Libya, Egypt, Yemen, Syria and Bahrain (Salih, 2013), becoming one of the first civil society movements that spanned a multitude of countries simultaneously without having any central coordinating structures, making it one of the first revolutionary waves to reflect the changing power relations partly with the assistance of new communication networks like social media (Tudoroiu, 2014).

This scenario illustrates the power social media can possess in democratising political influence. It also may be seen as a positive from civil society's perspective, as it helped to overthrow traditional structures of political influence by giving it back to the general public (Salih, 2013). But what happens when nefarious forces sow division and manipulate this power? Enter a new social media and political phenomenon known as computational propaganda, which is the act of using social media's power to spread inflammatory misinformation (Woolley and Howard, 2016).

The latest global research on social media indicates that the world's social media audience has grown to over 3 billion users daily (We Are Social, 2017). This rise in daily usage numbers around the world indicates that social media has begun to become a ubiquitous form of communication over the past two years (Katzman, 2016). While many benefits have come as a result of the growth of such platforms, there are some detrimental effects of this growth. One such effect is that social interactivity can present great reputational risk because it allows information to be shared at great speed with great reach, often with the page or profile owner-losing context, tone, and control (Carter, 2017).

While most existing crisis communication research is focused on the general public and their response to brands or complaint behaviour, political parties are no strangers to the rigors of social media. Whereas commercial brands are pitted against irate customers, the emotive and ideological nature of politics may lay political parties and figures victim to online aggression at levels beyond those experienced by brands (Woolley and Howard, 2017). Rost, Stahel and Frey (2016, p. 26) indicate that online aggression aimed at people and institutions of public interest has become a growing phenomenon, and it will continue to grow as digital civil society attempts to "enforce norms and contribute to the formation of latent interest groups". Due to the ideological nature of politics and the norm of online aggression against them, political figures have begun to fall victim to a form of junk news called "computational propaganda".

Computational propaganda can be viewed as a digital form of information dissemination wherein parties or their adversaries use social media and online aggression to propagate damaging, often untrue information in attempts to create false narratives. Woolley and Howard (2016) define computational propaganda as "the assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion". Automated bots are key to the manipulation of public opinion; these are automated social media accounts run by computer script, that are able to deploy messages, replicate and disseminate information at scale (Neudert, 2017).

While evidence suggests that computational propaganda is a growing worldwide phenomenon, South Africa has also been impacted. For example a 'white monopoly capital campaign', wherein Bell Pottinger, a United Kingdom based public relations

agency, set up Gupta-aligned bots that suggested white owned businesses in South Africa were more implicated in state capture and more harmful than Gupta-owned businesses who were involved in state capture (ANCIR, 2017).

South Africa is not the only location which is been affected by computational propaganda. The phenomenon has affected political processes the world over, with Brazil's 2014 elections being the earliest documented case. In this case, incumbent Brazillian President Dilma Rousseff was forced into a run-off election at the hands of centre right candidate Aecio Nevez with the assistance of a multimillion dollar budget spent on misinformation using social media bots deployed on facebook, twitter and whatsapp (Arnaudo, 2017). The developed world has also not been left unaffected; in Europe during the French presidential election, scholars from Oxford's Computational Propaganda project found that up to a quarter of all political links shared on twitter were found to contain political misinformation which was ideologically extreme or merely opinion presented as facts (Farand, 2017). In addition to this, further investigation into the use of botnets during the French election uncovered Russian interference with the intent to destabilise the European Union.

France is not the only European country to fall victim to botnets and computational propaganda. The effects of internet misinformation have also impacted electoral processes in Germany, where the growing right wing and their anti-immigration populist leaders gained audiences as a result of bot networks that were deployed to spread populist far-right sentiment (Neudert, 2017). Italy, however, determined the computational propaganda threat to be so great that an online task team was assembled to report junk news sources. Most recently, the most notable instance of computational propaganda emerged in the American presidential elections where a consultancy named Cambridge Analytica was found to be harvesting data from 87 million Facebook users' accounts to serve them with politically motivated content based on those users' psychological profile (Greenfield, 2018). Cambridge Analytica's project, which was done without facebook's consent, brought to light the large extent of political meddling taking place online, as their project is believed to have help mobilise neo-conservatives in getting to the polls in the 2016 US presidential elections, and thereby playing a critical role in Donald Trump's presidential campaign victory (Lewis and Hilder, 2018).

While the impact of digital marketing and social media in the American election may come as a surprise, it's important to note that digital marketing and social media have been an area of investment for political parties since Barack Obama's successful presidential social media campaign in 2008 (Aaker and Chang, 2009). Subsequently, investment in recent elections have been substantial, for example, Republican candidate Senator Ted Cruz's 2016 campaign made a human capital investment of 40 data scientists, digital marketers and web developers. In addition, \$4.4 million dollars of the \$13 million digital marketing budget was paid to Cambridge Analytica during the Republican primaries (Kroll, 2018). Ultimately, the Cambridge Analytica scandal brought the phenomenon of computational propaganda to the forefront in global mainstream media, given that it was the first large-scale instance where Facebook, the world's largest social network, admitted that it was used for political meddling, to the extent that Facebook founder Mark Zuckerberg admitted to having his own personal data leaked during presentations to the US Senate (Jenkins, 2018).

In the white paper entitled "Why does junk news spread so quickly across social media?" Howard and Bradshaw, (2018) indicate that the growth of the computational propaganda phenomenon and junk news are a result of a number of factors including the rise of social media as a news source, growing mistrust the public have in the political elite and the way algorithms curate information optimised for engagement. Two other drivers of computational propaganda are (1) the use of pay per click advertising to generate revenue (wherein salacious and misleading headlines referred to as clickbait generate a high amount of clicks in return for money) (Howard and Bradshaw, 2018); and (2) filter bubbles, where users have reduced exposure to opposing information due to algorithms serving them the information it deems them most likely to consume (Pfeffer, Zorbach and Carley, 2014) . All these elements have conspired to create what we've come to know as a "post truth" world (BBC, 2017)

This post-truth scenario creates difficulties for political parties and those falling victim to computational propaganda. Howard and Bradshaw (2018) indicate that it is challenging to design or regulate social media in a way that reduces electoral interference.

They further argue that a solution would most likely require a multidisciplinary approach, consisting of technological tools to manage platforms and oversight from civil society and government. What this solution does not take into account, however, is the ever-changing attacks on people's perceptions through communication, which suggests that a communication solution should also be found. The status quo suggests that political parties require communication defences that are just as fast, dynamic and adaptive as the attacks to which they fall victim.

1.1.1 Problem Statement

Although social media crisis communications have been an area of focus amongst communications scholars with the advent of web 2.0, computational propaganda has only come to the fore since 2012. Succinctly defined, Computational Propaganda is the use of algorithms and automation to distribute misleading information via social media. Instances of this form of political manipulation have impacted democratic processes in many countries globally (Woolley and Howard, 2017). As already discussed, in the case of Brazil and South Africa, twitter bots spread misinformation, and in America and Europe, stolen Facebook data was used to target and psychologically manipulate voters (Woolley and Howard, 2017). Hence, Computational Propaganda involves sophisticated social media strategies to sway voters (Wickenden, 2018).

Zhang *et al.* (2013) point out that the success of computational propaganda depends on its agents' ability to create and deploy bot networks that are difficult to differentiate from humans online. In addition to social bot networks, agents of computational propaganda have also been found to use paid media to spread disinformation, as recently discovered by Facebook's investigation into Russian use of paid Facebook adverts to influence election outcomes in America and Europe (Thompson and Vogelstein, 2018).

The automated nature of Computational Propaganda may mean that existing strategies defining and diagnosing digital brand risk and destruction may not be sufficient. In light of the growing influence of Computational Propaganda and growing social media users, South Africa needs to deploy mitigation strategies in the upcoming 2019 elections. Theory on digital brand risk, and computational propaganda is still in its infancy, so it is unclear how South Africa might ameliorate the risks.

Therefore, in this research I have explored how South African political parties can mitigate the impact of Computational Propaganda during the South African elections. It is important to note that risk mitigation can take on two forms: reducing risk at the hands of the agents of Computational Propaganda, and reducing brand risk by attending to stakeholder's perceptions once the computational propaganda has occurred, the latter is the focus of this study.

1.1.2 Purpose Statement

The purpose of this study is to help political parties avoid malicious online brand attacks by asking:

Q: How can the brand risk of Computational Propaganda be mitigated by political party brands in online brand contexts?

The potential answer to this question will be proposed based on an answer to the following sub-questions:

1. How does Computational Propaganda manifest itself online?
2. What strategies are political parties using to mitigate Computational Propaganda risks?
3. Which digital brand risk mitigation strategies can political brands employ to mitigate the brand consequences of computational propaganda?

The research proposed is of importance because a failure to identify and use relevant mitigation strategies against Computational Propaganda may cause political brands to lose their brand equity and, even worse, erode the legitimacy of their governance.

1.1.3 Research objectives

The objectives of the research conducted is to;

- Explore the nature of how Computational Propaganda manifests online.
- Investigate what strategies political parties are using to mitigate against Computational Propaganda risks.
- Discover which digital brand risk mitigation strategies political parties can employ to mitigate against the brand consequences of Computational Propaganda.

1.1.4 Theoretical Framework

This research is grounded in the modernist effectiveness model (Torp, 2015), wherein communication is a form of expression that occurs in a marketplace of different voices competing to persuade (Mumby, 1997). The research also draws on Verhoeven and Ihlen (2015) who argue that research is not only intended for administrative use at the organisational level, but also serves to supplement administrative perspectives with an approach that allows society to step back and evaluate the dynamics of societal and political influence. Ihlen and Verhoeven's theory draws on elements of the critical theorist's approach which value reflexivity and critical thought (Craig, 1999) – two aspects of research that will be used as a counterpoint to the modernist intent of exploring mitigation strategies for the communication crisis that is Computational Propaganda. Mumby (1997) indicates that democracy is central to the communication ethic of critical theory. A critical approach is important when interrogating phenomena that have influenced or changed the political power dynamic.

While the modernist view will be used to explore functional ways in which Computational Propaganda may be mitigated, a lens of Critical modernism will balance the research, because it is critical, but not a complete rejection of modernism, instead it is a manner of questioning the mode of rationality that has come to be synonymous with the modernism (Mumby 1997).

Social media in the political context, suffers a tension between its ability to empower the disenfranchised, on one hand, and on the other hand, its ability to be used as a tool for mass misinformation, manipulation, and political meddling (Karolak, 2017). Therefore, my research is cognisant of the complex relation between communication, power, identity, society and systems of domination explored by critical modernism theorists (Deetz, 1992. Cited in Mumby, 1997).

Beyond research paradigms, this study aims to close a knowledge gap that has risen out of the difference between the prevailing technological, political and communication context, versus existing theory. On one hand, political brands exist in the communication context of web 2.0, where communication can be shared on social media platforms at great reach and speed.

They also find themselves in a technological context wherein bad actors are automating social media bots to disseminate propaganda en masse in order to damage political brands. Furthermore, there is little to no regulation of social media platforms, ultimately putting political brands at risk of brand damage.

On the other hand, existing theory indicates that brand building is important to political parties, while Computational Propaganda has a propensity to create communications crises, which negatively affect brand equity. Since private organisations have been employing brand risk mitigating strategies for some time, it is clear that political brands also need to deploy such strategies, and that we need to fill the knowledge gap on mitigation strategies. Platforms may not be willing to act on instances of Computational Propaganda, and bot agents may not be stopped, but political brands could try to manage perceptions of individuals coming into contact with Computational Propaganda by employing strategies employed by private organisations.

1.1.5 Research Methods

The research aims to conduct semi-structured interviews with eight social media managers to explore their opinions on brand risk mitigation strategies as a result of computational propaganda, followed by an interview with South African political party representatives to assess what mitigation strategies are in place for computational propaganda in the forthcoming 2019 National Elections. The proposed research is not only qualitative, but also exploratory as it serves to gain insights on how political party brands are reacting to risks of Computational Propaganda and then provide suggestions on how they may respond (Creswell 2014). The relatively unpredictable nature of social media and the new nature of Computational Propaganda mean that insufficient studies are available that allow an outcome to be predicted, hence the need for a non-prescriptive, exploratory approach to provide broad guidelines for dealing with Computational Propoganda.

1.1.6 Limitations of the study

There may be gaps in how literature reflects the manifestation of computational propaganda and how this exists in the South African context.

In addition to this, the nature of South African politics means the sample size of political party communications practitioners is small with only two parties potentially having any experience in dealing with computational propaganda.

A second limitation of this study is the emergent nature of computational propaganda, which means that some concepts presented in this study will evolve with time, ultimately affecting one's interpretation of the outcomes. One such example is the use of the terms misinformation and disinformation. During the research and data gathering phase of this study, the interchangeable use of misinformation and disinformation emerged as a common trend in the literature reviewed, resulting in this practice being taken up by the author. One such example is Sergey Sanovich's, 2017 paper investigating the role of bots in Russia. Sanovich's paper titled "Computational Propaganda in Russia: The Origins Of Digital Misinformation," has a citation recommendation within the same paper indicating that the title be cited as "Computational Propaganda in Russia: The Origins Of Digital Disinformation", despite the content only referencing misinformation (Sanovich, 2017). Wardle and Derakhshan (2018) attempt to delineate between the concepts by identifying intent as being the key differentiator between the two. In the UNESCO journalism education handbook titled "Journalism, Fake News & Disinformation," Wardle and Derakhshan (2018) propose that "Misinformation" is information that is false, disseminated by people who believe it to be true, whereas "Disinformation" is information that is false where people disseminating the information know it to be false. This matter should be taken into account when reviewing any content relating to Computational Propaganda, as even academics at the forefront of this research like Phillip Howard and Samuel Woolley have used the term misinformation to describe propaganda distributed by bots, which is an intentional action and ultimately disinformation.

Finally, the assumption of this study is that social media practitioners from the private sector lead social media best practice, but this does not necessarily mean they are equipped or have any experience in dealing with individuals who are ideologically motivated and intent on wilfully damaging brands. Given that the research aims to provide insights, the small sample size, unique context and use of the purposeful non-probability sampling method mean that the research may not be generalisable.

1.1.7 Outline of the Report

Chapter two provides context relating to political brands and how parallels can be drawn between political brands and commercial ones; it also outlines the nature of digital brand social media crises and crisis communication, followed by existing crisis communication risk mitigation strategies. Chapter three provides an in depth rationale pertaining to the research approach in conjunction to an outline of how the research within this report was undertaken. Chapter four sets out to uncover the findings gleaned from the primary research. Based on the findings recommendations for political parties are provided.

1.1.8 Conclusion

This chapter outlined the context of the research to be conducted, along with its relevance and the research lens through which the study will be viewed. The following chapters will delve into literature reviewed for the sake of the study, followed by the research methodology and data analysis. Finally the research will culminate in the findings and recommendations regarding of mitigation strategies for computational propaganda.

2 . Chapter 2

2.1 Literature Review

2.1.1 Introduction

This study aims to explore communication-based mitigation strategies that political parties can deploy when facing the threat of computational propaganda. Therefore, in this chapter, the literature on political parties as brands and digital brand risk is explored in order to investigate the nature of social media and crises that come as a result of it. Thereafter Computational Propaganda and existing risk mitigation strategies employed in communication will be outlined.

2.1.2 Political Parties as Brands

In order to understand the relevance of digital brand risk, the importance of brands to political parties is discussed. A brand can be defined as a name, term, sign, symbol or design intended to identify the goods and services of one seller, or group of sellers and to differentiate them from those of competitors (Keller, 2013). While the physical attributes of a brand are described in this definition, the all-encompassing nature of brands and the extent to which they influence marketing effectiveness is best outlined by Keller's (1993) model of Consumer-Based Brand Equity. Within this four step model, brand effectiveness is based on sentiment, and that brands can reach the ultimate goal of brand resonance by answering four questions in relation to the consumer, namely, (1) who is the brand, (2) what is the brand, (3) what is the brand's relevance in consumers' lives, and (4) how does the brand make the customer feel. Consumer-Based Brand Equity is defined as the differential effect brand knowledge has on consumer response to the marketing of the brand. Based on Keller's definition, Consumer-Based Brand Equity is a function of knowledge and experience over time. This knowledge and experience can either positively affect or negatively affect the customers' response to a brand. Ultimately, brands can allow an organisation to gain supporters and fend off attempts by competitors.

Keller (2013) suggests that a brand can improve customer's feelings towards products, improve repeat purchase and make competitors actions less effective.

Brands are not only trademarks or reputations, but also complex intangibles whose character emerges from a blend of attributes. If one considers the attributes of the Customer Brand Based Equity model one can surmise that building an organisation's brand is important for building relationships with consumers/audiences. Audiences as voters are also important to political parties, which Butler, Collins and Speed (2011) describe as the complex sum of three main parts which are party, person and policy. Pich, Armannsdottir and Spry (2018) argue that the application of corporate brand theory to the political arena has helped political parties to develop desired identities in order to create credible offerings to stakeholders. Therefore, political party brand management has begun to generate a return on investment from a reputational capital and social capital perspective. However, the brand can build or damage voters' trust, especially in the context of social media and crisis communication, because crises may erode loyalty amongst political party members and make organisations vulnerable to tactics of competing political entities.

The notion of political parties as brands has become a prominent area in the growing field of political marketing (Harris and Lock, 2010), which according to Lees-Marshment (2003) is a powerful way in which parties can foster deeper relationships with voters. Mensah (2017) indicates that the prominence of political branding has come about as a result of political convergence where parties are increasingly moving to the centre in order to focus on voters' needs, coupled with a decline in ideology politics. The ideology-centred politics is similar to the mostly outmoded practice of product and sales marketing, which serves customers based on what the organisation believes, is valued by the customer. Downer (2016) reinforces this assertion by indicating that the shift in politics to voter needs is akin to a shift towards the market-oriented marketing perspective where businesses research customer's needs and market their products or services according to these needs. Drawing on Keller's (1993) definition of brand equity, Downer (2016) further points out that the shift to viewing political parties as brands indicates a shift to an emphasis on a long term view on marketing decisions.

Ahmed, Lodhi and Ahmad (2017) also affirm the relevance of brands in the political context, arguing that brand management helps parties learn about voter preferences. Branding assists voters by providing benefits by which they are able to evaluate their political choices. O'Cass and Voola (2011) more directly point to the link between political

party and brand, arguing that party managers, politicians and members relate to their perception of their brand and how the brand links to a set of capabilities which set the party apart in the political arena.

Based on the above literature, it is clear that concepts of marketing and brand equity are easily imported into the political space, even though the brand literature does not account for religion, social class and social change, which in recent times have seen a resurgence of prominence within the political landscape, most especially as it pertains to the rise of right wing populism and religious extremism (Wood, Daley and Chivers, 2018). Mensah (2017) nevertheless argues that class, religion and social change are not any more significant than other interests and behaviours that are subject to influence

Given that brand equity is important to political parties, they are susceptible to the brand risk just as commercial brands are, so it is important to explore mitigating strategies against this phenomenon. The concept of social media and brand risk will be further explored in order to provide context into the nature of this phenomenon and to explore whether there is scope for potential mitigation strategies.

2.1.3 Web 2.0 and Social Media

According to Castells (2007) and Manovich (2009), two-way networked sociality arrived with the advent of web 2.0 during the turn of the millennium. Web 2.0 is often referred to as the successor to the “read only web”, or web 1.0 which existed from 1989 to 2005 (Choudhury, 2014) and was characterised by data posted to websites for users to simply view, read or download. During this period user contribution and feedback was not available to most internet users and websites on the internet resembled traditional mass communication platforms in terms of their one-to-many orientation (Mangalore and Shivalingaiah, 2014).

In contrast to the read only web, the read-write web, or web 2.0 as it is commonly referred to (Dougherty 2004), was built to harness the power of network effects (O’Reilly, 2006) and transitioned one-to-many communication into many-to-many communication. Choudhury (2014) argues that Web 2.0 facilitates participatory, collaborative, distributive practices, and has distinct, characteristic relationships to technology such as wikis,

podcasts, RSS feeds and Application programming interfaces (Mangalore and Shivalingaiah, 2014).

The advancement from web 1.0 to web 2.0, characterised by mass participation and openness, have played a critical part in the new political context in which Computational Propaganda has thrived. Social media networks are at the centre of the new political context, since they allow for interactivity where participants can send, receive and process content, thus levelling the playing field such that users can give each other feedback in realtime, instead of just consuming mass media (Aula, 2010). Carr and Hayes (2015) describe social media as internet-based channels of mass-personal communication, facilitating perceptions and interactions among users. Their definition touches on social media's unique duality in that it can be personal and mass communication at the same time, while also allowing anyone to become a publisher. Social Media however, is not just the ability for users to provide immediate feedback; these networks are more than the sum of their parts and represent a new paradigm of openness, community and democracy.

Kaplan and Haenlein (2010) further illustrate the collaborative power of social media that has risen out of web 2.0, arguing that social media networks are internet applications which build on the ideological and technological foundation of web 2.0, thus allowing creation and exchange of user generated content. Key to this web 2.0 ideology, as well as the creation and exchange of user-generated content are levels of openness amongst different social media platforms. Deng, Fang, Monod and Qi (2018) distinguish between three levels of social media openness, i.e. (1) open platforms such as Twitter by default allow any users to connect without permission and see and share content posted; (2) semi-open platforms such as Instagram allows users to primarily engage only with the followers they select; and (3) closed networks such as Facebook which require users' permission before connections are made. The importance of openness is critical to the study of Computational Propaganda as this directly impacts on how easy or difficult it is to identify Computational Propaganda. According to Kramer (2017) Twitter's openness allows developers to access its Application programming interface, which in turn allows network analysis of connections between accounts. By contrast, Facebook's closed nature does not allow for network analysis and therefore it is more difficult to uncover and expose Computational Propaganda.

While the perks of relationship technologies include collaboration and participation at no cost to the end user, the pitfalls of web 2.0 and social media include less control by its users and reduced data security since these platforms increase the flow of personal information onto the networks where data is hosted and controlled (Grabner-Kräuter, 2009). Data vulnerability and its effects are further compounded by the monetisation models used by large social networks like Facebook, Instagram and Twitter. These social networks allow users to access content and worldwide networks at no cost, but due to the cost-intensive nature of the infrastructure to run these networks, social networks are monetized by using their depth of freely acquired user data and selling it as audiences to advertisers. This monetization model has turned social networks into “defacto data brokers, who go about aggregating data on users for the purpose of implementing powerful advertising platforms” (Venkatadri *et al.*, 2018, p. 89). Krishnamurthy, Willis and Naryshkin (2009) point out that mainstream social media sites, when used on default, have great potential for data leakages. Venkatandri *et al.* (2018) corroborate this assertion, explaining that social media networks have been a vector for privacy attacks due to bad actors that are able to predict an individual’s attributes based on small pieces of users information which are easily acquired online. An illustration of this scenario can be found in Facebook’s recent instances of data leakages wherein the world’s largest social network by daily users fell victim to manipulation by bad actors (Facebook, 2018). The most prominent instance being 2018’s Cambridge Analytica scandal, where researchers violated Facebook’s terms of service by gathering 87 million users’ personal data (Wagner, 2018) which was acquired via friends who had completed a quiz application (Cadwalladr and Graham-Harrison, 2018). These records were subsequently used to develop psychographic profiles of users in order to deliver specific pro-Donald Trump adverts to them (Meredith, 2018).

E-proponents have long argued that Web 2.0 platforms such as social media have the potential to reconnect citizens with governments and open up new civic spaces online (Ward, 2017). This argument is in line with Kaplan and Haelein’s (2010) definition of Web 2.0 which highlights the ability for users to create content, help set the agenda and, ultimately, create a shift in power. Social media use in the Arab spring (Salih 2013) and the resultant revolutionary wave, which helped to rearrange power relations in the North African, and Middle Eastern region (Tudoroiu, 2014) are a testament to social media’s ability to open up civic spaces online. However, Kaplan and Haenlein’s thoughts are in stark contrast to traditional management scholars who possess a modernistic worldview

like Anshul, Pathak, Safiullah and Singh (2017) who believe that social media is a form of digital media that provides political marketers with a marketplace where they compete to drive public opinion in a desired direction, ultimately suggesting that political marketing is still a discipline in which narratives can be controlled .

The initial rise of web 2.0 technologies led scholars to believe that social networks gave a communication platform to the general public, ultimately dis-intermediating traditional communications organisations and handing power over to users (Rust and Oliver, 1994). However, consensus is changing as knowledge regarding how social media users' data is being used increases. Although users of social media have helped to "transform everything from political arrangements to business models, organisations and philosophies" (Fitzpatrick, 2012), the power has actually shifted from social media users to social media platforms that are now able to influence their users' perceptions through the power of their data and algorithms, which were initially developed to benefit advertisers. Martin (2018, p. 30) succinctly touches on this paradigm in the MIT Technology Review, arguing that "Facebook, Google and Amazon all have business models that require them to scoop up large amounts of data about people to power their algorithms, and they derive their power from this information". The power of social media platforms create tension for political parties trying to set the agenda in that these traditional arbiters of power are pitted against a society that has relatively more control and has grown increasingly sceptical of the political elite's motives. However the tension is layered on top of social media platforms whose algorithms have potential to influence users and invariably set the agenda (Unver, 2017), especially when they are manipulated by bad actors, all of which pose potential threats for political party brands. A larger question, which falls outside the ambit of this research, is the intention versus business model debate, which asks if social media platforms are deliberately facilitating negative political messaging to maximise user engagement and thus increase revenue; this business model invariably leads to more extreme emotional messaging on social networks (Unver, 2017).

2.1.4 Digital Brand Risk

Hofman and Simeon (2013) define brand risk as any element that can diminish total brand value. They also indicate that this destruction can take on many guises by pointing out that brand risk ranges from malicious attacks to self-inflicted action, both of which affect brand value negatively.

Patrick Marrinan, in an interview with GfK-Marketing Intelligence Review (Hupp, Robbins and Fournier, 2018), corroborates Hofman and Simeon's assertion by indicating that Brand Risk is any event, condition or action that has potential to negatively affect a brand's value in the market. In creating their mathematical model of Brand Risk, Florea, Munteanu and Postoaca (2016) point out that consistent analysis of brand risk and brand profit are integral to the success of an organisation, as these are two of the most important indicators of brand equity, which in turn is a key but intangible attribute of any organisation.

While it is not possible to outline all brand risks, an exploration into nature of digital brand risk is imperative for the purpose of this study. In an outline of the nature of Digital Brand Risk, Hofman and Simeon (2013) borrow from David Abraham's (2007) Brand Risk model to delineate four areas of brand risk faced online, i.e. identity risks, nature of presence risks, equity risks, and reputation risks. Identity risks entail using a brand's trademark, usernames and domain names to take advantage of the high levels of traffic brands receive online. Presence risk is similar to identity risk and occurs when competitors take advantage of a brand's identity and attributes to attract potential buyers, only to sell their own competing products. Equity risks entail damage sustained to a brand when its functional and emotional benefits do not meet expectations of customers (Abrahams, 2007). Hofman and Simeon suggest that equity risks can have the most detrimental impact on brands as emotional connections take time to cultivate and are not easily regained (Hofman and Simeon, 2013). The fourth and final brand risk is that of reputation when a brand does not deliver according to expectations and falls short of legal or ethical requirements.

Reputational and equity risks are two of the most detrimental risks for any organisation because reputation and equity take extremely long to build, which is why they have become targets of attack by actors in the political space in recent years (Hofman and Simeon, 2013). Theory pertaining to brand risk, unfortunately, does not explore the nature of sabotage by external actors. This shortfall is however covered by the theory of brand destruction (Bokor, 2014), which is the seizure of power by consumers. Although communicating on social media lends itself to self-inflicted communication crises, the phenomenon of brand destruction is described by Bokor (2014, p. 40) as "the intentional destruction of a brand by a gatekeeper, opinion leader, consumer group or internet users, and may come as a result of conflicting worldviews or a conflict with a brand". Bokor builds on research conducted by Krishnamurthy and Kucuk (2009) who investigated the rapid

growth of anti-branding websites, which came as a result of growing customer influence initiated by the advent of the internet. Kucuk and Krishnamurthy (2009, p. 1120) explain that “[a]nti-brand web sites are online spaces that focus negative attention on a specific targeted brand. Such sites use visual expression, memorable domain names, and critical language to create a negative online identity for the targeted brand”.

They further argue that anti-branding differs from complaint behaviour because complaint behaviour attempts to improve or affect change in future business transactions, whereas anti-branding aims to create a negative brand image with no intention of future transactions (Krishnamurthy and Kucuk, 2009). Kucuk’s other research postulates that brands attract anti-brand behaviour based on the level of brand equity they attain, he also goes on to put forth response strategies to anti-brand behaviour based on a brand’s level of equity (Kucuk, 2008). Kucuk’s typology thus points to the type of mitigation strategies, even when dealing with bad actors that seek no resolution, that could be relevant to how political parties address Computation Propoganda, and the bots-as-bad-actors. While there is a growing amount of research relating to anti-branding from a website perspective, Bokor’s wider reaching Brand Destruction on social media theory has not gained significant traction, most likely because attacks by customers or the general public is considered to fall within the ambit of crisis communication. Kucuk (2008) shows that the literature often obscures the difference between anti-branding and complaint or evaluation platforms. The issue with this however is that existing crisis communication theory does not take into account the vindictive actions of competitors, or other automated bad actors who generate firestorms with no intention of achieving resolution or enacting a behavioural change.

2.1.5 Computational Propaganda

Researchers at the forefront of Computational Propaganda research and founders of Oxford’s Computational Propaganda Project, Samuel Woolley and Philip Howard, have undertaken a two-year project to analyse social media platforms, national security incidents and political crises around the globe. The ground-breaking, extensive research into Computational Propaganda has led them to define it as: “[t]he use of algorithms, automation and human curation to purposefully distribute misleading information over social media networks” (Woolley and Howard, 2017).

Given that Computational Propaganda research is still in its infancy, researchers worldwide have cooperated to form the Computational Propaganda Project and hence opposing perspectives are not yet prominent. However, the literature does cover some different perspectives on the use of algorithms, automation and human curation, which are key elements within Computational Propaganda.

2.1.5.1 Algorithmic filtering

Research undertaken by We Are Social indicates that the world's population of three billion social media users spend up to three hours and 57 minutes a day on social media (We Are Social, 2018). While one dimension of this stickiness relates to our ability to connect to the content and people closest to us (Mosseri, 2018). The other dimension of this stickiness comes as a result of algorithms designed to keep users engaged on platforms, by serving tailored content and adverts based on user interests. Early Facebook investor and advisor to Mark Zuckerberg, Roger McNamee (2018) crystalizes this assertion by indicating that these algorithms have allowed social media platforms to commoditise user attention to the extent that the technology community often refer to advertisers as social media's true customers, while social media users are referred to as the product. For this reason, Howard (2018) suggests that social media's ubiquity, coupled with users' ability to voraciously consume content, creates an ideal target for political operators to manipulate and deceive, especially when taking into account the highly automated nature of newsfeed algorithms and their predisposition for serving users with tailored, engaging content, which is sometimes inflammatory, and often emotive and polarizing (Brady *et al.*, 2017).

In "Gatekeeping Algorithms with Human Ethical Bias", Dr Martijn Van Otterlo (2018) draws on Eli Pariser's work which investigates the rise of internet filters that narrow the amount of information we see based on preferences (Pariser, 2011). Van Otterlo (2018) indicates that algorithms have the potential to create filter bubbles which can reinforce people's biases; conversely, he also indicates that disallowing some content may be seen as a form of censorship given the size of Facebook's more than 1.7 billion active users. Ciampaglia (2017) is a little more nuanced in his assessment of algorithmic filtering and points out that biases are a natural element of social behaviour and to exist in a world with limited attention spans, social media platforms need to tune their algorithms for engagement and popularity signals. He does however acknowledge that algorithmic bias coupled with the 'homophilistic' structure of social networks are a cause for concern given their potential to

create echo chambers. Finally, he indicates that solutions for filter bubbles are a moving target for computational social scientists due to the fact that social media platforms are continuously tuning their algorithms.

The concern related to filter bubbles is in stark contrast to the future envisioned by scholars such as Professor Yochai Benkler (2006) who, during the rise of Web 2.0, theorised about a future “networked information economy” where platforms like Wikipedia would bring about the democratisation of information due to the rise of user generated content and social production or decentralised, consensus based information. Akin Unver (2017) reinforces this idealistic notion by pointing out that the rise of digital connectedness was supposed to do good for democracy by helping to give representation to disenfranchised segments of the population.

One might argue that Yochai Benkler's idealistic prediction was made before the rise of platforms like Facebook, which, due to the sheer number of its user base, is viewed in developing countries as the internet itself (Mirani, 2015). Benkler's prediction also assumes that the internet simply connects people, whereas Howard, Woolley and Calo (2018, p. 81) believe this is not the case because the web 2.0 internet connects people through a layer of technology or “an interface, platform, or network which someone has designed”. They further argue that algorithms may be prone to reinforce the biases of their creators.

Unver (2017) agrees with Howard, Woolley and Calo's (2018) assertion, arguing that algorithms have created polarisation and confusion within online communities through the oversupply of information. These concerns are a central tenet to the study of algorithmic bias (Garcia-Gathright, Springer and Cramer, 2018), but it also points to how algorithms can assist in the ‘weaponisation’ (Ahmed, Kuchler and Garrahan, 2018) of social media.

In contrast to the popular critiques around algorithms, Messing and Westwood (2014) question the growing apprehension towards algorithmic filtering. They argue that selective exposure was inherent in watching television, reading the newspaper and consuming web 1.0, and this reduced the public's exposure to ‘counterattitudinal’ content well before algorithms gained prominence. Messing and Westwood (2014) go further to indicate that social media users, with their connections to colleagues, friends, family and acquaintances, are more likely to come into contact with diverse political views and

opinions. Most importantly, their research suggests that social sharing of political articles act as social endorsement, because more people with diverse views read it since social endorsements are a stronger predictor of news selection than news source. Flaxman, Goel and Rao (2016) subsequently conducted research using browsing data to investigate the veracity of both the filter bubble and social endorsement theory. They found a higher ideological segregation amongst articles discovered via social media channels, however, they also found that the websites visited were associated with high exposure to direct visitors with opposing perspectives, ultimately finding in favour of both sides of the debate.

Algorithmic filtering remains an area of great debate within both the computational social science and technological arena (Ciampaglia, 2017). Unfortunately, scientists' ability to come to a definitive understanding of its effects may not be feasible given that these algorithms are proprietary, change constantly, and form a critical part of social networks' revenue generation models (Hosanagar and Jair, 2018). For this reason, how these algorithms work and their effects may remain hidden under a veil of secrecy.

2.1.5.2 Automation

According to Woolley and Howard (2017), bots are automated programs integral to the spread of Computational Propaganda and are built to perform simple, repetitive, robotic tasks rapidly. Due to their wide-ranging abilities, bots have been used successfully to spread misinformation. However, Anstead, Carr, Halford, Murthy, Powell, Tinati and Weal (2016, p. 4955) view bots as a "subcategory of algorithmic media elements, because they are programmed to intervene in the way knowledge and information is communicated". Combining these two positions, Unver (2017) suggests that bots and algorithmically-generated search results can operate in tandem to disrupt the flow of information with incorrect or old information.

Ultimately these theoretical perspectives indicate that bot nets and algorithmic filtering have worked hand-in-hand to spread misinformation on social networks due to the bot's ability quickly disseminate inflammatory content widely so users can engage. Engagement ultimately leads to more users seeing the content as a result of how social network algorithms were designed. While the 2016 American presidential election was a watershed

moment which saw the evolution of Computational Propaganda techniques (Howard, 2018), automation in the form of bots have long been identified as an early tool for the spread of misinformation on social media. The earliest documented large-scale instance originated in Russia when 14 million tweets targeting Ukrainian citizens were published by 1.3 million fake accounts between February 2014 and December 2015 (Woolley and Howard, 2017).

Phillip Howard (2018) outlines five tactics employed by bot nets to achieve nefarious political ends on social media. The first tactic is termed Zombie Electioneering, which is the use of bots to give the appearance of wide support for a political candidate by automated commenting, scripted dialogue and other means. The second method, termed astroturfing is the technique of making an electoral campaign appear to originate from a grassroots effort, appearing to have public consensus where there is none. Third is hashtag jacking, which is the practise of appropriating a candidate's hashtag to distribute spam and undermine support. Retweet storms are the fourth commonly used tactic which entails simultaneously reposting or retweeting posts or tweets by hundreds or thousands of other bots. The last tactic employed is strategic flagging, which is the use of bots to flag legitimate content as inappropriate, which can lead to erroneous deletion by social media platforms (Howard, 2018) .

Automated bot networks have become a popular weapon in the Computational Propaganda arsenal. Ciampaglia (2017) points out that social bots, despite being responsible for the spread of large amounts of misinformation, can be employed to positive ends. Howard and Kollanyi (2016) reinforce this notion by pointing out that bots can perform tasks that range from legitimate actions like sharing news, updating feeds, responding to customer queries, and fact checking, which suggests that good bots can be deployed in the fight against misinformation. As reassuring as this suggestion might be, empirical research conducted by Murthy *et al.* (2016) points out that creating and deploying bots effectively requires technological, social, economic, and temporal capital, which suggests that only people, institutions or organisations with large financial resources are able to implement successful fact-checking or counter propaganda campaigns using automation.

2.1.5.3 Curation

According to Santini et al. (2018) bots are the most widely investigated manipulation agents when it comes to computational propaganda, but trolls who curate and propagate content can also be used to create noise. Research conducted by Oxford's Computational Propaganda project indicates that social media curation by trolls formed a fundamental part of Russia's Internet Research Agency's misinformation attacks during the 2016 US Presidential election (Francois, Ganesh, Howard, Kelly and Liotsiou, 2018). A key finding of the research, which drew on Facebook, Twitter, YouTube and Instagram data between 2015 and 2017, is that a total of 195 032 content pieces were posted on these platforms, and resulted in more than thirty million shares, thirty eight million likes, and three million comments (Francois, Ganesh, Howard, Kelly and Liotsiou, 2018).

These posts, which were made to appear as being posted by concerned American citizens, received exponentially more traction than misinformation adverts and bot propagated content run at the same time (Salinas, 2018). The difference between this campaign and regular bot networks was that some posts referred to Russian troll farms with messages of denial, while other accounts complained about the various social media platforms' political biases when faced with the prospect of being suspended. These dynamic responses to common complaints about bots made the trolling appear to be more authentic and effective due to being operated by humans (Howard *et al.*, 2018).

In a summary of worldwide computational propaganda events which was compiled by Oxford's Computational Propaganda project, Woolley and Howard point out that some of the most powerful forms of computational propaganda involve the coupling of algorithmic distribution and human curation (Woolley and Howard, 2017). The findings of Francois, Ganesh, Howard, Kelly and Liotsiou's 2018 report reinforce this assertion by pointing out that the success of the Russian's organic campaign came as a result of Russian's Internet Research Agency's use of click farms and their fluency in American trolling culture. Santini *et al.* (2018) indicate that there is a growing trend of combining human action, big data, and automation to refine the application of Computational Propaganda. The level of sophistication due to dynamism inherent with having humans curate content suggests that

a single technological, legal or platform-based measure is not enough to reduce the effects of computational propaganda, but a multi-disciplinary approach may be required.

2.1.6 Online Reputation Management

The interactive collaborative nature of web 2.0 has created an environment where a brands' meaning is no longer what corporate organisations say they are, but are rather a negotiated construct between brand users and the creators of these brands (Ligas and Cotte, 1999). In *Managing Online User Brand Risk*, Verwey and Muir (2014) make mention of web-based power struggles between marketers and consumers who challenge accepted branding truths and paradigms, which has given rise to the discipline of Online Reputation Management, more commonly known as ORM. By definition, Online Reputation Management is the practice of monitoring media, detecting relevant contents, analysing what people say about an entity and if necessary, interacting with customers (Amigo, Artiles, Gonzalo, Spina, Liu and Corujo, 2010). Coupled to this definition, Amigo et al. (2010) point out that negative comments in online media can seriously harm organisations and therefore ORM has become increasingly important. Portmann (2012) takes the basis of the Amigo et al. definition and provides a more succinct and proactive definition for online reputation management; he points out that online reputation management is not only the task of monitoring but also addressing or rectifying undesirable or negative search engine results pages, or mentions on social media. According Cerebra, one of South Africa's leading social media management agencies, in the South African context Online Reputation Management is a two-stage process where the task of monitoring, detecting and analysing content falls within the ambit of the social media analyst function, while the job of addressing, interacting and responding falls under the responsibility of the community manager (Beale, 2012). Cottica, Melançon and Renoust (2017) outline the importance and dynamism inherent in community management by indicating that successful online communities employ professionals sometimes called community managers or moderators who mediate conflict, police unwanted behaviour, and influence emergent social dynamics because online communities encompass interactions by many individuals.

These definitions and descriptions suggest that community managers are often on the front lines, defending and protecting brand equity when organisations face brand risk situations on social networks and online communications channels. Syme (2014) corroborates this and goes on to show that individuals managing social media for brands are required to be communications professionals, with creative sensibilities and backgrounds in marketing. Syme (2014) also points out the ability to recognise the warning signs of a crisis, create triage responses, respond in brand voice, understand crisis cycles and operate under pressure as being key abilities of social media or community managers. Ultimately, the contributions of Syme (2014), Cottica, Melançon and Renoust (2017), Beale (2012), Portmann (2012) and Amigo et al. (2010) indicates the insight, skill and value social media community managers can bring to political brands when dealing with crises that arise as a result of Computational Propaganda.

2.1.7 Risk Mitigation Strategies

Taking Bokor's (2014) assertion "that brand destruction is the intentional destruction of a brand by internet users" into account, one can view computational propaganda as a form of brand destruction through the use of algorithms and automation. Given that Computational Propaganda can create communication crises, it may be possible to use existing crisis communication strategies to deal with Computational Propaganda, which is the premise of this study.

A number of risk mitigation strategies exist in communications at the moment that may act a basis for which to respond to brand risk and Computational Propaganda. Hirschman's (Hirschman, 1970) work on public choice theory titled "Exit, Voice and Loyalty" provides a basis for understanding stakeholders' perceptions and encourages maintaining a dialogue with disgruntled stakeholders as this is good for the organisation's defensive marketing efforts. Singh's Dissatisfaction Response Theory (Singh, 1990) builds on Hirschman's theory and brings into focus how different individuals will react in situations where a brand falls short of expectations.

The Dissatisfaction Response Styles Theory indicates certain levels of dissatisfaction can be positive, but it also allows us to focus on the stakeholders that are willing to go to great lengths to tarnish brands. (Coombs, 2007) puts forth that a crisis can be defined as a

sudden and unexpected event that serves to disrupt organisational operations, ultimately posing both financial and reputational threats. Coombs (2007) further notes that crisis communication begins with attending to concerns of stakeholders from a physical and psychological perspective, an assertion that highlights the importance of managing perceptions.

Coombs reinforces Benoit's (1995) notion by describing crises as socially constructed situations. The key take away from these theories is that it is not facts, but stakeholders' interpretations that matter in a crisis and that these interpretations should be managed depending on context (Coombs, 2014). Coomb's Situational Crisis Communication Theory (SCCT), a framework that determines how organisations should respond in times of crisis, has become a seminal work in the crisis communication field; scholars have adapted SCCT for application in web 2.0 contexts, giving rise to the Blog Mediated Crisis Communications model (BMCC) and the Social Mediated Crisis Communication model (SMCC) (Cheng, 2018). Coombs' SCCT and the subsequent SMCC model posited by Liu, Austin and Jin (2011) may mean that while a brand may not want to give credence to fake news by engaging the agents of Computational Propaganda, it may want to assess the perceptions of its followers that come into contact with this propaganda and take action (Timothy Coombs and Jean Holladay, 2014).

While existing crisis communications strategies have merit, they do not account for web 2.0 and the inherent speed, reach, impact and complexity of crisis communications in a connected world (Veil, Buehner and Palenchar, 2011). This gap has given rise to the concept of online reputation management, which entails assessing stakeholder sentiment, identifying discourses and detecting online communication threats (Steenkamp and Rensburg, 2016). Online communication threats are said to differ from communications crises of old as they are characterised by high volumes of negative word of mouth, disseminated with extreme speed, often with intense indignation and no specific criticism (Pfeffer, Zorbach and Carley, 2014). Aula (2010) argues that the interactive nature of social media dictates that participation and continuous efforts to create shared meaning is encouraged during crises. Aula (2010) further states that the unique nature of social media crises will result in a general shift from a world of careful planning and strategy, to one of continuous uncertainty and risks.

2.1.8 Conclusion

The outlined environment and existing academic theory means that positive brand equity can help ensure the long-term survival of political organisations. However, the unpredictable nature of social media coupled with computational propaganda can expose gaps in existing crisis communication practises because they have a basis in theory conceptualised in a time before web 2.0.



3 . Chapter 3

3.1 Research Methodology

3.1.1 Introduction

This chapter discusses the methods with which to explore mitigation strategies for Computational Propaganda. Firstly the research approach and rationale will be outlined, followed by a description of the sampling strategy; thereafter the method of data collection and analysis will be provided. The chapter will close with ethical considerations and trustworthiness of interviews conducted to explore mitigation strategies for computational propaganda.

3.1.2 Research Approach

Given that this research serves to explore mitigation strategies for political brands that may face Computational Propaganda, it is important to note that although brand value is a quantifiable concept, the equity of a brand is often based on subjective concepts like judging, feeling and resonance (Keller 2013). As a result, the extent to which Computational Propaganda affects a brand in this context cannot be quantified by numerical analysis, nor can the effects of mitigating factors. The subjective nature of this topic means that the research relies on qualitative data based on the opinions of experienced respondents in order to maintain credibility.

According to Creswell (2014) researchers use the qualitative method to probe a topic when variables and base theory are unknown. Flick (2015) reinforces this notion by indicating that qualitative research is less focused on testing what is known, and instead aims to discover new aspects. According to Garner, Kawulich and Wagner (2012) qualitative research is concerned with understanding the process, social and cultural contexts which shape various behavioural patterns, it strives to create a coherent story as seen through the eyes of those who are part of the story. In order to do this, qualitative research seeks insights through structured in-depth analysis that is mainly interpretive and subjective (Garner, Kawulich and Wagner, 2012).

Creswell references Janice Morse when outlining additional criteria for using a qualitative research design; Morse (2011) indicates that a qualitative approach is best employed when (1) there is a lack of theory relating to a concept, (2) existing theory may be inappropriate, (3) there is a need to explore a phenomenon, or (4) when the nature of the phenomenon is not suited to a quantitative approach or cannot be quantified. To this end, the phenomenon of Computational Propaganda is a relatively new, which invariably fulfils one area of Morse's criteria, i.e. the lack of theory on the concept. The intention to explore strategies, which can mitigate computational propaganda's effects, dictates that the research undertaken was exploratory and thus qualitative. This research report gathered insights on how some of South Africa's most experienced social media managers tackle social media crises that arise as a result of Computational Propaganda by gathering their opinions on the subject matter. The research approach drew on these social media managers' experience, context, skills and perspectives in order to explore the mitigation strategies political parties could implement when facing the threat of Computational Propaganda.

3.1.3 Sampling Strategy

3.1.3.1 Sample Population

Harper, Laws and Marcus (2007) define sampling as the process of selecting respondents within a population, whereas Alvi (2016) defines a population as being all the members who meet particular criterion for specified investigation. According to Flick (2015), qualitative researchers select participants purposively and integrate small numbers of cases based on their relevance, because qualitative research aims to grasp subjective meanings of issues from participants' perspectives. It also brings latent meanings of situations into focus so the practises and lives of participants are known. For this reason, the researcher is not required to produce a statistical representative sample as one would when conducting quantitative research. Therefore, large sample sizes are not as critical to qualitative research as they are to quantitative methods.

Given the sequential nature of the research, this study drew on two sample populations: the first sample population drew upon social media managers in South Africa, while the second sample population drew on political party representatives operating in the communications functions of their organisations. Within both these sample populations, people have different backgrounds with varying levels of expertise, so a clearly defined sample is necessary.

3.1.3.2 The Sample

The research sample was selected using the purposive, non-probability method wherein a population of social media practitioners and political party representatives were drawn upon and sampled for in-depth interviews (Creswell 2014). Purposive, non-probability in this instance indicates that respondents who were selected to participate in the primary research, were selected intentionally using substitute criteria such as work experience and areas of expertise within their field of work, and due to this, only certain members of the population have been selected to take part in the research (Wagner, Kawulich and Garner, 2012). Initially, the intent was to interview political party agents, and then based upon their insights, approach social media managers for guidance on how to mitigate against Computational Propaganda. Unfortunately, due to unavailability of political party agents, the opposite occurred.

For the first stage of research the purposive, non-probability approach was taken to select eight social media professionals for in-depth interviews (Creswell, 2014). The required sample were social media professionals that have had five year's social media experience in addition to experience managing social media accounts of brands represented in Ornico's (2017) African Brand Index, which ranks the top 20 best performing brands on social media. Within this ranking system, broadcasters, banks, telecommunications and automotive industries received the most representation, which may be a result of these industry's high levels of engagement, large follower sizes and high user involvement. The respondents were selected using a snowball sample in which members of a social media manager's forum were asked to refer social media managers who had experience working on the telecommunications, bank, broadcast and automotive brands in the Africa Brand Index list. The rationale behind selecting social media managers who have experience from working on South Africa's twenty best brands according to Ornico's 2017 Africa Brand Index was based on the notion that the private sector has led innovation at the

intersection of brand equity and social media, and is likely to have the most relevant insights for political brands facing crises in the space. Large private sector brands with large followings are also more likely to have encountered different types of complaint or hostile behaviour, which may further assist their political counterparts.

The second sample of respondents were also arrived upon by using the purposive, non-probability approach. While the initial sample included political party agents responsible for managing social media at four of South Africa's largest political parties, only two parties agreed to participate, ultimately this sample was reduced to one due to availability problems.

To this end, the research sample for political parties is the Head of Communications in the Gauteng branch of South Africa's largest political party, the ANC. This communications officer who actively manages the social media account of the party in the Gauteng offered insights on how the ANC was dealing with computational propaganda during these in-depth interviews. South Africa's largest party (Parliamentary Monitoring Group, 2014) is relevant to the research because incumbent parties are most susceptible to being victims of computational propaganda based on trends from global Computational Propaganda research (Woolley and Howard, 2017).

3.1.4 Data Collection

In-depth interviews were selected as the method of data collection in this research study. According to Boyce and Neale (2006), in-depth interviews are a qualitative research technique which entails conducting intensive individual interviews with a small number of respondents in order to explore new issues in depth. These interviews were conducted face-to-face using nine supervisor approved semi-structured interview questions for the social media managers and six supervisor approved semi-structured interview questions for the political party's Head of Communications. Cohen (2006) indicates that semi-structured interviews allow the researcher to follow topical trajectories that may stray from interview guides if the researcher determines it to be appropriate. In *Mastering the Semi-Structured Interview and Beyond*, Anne Galletta (2013) touches on the strengths of semi-structured interviews by pointing out that they can help attend to complexity and phenomena in need of contextualisation. In addition, Galletta notes that semi-structured

interviews are sufficiently structured to address specific dimensions of the research question, while leaving space for participants to offer new meanings to the topic of study.

The pitfalls of semi-structured interviews are numerous and the ability to mitigate against these pitfalls is highly dependent on the skills of the individuals conducting the interviews. Creswell (2014) indicates that the results of in-depth interviews can be negatively impacted by the researcher's presence, which may bias responses; alternatively, data captured may be adversely affected by the researcher's inability to encourage articulation on the part of the respondent. Galletta (2014) suggests it is important that the researcher pays attention to the respondent's narrative as it unfolds. Furthermore, the researcher must guide respondents with further inquiry while refraining from leading respondents, which is ultimately an extremely delicate balance. Respondents of this research study were interviewed in neutral public environments; interviews were recorded on two devices, while field notes were taken to note respondent's interactions. Great care was taken to extract unique perspectives that may have arisen as a result of answers to initial questions, without leading respondents to desired answers.

3.1.5 Data Analysis

A number of methods can be used to analyse data collected. Woods and Gaber (2016) correctly point out that selecting procedures that best meet the philosophic orientation of the research is the responsibility of the researcher. However, the researcher must ensure methodological rigour regardless of the approach taken. Marshall and Rossman (1999) define data analysis as a process of ordering, structuring and providing meaning to a mass of collected data. Miles, Huberman and Saldaña's (2014) approach to content analysis of qualitative data, which entails data reduction, data display, verification and coding was chosen as a method to analyse the output of the interviews with the social media managers. Content analysis is the procedure for analysing textual material of whatever origin, it aims to classify the content of texts by categorizing statements, sentences or words (Flick, 2015). Creswell (2014) indicates that the intent behind content analysis is to make sense out of text and data, which involves segmenting and taking data apart.

Elo and Kyngäs (2008) indicate that there are two distinct approaches to content analysis, where theory exists, a deductive approach is taken, whereas an inductive approach is taken when research is exploratory. The inductive approach focuses on specific units of analysis, which are later combined into larger segments or categories.

According to Flick (2015), when using the inductive approach the content analysis method follows four distinct phases. The first phase entails transcribing and summarising the content, summarising allows one to omit unimportant or redundant passages. This phase is commonly known as the reduction phase. The second phase termed coding, entails assigning a code to each recurring subject matter. Coding is essentially a way of grouping concepts in categories in order to uncover themes. The third phase entails classifying or indexing subject matter under themes outlined in phase two. The fourth phase entails presenting the themes in a manner that answers the research question.

Finally, once the themes from semi-structured interviews were identified, these were overlaid with responses from the political party communications officer in order to assess existing gaps in the political party's approach and suggest mitigation strategies that may be employed by them.

Although great care was taken to collect and analyse data correctly, one pitfall of the research conducted was that data collection and analysis occurred separately. Separating the data collection from the data analysis process means that the research conducted does not benefit from collecting new data to fill in gaps or test new hypotheses that emerge during analysis (Miles, Huberman and Saldaña, 2014). Miles, Huberman and Saldaña (2014) suggest a process of concurrent data collection and analysis, which allows the researcher to think about existing data and creating strategies for collecting new and better data.

3.1.6 Ethics

Beyond the written consent required by interviewees, the sensitive nature of politics within the South African context dictates that it is necessary to represent political party representatives and social media managers as anonymous, in keeping with their rights to

privacy in accordance with points 11.1 and 11.2 of the University of Johannesburg code of academic and research ethics (2007).

An ethical consideration that significantly affects the study's validity is the ability to test the efficacy of computational risk mitigation strategies proposed by social media practitioners. It is not possible to test mitigation strategies without engaging in Computational Propaganda itself, which contains an element of misinformation. Doing so may have damaging effects on individuals that come across it, so this was not done, in accordance with point 5.3.2 of the University of Johannesburg's academic code of conduct (2007)

3.1.7 Trustworthiness

In order for research to be persuasive and trustworthy it's important to show that the methods and conclusions of the research are credible, transferable, dependable and confirmable. Guba (1981). According to Guba (1981), credibility in the context of qualitative research refers to the truth-value of a study and the confidence one can have in the truth of the research findings, whereas confirmability relates to objectivity or neutrality in undertaking the research. Both credibility and confirmability were attained through the triangulation of sources (Turner and Turner, 1970), wherein two different populations were interviewed. In addition to this, respondents with different perspectives were interviewed individually, over different periods of time, in a variety of settings.

Guber (1981) indicates that two other elements of quality research is the ability for academics to transfer findings to other contexts and consistently coming to a similar conclusion if research is repeated through stable measurement. These two concepts are described as transferability and dependability respectively. The dependability of this study was ensured by an auditable trail of data starting with an interview schedule and recordings of social media managers and political communications officers based on supervisor approved interview questions. These recordings were referred back to the respondents after the interviews for their approvals. The respondents subsequently signed research consent forms and following this, interviews were thematically coded at both stages of the research undertaking.

3.1.8 Limitations of the Study

There may be gaps in how literature reflects the manifestation of Computational Propaganda and how this exists in the South African context. In addition to this, the nature of South African politics means the sample size from political party's is small given that only one political party agent availed themselves to provide insights into how they deal Computational Propaganda. The assumption of this study is that social media practitioners from the private sector lead social media best practice, although private sector brands are often recognised for their excellence, it does not necessarily mean they are equipped or have any experience in dealing with individuals who are ideologically motivated and intent on wilfully damaging brands.

Furthermore, the unfortunate deviation from the original research design means the interviews conducted with the social media managers do not benefit from the context created by the interview with the political party's representative. Despite this, it is important to note that the political party agent's responses were captured without their knowledge of the social media manager's answers. Any alignment or correlation between the social media manager's responses and those of the political party representative indicates that the political party is engaging in some positive practices.

In addition to the limitations illustrated above, the data collection and analysis phases were done one after the other, which present a problem from a research optimisation perspective. According to Miles, Huberman and Saldaña (2014), the data collection from the data analysis process means that the research conducted does not benefit from collecting new data to fill in gaps or test new hypotheses that emerge during analysis. Given that the research aims to provide insights, the small sample size, unique context and use of the purposeful non-probability sampling method mean that the research may not be generalisable.

4 . Chapter 4

4.1 Exploring mitigation strategies for computational propaganda

4.1.1 Introduction

The research data codified in the following passages originate from eight interviews conducted with social media managers who have experience operating in a wide range of industries from telecommunications, banking, broadcasting, automotive, petrochemicals, retail, and airlines. The respondents surveyed all have a minimum five years of social media working experience, having operated as hands-on community managers and subsequently played strategic roles leading social media teams. This selection ensures respondents have the right balance of hands-on experience attending to comments, queries, complaints and crises; mixed with the ability and experience from operating at strategic levels on the social media accounts of South Africa's biggest brands.

In order to attain a wide range of perspectives, social media managers who work both for corporates and agencies were interviewed. According to Mike Stopforth, founder of Cerebra, one of South Africa's most awarded social media agencies, outsourcing corporate social media is a short term solution (Mike Stopforth, 2014) and over the long term, corporates should insource this function. Recently, insourcing has become a trend amongst large organisations and has led the rise of the social media community management function taken internally. While social media agencies have long operated at the cutting edge of social media management, it is important to incorporate perspectives of those managing social media accounts within organisations, because political parties may be taking the same approach due to the sensitive nature of their work. To that end, three respondents represented internal corporate-based social media teams, while five respondents were agency-based. Job titles amongst respondents surveyed include, Social Media Account Director, Group Online Media Manager, Head of Social Media, Social Media Director, Social Media Strategist, Digital Social Media Content Manager, Social Content Lead, and Social Media Brand Manager.

After the interviews were conducted they were transcribed for analysis, which entailed outlining common themes and ascribing codes to these themes.

The data was then organised and displayed according to each respondent's answers so as to illustrate patterns, the rationale being that commonalities in responses might present possible mitigation strategies that political parties can further explore and bring light to important issues that should be considered when coming into contact with computational propaganda. What follows is a code matrix showing main themes uncovered in interviews.

Interview Code Matrix

Question	Respondents							
	R1	R2	R3	R4	R5	R6	R7	R8
1								
2	ACCS,ORM OBJ	OBJ, ORM	OBJ, ORM, BRAND	ORM	ORM, ACCS, OBJ	ORM, OBJ	ORM,	OBJ, STRAT, ENGA, SMMC, ACSC, ORM
3	RSK, PRACT	RSK	RSK	RSK	RSK	RSK		
4	BRAND, ITCM, PRACT, SMMC	INTCOM, PRACT	SMMC, INTCOM	SMMC, INTCOM, ACCS, ENGA	PRACT,	SMMC, ENGA, PRACT,	INTCOM, PRACT	INTCOM, PRACT
5	STRAT, BRAND, SMMC, CALM		BRAND, CALM, SMMC. OBJ	BRAND, ACCS, ENGA	ACCS, CALM, OBJ, BRAND	BRAND, ORM, ALFIL, STRAT	BRAND, SMMC, CALM	STRAT, SMMC, OBJ,BRAND, CALM
6	AUTO	AUTO	ENGA	AUTO, ALFIL	BRAND	AUTO	AUTO	AUTO, ENGA
7	CALM	CALM, BRAND	CALM, BRAND	PRACT, BRAND, CALM		PRACT	ALFIL	ALFIL, INTCOM, PRACT
8	INTCOM, BRAND	INTCOM, BRAND	INTCOM	SMMC, PRACT	SMMC	PRACT, SMMC, BRAND, INTCOM	INTCOM, CALM, BRAND	CALM, INTCOM

9	ENGA	ENGA	ALFIL	ENGA, CENS	CENS	CENS	ENGA	ENGA
---	------	------	-------	---------------	------	------	------	------

The table below provides descriptions to the codes contained in the matrix above.

Code Matrix Descriptions

Code	Description
ACCS	Accessibility: Ability for users to openly engage political parties
ALF	Algorithmic Filtering: Algorithms that filter information served to social media users based on their interests or what users are most likely to engage with.
AUTO	Automation: Use of digital technology to perform repetitive tasks, commonly used to refer to bots.
BRAND	Brand Identity: Brand image, tone, personality, logo and graphics. Elements by which brands are commonly identified.
CENS	Censorship: Suppression of communication
CALM	Communication Alignment: Similar policy-based messaging from all members of a political organisation
RSK	Digital Brand Risk: Any element that can diminish total brand value online.
INTCM	Integrated Communication: Communicating the same message across media channels in channel-relevant way.
ORM	Online Reputation Management: Detecting and analysing content then interacting online with consumers based on this analysis.
OBJ	Operational Objectives: Objectives that concern the day-to-day social media management.
PRAC	Proactive Communication: Proactive engagement with customers via social media.
SMMC	Social Media Crisis Communication: The process of responding to crises on social media with the intention of de-escalating such crises.

ENGA	Social Media Engagement
STRAT	Strategy: Long-term plan social media plan intended to reach a specific aim.

What follows is a discussion of the research data based on the themes presented, this will be contrasted against responses received from a regional head of communications from South Africa's largest political party. The main themes arising from the semi-structured interviews centred around issues of Brand Identity, Communications Alignment, Communication Integration, Social Mediated Online Reputation Management. Ancillary themes centred around Engagement, Algorithmic filtering and Censorship versus Freedom of Speech; while the ancillary themes did not feature prominently there were deemed important to include given the framework of critical modernism that has been employed for this study.

The interviews with social media managers revealed a strong interplay amongst certain themes, so for the purpose of coherence, the themes uncovered in the content analysis have been grouped as follows.

Preventative measures:

- Brand Identity
- Communication Alignment

Defensive measures:

- Online Reputation Management
- Communication Integration

Contextual Considerations:

- Algorithmic filtering and engagement
- Freedom of speech and censorship.

4.1.2 Preventative Measures

The overarching commonality between respondents was that they worked in general to prevent communications crises. These themes relate to measures political parties can put in place to help prevent or reduce the likelihood that they fall victim to social media crises in general or as a result of Computational Propaganda.

4.1.2.1 Issues of brand identity

In most of the interviews conducted with social media managers, the most prominent theme related to a focus on brand identity, and how political parties can import stringent brand management (Ahmed, Lodhi and Ahmad, 2017) practices from the private sector in order to improve their social media impact and protect political brands in communications crises'.

As a starting point, it was acknowledged that the principles of brand management on social media apply to political parties in the same way they do to corporates, as pointed out by respondent 6 (R6): *"... they [political parties] are a brand with a reputation that they need to build and protect. ... the things that we do as social media managers relate to protecting brands and creating brand affinity with our audience and at the end of the day that is what a political party is, they want to create brand affinity with an audience so that audience can vote for them."*

Respondent 1 (R1) essentially affirms the relevance of brands in the political context as postulated by Ahmed, Lodhi and Ahmad (2017). Respondent 3 (R3) brings a little more detail to Respondent 6's example by pointing out how corporates use brand based tools to enact effective social media management: *"I think to be honest many people say it's supposed to be strategic and high level, for me the most important things are really the basics, so for example, a brand tone and a good moderation plan. So when I speak to you is your approach to reply or not say anything, what kind of plan do you have in place for negative and positive experiences?"* Further to this, three respondents noted that the Economic Freedom Fighters (EFF) are one of the best parties at effectively at managing their brand. They went further to point out that this effectiveness has extended into social media, to the point that their single-minded message has rallied like-minded individuals around their cause.

To this end, Respondent 7 (R7) says: *“If you go online, be consistent, have a message and stand by it. If you respond to every troll, you’ll never get to why people should think you’re interesting and vote for you. ... With the EFF next year it’s going to be land and every EFF person in this country, the only thing they will say is we want the land, you can say what you want until you’re blue in the face.”*

Respondent 1 (R1) confirms Respondent 7’s (R7) assessment: *“Have a strategy that speaks back to your values, stick to your guns on social media, if you’re argumentative be that, don’t change because you’re on social media, they [EFF] act on social media just as they do in parliament.”*

Another theme linked to brand identity is related to how political parties can use their brands as a bulwark against attacks. Regarding this, one respondent (R4) noted: *“Although political organisations do have a level of branding, I do think it’s not as heavily invested in from a protection perspective.”*

Brand management in the context of protection, is the notion that continuous investment in brand identity, and how stringent adherence to good branding principles can give political brands the ability to passively defend against attacks or communications crisis. By ensuring good brand management, political parties help social media audiences identify that they are potentially dealing with misinformation, because the content they see from bad actors does not fit with their brand’s values. Alternatively, good brand management can help audiences recognise that a piece of fake content does not originate from the brand it is purported to be from because the content does not fit the organisation’s corporate identity.

Respondent 5, (R5) affirms this idea with her illustration on the power of good brand governance wherein she points out how a social media account she manages experienced an account hack. Her team were quickly alerted to the hack by fans of the brand because the messages and comments published by their account were not in accordance with the

brand's established tone: *"We were getting a lot of messages from fans saying, guys what's wrong, what's going on, your tone of voice is off, everything is wrong."*

Respondent 2 (R2) reinforces the power of good brand practice by suggesting this allows parties to be selective in what misinformation they attend to. Respondent 2 does so by pointing out that internet users have become savvy and are able to identify unsophisticated computational propaganda: *"Internet users are becoming savvy to fakes and frauds. They notice if logos aren't correct and even grammatical errors."*

Respondent 7 (R7) verifies Respondent 2's (R2) take on this change: *"What I've seen in the last few years is the general social media population wising up to identifying fake accounts and we tend not to react as quickly."*

Respondent 5 reinforces the idea that strong brands can be selective in their responses to social crises as a result of brand power and an acknowledgment that a response can be risky because it has potential to bring more attention to the crisis or misinformation: *"You need to look at your monitoring tools to decide if something is worth responding to. You've got to look at it like minority versus the majority of stuff, sometimes stuff might have a small spike and then die out ...otherwise you risk bringing more eyeballs."*

Respondent 6 however, indicates that some political parties, specifically the EFF, have managed to implement branding principles successfully to the extent that they do not need to defend themselves in times of crisis. Respondent 6 is the fourth person in our sample of eight to positively reference the EFF's use of social media:

I'm not sure if it's the result of the party's strategy or if it's a result of the community, but they [the EFF] have built a strong brand on Twitter to the point that if you say something negative, there is this EFF Twitter army that will defend them.

In contrast to Respondent 6's glowing assessment, Respondent 1 suggests that the EFF's loyal following may not be the result of good brand practices, but rather the use of Computational Propaganda. Respondent 1 alludes to this in their response to whether they are familiar with communications crises that have been initiated by bot networks or fake

accounts: *“Whenever someone tweets something negative about the EFF, there’s a flurry of tweets defending them. There is also an increase in social media accounts with partially incorrect black names that are tweeting against the EFF. There’s a lot of that right now, another thing is we’re headed to election year next year.”*

Respondent 1’s assessment is ratified by research conducted by Superlinear and Daily Maverick (Haffajee, 2019), which suggests the EFF has engaged in four ‘disinformation campaigns’ to date. The data, which was collected over the course of three years, uses network analysis to indicate the EFF has been able to mobilise vast networks of Twitter users to shape narratives around Pravin Gordhan, VBS Mutual Bank, Eskom and the SARS Rogue Unit. In two instances, this social media activity spilled over to traditional media. A point of contention however, is whether bot networks, or human curation initiated these disinformation campaigns.

The respondent’s identification of the EFF as having good social media capabilities coupled with evidence of their Computational Propaganda activities suggest that Computational Propaganda is more sophisticated than the respondents think, and that some of our respondent’s suggestions, may not be effective mitigation strategies due to not having an appreciation of Computational Propaganda’s sophistication. Despite this potential flaw, it’s important to point out that the concept of brand identity being an important defence mechanism against crises and misinformation is in line with Timothy Coombs’ (2007) Situational Crisis Communication Model outlined in Chapter 1. The Situational Crisis Communication Model takes the contextual nature of an organisation’s reputational threat into account before suggesting response strategies. According to Coombs, one of the key aspects affecting an organisation’s ability to respond to a threat is the organisations reputation or brand equity at the time of crisis.

Interestingly, the political party respondent was in close alignment to social media managers on the importance of upholding stringent brand management practises in order to mitigate against the effects of fake news. The respondent indicates that the biggest threat to political parties and media in general is fake news: *“Anybody can create content and anybody can publish content, so the security of content is not really, well there is no security of content really, because of that you have to build your reputation and*

credibility. Branding and imagery, PR, your image management becomes very important so that people know by looking they can pick up what is fake and what is not, I think we're getting better at it."

The ANC Respondent nevertheless acknowledged that improvement should be made in this regard. In terms of consistency in brand tone, the respondent indicates that the party has noted the interactive value of social media, so great effort is made to ensure consistency before any content is published or announcements are made: *"We've had to adapt the way in which we communicate because it's quick and because it's immediate, everything has got to go at the same time to everybody. So the way we package our communication is to be able to prepare adequately for responses to possible issues that may come up in whatever we raise."*

With that being said, the respondent also gives an indication that the party also aim to play to the strengths of social media, which is its interactivity, suggesting that an overemphasis on playing it safe in order to mitigate against brand risk may prevent the party from achieving its goals: *"In Gauteng we have the highest population of the country concentrated in the smallest area space and the majority of those are young people, so if you really want to reach citizens and interact with them and have meaningful public participation at government level, you've got to use social media"*.

The respondent further argues: *"As head of communications portfolio in the province my role and responsibility in the party is what we call the battle of ideas, which is to discuss and engage with society on critical issues and political discourse both internally and externally, both in the government and party, the goal is to interact with society."*

The respondent raises an important consideration for political parties about the balance between well planned and produced content that conforms with corporate identity, versus ephemeral content which is growing in popularity amongst the youth. Ephemeral content is raw in-the-moment social media content that disappears within 24 hours (Sheetrit, 2017), it serves to communicate authenticity and capture real live situations, taking the form of live broadcasts on Facebook and Instagram or short video stories on Facebook, Instagram,

SnapChat and WhatsApp. Ephemeral content has been identified as an increasingly effective way to connect and engage with millennial social media users (Andrews, 2018), which makes striking a balance an important consideration.

4.1.2.2 Communications Alignment

The second prominent theme uncovered in the content analysis related to communication alignment. More specifically, it focuses on how disparate messaging negatively impacts political party brands' social media efforts, and puts these political parties in a position of vulnerability. Respondent 8 (R8) touches lightly on communication alignment with reference to brand, indicating that documented processes are important for governance and communication alignment: *"A social media playbook and guide is so important, it shows individuals how they show up online. In corporate, you don't have a problem where employees speak for brands unless they're CEOs, in political parties there are individual representatives too."*

Respondent 3 (R3) points out that alignment can act as a defence mechanism, ultimately closing gaps that may open political organisations up to misinformation and false narratives: *"What we need to do is ensure consistency around that truth, authenticity as well as an unyielding commitment to living out that truth...a brand has to ensure that all platforms and touch points have a level of consistency, so if someone does believe something about your brand, you can prove them wrong."*

Respondent 1 (R1) further reinforces the importance of alignment, while pointing out the potential pitfalls that come with not having the correct procedures in place. *"Parties like the ANC will have one area of the organisation tweet something that's totally out of step with what the entire organisation is saying. It's important to have checks and balances. Also don't have random accounts, the ANC has dormant accounts that aren't being used, they have accounts that are just existing, which ultimately become easy pickings for hackers."*

Respondent 4 also touches on how hackers and impersonators can aid in the spread of misinformation by referring to a recent crisis at the Global Citizen Festival, wherein criminals targeted concert goers *en masse*. Respondent 4 alleges that the communications crisis the South African Police Service (SAPS) dealt with was exacerbated by a parody account that was impersonating the South African Minister of Police. *“We see today for example the Global Citizen concert that happened on Sunday and the subsequent problems that ensued at various locations including service stations, there was a parody account for the Commissioner of Police Bheki Cele, and that parody account was leaving comments and people were thinking that this was the official minister.”*

Hackers are not the only worry for non-aligned political organisations on social media, according to two respondents, political party community managers and representatives risk being baited into emotive exchanges, leaving themselves at odds with their party’s communication objectives. This type of misalignment ultimately creates more opportunities for bad actors to capture these exchanges and use them for nefarious purposes. Respondent 3 (R3) touches on the potential for individuals to be baited into negative exchanges: *“It’s so important to have your themes and [content] pillars set out initially so your message is clear and you aren’t sort of tempted to sway and put your own view in, especially when it’s political.”*

Respondent 7 gives context to the importance of alignment amongst key political figures by providing some contextual examples. The respondent then proceeds to bolster the importance of alignment by providing perspective on its role in one of South Africa’s most impactful Computational Propaganda campaigns: *“It’s like the DA, there’s a guy in PE, Renaldo Gouws, his individual views are always clear, but they don’t always align with the DA’s views or policies...You need a core party strategy and then to think of a strategy and a process for individuals as well ... I think the Gupta campaign was so hard to defuse because there was a definite golden thread, and message that ran through all of it. As the media, rival political parties and citizens, we were fighting all these individuals, but that campaign definitely had a singular golden thread.”*

Although Respondent 7 touches on the effectiveness of a Computational Propaganda campaign, the respondent inadvertently reinforces the argument for succinct brand identity coupled with message alignment which are two key constructs of integrated marketing communication, which according to Baalen and Mulder (2016) enables companies to integrate promotional mix elements with elements of brand so as to create a unified message.

When describing the social media operating structure of the ANC, the political party respondent went to great lengths to indicate that the party had well-defined approval structures with a centralised communication function at the center: *“The use of official accounts for content and centralising communications has helped, so in the ANC you have dedicated spokespersons. During elections it does get a bit blurred because of the amount of work that we do on a daily basis, but still the communication lines are quite defined in ANC. So in each structure there's a political head responsible for the content, so that's the office of the secretariat where it's the secretary their deputies and the spokespersons, so the three of us are responsible for everything that goes out. In terms of social media you would have people that create content whether its visual content it doesn't matter but it goes out on approval.”*

The respondent does however indicate there are instances in which unsanctioned messaging is published. This indication may point to merit in Respondent 3's assertion that those managing the accounts of political parties could risk being baited into negative exchanges due to an inability to separate one's own opinions from those of the party. The respondent does however indicate that in instances where this occurs, the party is quick to distance itself from such views: *“Where you may have seen, or when it [the approval process] doesn't happen and political principals haven't approved it, then we're quick to say that this is staff of the organisation or whatever. It does create a bit of a PR mess sometimes but we do disown PR content that's not approved.”*

The respondent goes further to indicate that the party also has issues of alignment between individual party brands and the political party brand as indicated by Respondents 7 and 3: *“Another threat is the blurred lines of party position versus personal views. So an*

official of the party would say something, which is his personal views, which he has a right to do, but, if they straddle into areas of policy it becomes really difficult, so that's always a threat. It's not possible to... we do have communications protocol, it's in black and white it's approved, everybody has them, but you're not always able to police human behaviour. At the end of it you find yourself always having to put out fires or reminding people what they can and can't do. I think another threat especially for an organisation is when internal mechanisms are not as effective as they should be, you then find members turning to social media to express frustrations and irritations.”

While approval processes do exist within the party, social media is fast paced, and for an organisation aiming to engage with youth on its platforms, consideration should be given to process behind reactive engagements on social media where exchanges are rapid and require quick thinking. Ultimately this candid response reinforces the importance of Respondent 3's suggestion that political parties set out content pillars and clear policy indicating response do's and don'ts when staff respond from official party accounts. In terms of individual versus party views, it may be beneficial to either enforce disciplinary measures or delineate what party representatives can include in their social media biography, such as party affiliations, this is a practice that is common in the private sector. That being said, political parties do not operate in a vacuum, robust opinions, ideas and debate are core to the arena in which politicians operate. So while there may be merit in suggestions from social media managers who suggest individual communication policies be implemented, they provide this advice without having an appreciation that debate and discourse is a key performance indicator for the political party's social media team.

The data gathered from social media managers and the political party respondent indicate that good brand management practices like adherence to corporate identity and communication consistency can help reduce the risk of Computational Propaganda. For the ANC at least, this seems to be an area of focus, and may apply to other political parties. Unfortunately, a focus on brand identity and alignment of messaging across political party brands can only assist to minimise the effects of Computational Propaganda in very specific instances, such as instances of misinformation as a result of impersonation of accounts or political parties. Other instances relate to when inflammatory content is shared and made to look as if it originates from a particular party. While the measure

outlined may be effective against these forms of misinformation, they are but two ways of combatting Computational Propaganda so that those who come into contact with it are not affected by it. The following passages look at respondents' suggestions on how to actively deal with the spread of misinformation as a social media manager.

4.1.3 Defensive Measures

The common characteristic of themes within the defensive measures cluster is that they are a step beyond the passive solutions offered by the social media managers, and entail methods in which to actively react and manage communication crises that arise as a result of computational propaganda. These measures, when assessed, ostensibly draw on two areas in particular: online reputation management and integrated marketing communication.

4.1.3.1 Online Reputation Management

The first point of departure with regard to exploring mitigation strategies for social media is whether it is possible to mitigate against misinformation propagated by automation and algorithms by changing the perceptions of those who have come into contact with it. The general consensus, from six of eight respondents is that this is possible, however, doing so would be extremely difficult and would require a multidisciplinary approach. The foundation of any multidisciplinary approach would be online reputation management. As indicated in Chapter One, online reputation management is the process of monitoring media, detecting relevant contents, analysing what people say about an entity and if necessary, interacting with customers (Amigo, Artiles, Gonzalo, Spina, Liu and Corujo, 2010).

Respondent 1's answer on how a social media crisis should be handled aligns perfectly with the online reputation process espoused by Amigo et al (2010): *"The first thing about a crisis is don't assume what a crisis is, get to the crux of it, what is the issue? Secondly, check where the sentiment is and where most of the complaints are coming from, then acknowledge the issue, but don't ignore while investigating, really do investigate,*

communicate it and get to the crux of whatever the crisis could be. In that process keep updating people as to where you are in it.”

While respondents have their own methodologies that have been developed within their agencies and companies, their responses generally fall within the detect, analyse, interact process, however when asked how they would recommend political parties actively mitigate against crises brought as a result of misinformation campaigns initiated by bots and automation, respondents adapted the online reputation management process to a more multidisciplinary approach. Detection and analyses remained, but the third step varied.

Respondent three explains the detection aspect: *“The hardest thing is people can create accounts whether its bots or not, especially with bots faster than you can shut things down, so I think in that case the easiest way is to be on really high alert and have all your alerts set up so that you get sort of pinged immediately as soon as a bot, and you would know it’s a bot because they will probably spit out 20 tweets in two minutes.”*

Respondent 5 on the other hand, covers the analysis aspect: *“It’s important to first analyse volumes, data and sentiment, otherwise you risk bringing more eyeballs, another thing is influence, it could be one hundred people tweeting with no followership or one tweeting with a big followership of 100 000.”*

While not going into detail about the ANC’s online reputation management process, the political party respondent indicated that the ANC does engage in monitoring all media formats including social media: *“So we do have a monitoring system we monitor media as a whole and a big part of that is social media. So we monitor the reach, we monitor the interactions, we monitor the negative, and the positive and we monitor the issues that come up as people engage. When there’s topical issues outside of election periods we monitor that as well.”*

The respondent goes on to indicate that the party has been able to identify bots because of the way they operate as soon the ANC account publishes content. The respondent had the following to say in response to how they identify bot attacks: *“It’s the way they operate, it’s immediate, they are issue based and they pick on certain things all the time, so it’s easy to identify.”*

Further to this, the political party respondent indicates that they, as someone who often posts and tweets on behalf of the ANC has been affected by bot campaigns: *“There’s quite a lot of them. There’s always a fight between big parties saying that the DA has a whole team of bots and they say the same thing about us. I mean it’s impossible to trace and police and that sort of thing so people do get away with a lot.”*

Continuing with the online reputation management process; following the analysis step, respondents deviated in their responses relating to what action should be taken thereafter. According to Respondent 1 the best method is to battle content with content: *“You need a strong strategy around your messaging. What content can you put out there to refute claims being made and use different avenues, partnerships and networks to help that message reach as many people as possible. Then also use a media strategy, take the fake news head on and create content that identifies and debunks it.”*

Respondent 7 focuses on the importance of having relationships with social media platforms in order to report bot networks and malicious accounts: *“I think a lot of it is know your enemy, know what you’re up against, if there are short term tactics, like if you come up to a Twitter bot network ... try and have relationships in place with the platforms so you can say, hey, we’ve come across these accounts and believe these accounts to be malicious.”*

Respondent 6 suggests notifying online communities of misinformation and having the organisations’ accounts verified. *“A simple thing to do is get all your accounts verified. Sort of like a nice technical thing is to you know, make sure that there’s no confusion ...*

continuously communicate to your audience and community that these are you official channels. These are our official accounts and if you see anything that looks untoward from other accounts it's fake ... just ignore it. It's very tricky because with social media there's equal power across the board, so the only thing you can do is communicate, we're official , this is not official."

In providing the above solution Respondent 1 inadvertently touches on a flaw inherent in the idea of social distribution of content that aims to debunk fake news on social media; social media by its very nature allows users to self-select, because of this it is difficult to assess who has come into contact with junk news if one wishes to give those people a different perspective.

Respondent 4 touches on this: *"I was doing an interview on Al Jazeera and the discussion was, is social media subjective or objective and I'm like by its very nature it's subjective because you self-select, because you're using the search parameters to look for what you want to look for, you see what you want to see and it's almost given a platform for like-minded individuals to find each other."*

Secondly, the only way to reach these individuals that come into contact with misinformation *en masse* would be via a paid promotion strategy, which may invariably raise skepticism (Yaylagul, 2018). Respondent 4 goes on to offer a unique insight into actively dealing with Computational Propaganda as a result of having their brand fall victim to bots during Bell Pottinger's White Monopoly Capital Computational Propaganda campaign (Khoza, 2018): *"We had a tax dispute with SARS last year which we won this year, basically SARS were saying we owed them R2 billion. What happened was, some of the WMC bots got hold of that and started pushing their narrative that we aren't playing [ball] with government, we're white monopoly capital, that became a thing and that spread on a bot network including a lots of websites like WMC exposed. What we did to counter that was just to be frank, go into traditional media, push it out as soon as possible and to also change your SEO strategy quite heavily to combat it."*

By including search engine optimisation as a tactic, Respondent 4's response outlines a possible approach toward dealing with Computational Propaganda as a result of automation and algorithms, the first and only response to do so. Search Engine Optimisation (SEO) can succinctly be described as the use of various techniques marketers and web developers use in order to make their websites rank higher on popular search engines (Matošević, 2019). SEO in this context entails targeting specific keywords so Respondent 4's brand messaging appears prominently in searches relating to white monopoly capital; this gives the respondent the opportunity to have their message read first, it also reduces the impact of Computational Propaganda by reducing the amount of traffic going to those sites. Respondent 4's response crystalizes the importance of a multidisciplinary approach to dealing with Computational Propaganda, an insight which will be explored further in the following passages.

Although the political party respondent acknowledges that the Computational Propaganda or fake news serves as a big threat to political parties they indicate that there are not any plans in place to deal with the matter despite being able to identify it. The respondent says the follow regarding defensive measures to deal with computational propaganda: *"I must say, not that I know of, if it's there it's top secret high level stuff, but I don't know anything about that. Yeah so I think everybody is struggling with it and I don't think anybody has got an absolute answer as to how to deal with them. As a party we don't have any relationships with the social networks, maybe as a state, but not as a party."*

4.1.3.2 Communication Integration

Integration of brand messages has become an important tenet of modern marketing communication as seen with the rise of Integrated Marketing Communication (IMC) during the late nineties and early two thousands. The central concept to IMC and subsequent, more strategic theories relating to communication integration, is that a single-minded message, across multiple media forms, is more impactful than disparate ones (Baalen and Mulder, 2016). This idea of integration is encapsulated by Bruhn's (2008, p. 17) definition of IMC which is:

“a process of analysis, planning, organization, implementation and monitoring that is oriented toward creating unity from diverse sources of internal and external communication with target groups to convey a consistent impression of the company or the company’s reference object”.

Subsequent theories of IMC and the more strategic IC have their basis in integration, a concept that the respondents of this study also identify as being important to combatting the effects of Computational Propaganda. The theme of integrating messages and using multiple channels to communicate to end-users was the fourth most popular theme to come out of the content analysis. Respondent 7 touches on this: *“You need to begin engaging with influencers on the platforms as well as media partners to try and mitigate and contain the matter by saying look, this is our side of things.”*

Respondent 6 warns against an over-reliance on social media suggesting that using other platforms such as websites can assist in turning the tide against Computational Propaganda: *“Another tactic that can be used is always refer back to a website, a credible web presence to reaffirm the credibility so say to your community, if this statement is not on our website, then its untrue... Don’t be too reliant on your social media presence.”*

Respondent 8 suggests doing the same, albeit more aggressively: *“What I would do to mitigate against misinformation if I were a political party, would be to bake the facts into every piece of communication that goes out and link an information portal at every turn.”*

Respondent 7 references KFC in the UK and their handling of supplier change which led to a stock outage, resulting in closed stores across the country and a trend for the #KFCCrisis hashtag (Topping, 2018). The respondent indicates that KFC turned the crisis into a positive by rolling out a print ad which swapped the words KFC to FCK, wittingly using its powerful brand name to admit failure and subsequently trending again and earning one billion impressions this time with positive sentiment (Griner, 2018): *“There’s room to use other channels, as digital people we rely on digital too much and forget the real value that a great print advert can do.”*

Respondent 1, shows the importance resolving crises in action and not just message, a practice which can ostensibly be carried out when debunking misinformation too: *“It’s*

important to take corrective action by linking back to what the company does so as to ensure it doesn't happen again. It shouldn't just play out on social media, social media is just another tool."

Integrating messages and delivering them across multiple forms of media like television, radio, print and coupling this with consistency has become a popular method for building brands. Based on the insights provided by the respondents, this may also be a viable approach for brands in terms of crisis, whether it be self-inflicted or the result of Computational Propaganda. The effectiveness of using multiple channels beyond social media to reduce the impact of Computational Propaganda is further reinforced when considering that algorithmic filtering is central to how social media platforms operate. What this means is that unique content is distributed to users based on their preferences, so information debunking fake news may never reach its intended end user.

In terms of communication integration the political party respondent indicates an appreciation for distributing a unified message: *"We still do rely heavily on traditional mediums ... Over the years we've had to be able to sort of adapt the way in which we engage, so it's almost got to be simultaneous. In the past we would just issue press statement and be interviewed we now do everything at once so when I issue a written statement I also do a video recording of the main thrust of this statement as I know society can engage with it or media would engage"*.

This appreciation for distributing a unified message across social media platforms indicates the ANC may be well positioned to take the social media managers' advice in using these channels to debunk misinformation.

A rebuttal to the use of other media channels to distribute information debunking fake news may be that some users, by nature of actively consuming fake news, aren't interested in information that may debunk their wrongly held beliefs, a point raised by respondent 8: *"I see something that supports my belief system, I don't want to hear a*

counter argument, then I want to share it with everyone else to show them I'm right. People really want to share things that prop themselves up. There may be instances where people have been able to nip things in the bud, but I think the only thing you can do is make all the information available and give a link to it like Snope, I think snope is amazing and I'm seeing more and more of it in threads where people are using it to debunk misinformation."

Clearly the discussion around algorithmic filtering and beliefs is nuanced, although this theme was present in the research, it surprisingly did not feature prominently. However, given that a critical modernism paradigm was chosen to underpin this research, it is important to unpack algorithmic filtering, censorship versus freedom and the power dynamics at play in computational propaganda, a look at these issues follows.

4.1.4 Contextual Considerations

4.1.4.1 Engagement and Algorithmic Filtering

As indicated in Chapter 1, an important premise of the research conducted relates to political parties having a plan in place to deal with Computational Propaganda. The rationale behind having a plan is that social media platforms may not be fast enough to respond to bad actors on social media. Additionally, the fast moving nature of social media allows bad actors to continuously find new loopholes to exploit. As Louise Matsakis (2019) explains, companies like Facebook continue to play "whack-a-mole" with agents of Computational Propaganda. Given these circumstances, my research proposed that political parties should use communication techniques as their first line of defence.

Because social media platforms value engagement to sell advertising, it is difficult for them to curb Computational Propaganda. The main drivers of engagement are algorithms, which are being exploited for the purposes of computational propaganda. When asked if social media platforms are doing enough to curb Computational Propaganda, respondent 2 indicated: *"No. They are for-profit companies for whom engagement trumps trust. 20k people fighting over a fake tweet is better for Twitter than hiring more team members to verify accounts."*

Respondent 8 paints an even more sceptical picture of Facebook. *“Facebook sells eyeballs, reach and frequency, if they have almost two billion people on Facebook and five hundred or six hundred million of them are fake, then it’s not in their best interest to tell you or to get rid of them, so they’re conflicted from a business interest point of view.”*

Respondent 1 echoes the sentiments of Respondents 2 and 8 but makes a fairer assessment by portraying the conundrum social media platforms find themselves in: *“Bots are odd. It’s good for social networks and bad for them. On one side it inflates their user numbers so advertisers approach them. Meanwhile they generate distrust towards the social networks. They’re not doing enough but they won’t do enough because it serves them not to.”*

Although it is easy blame social media platforms, Respondent 5 believes doing so is unfair, and that Facebook, Instagram and Twitter have removed or suspended malicious accounts in the past, provided users report them. The respondent goes on to point out that the sheer scale of these networks make it nearly impossible to stay up-to-date on how bad actors are manipulating their platforms: *“Their [Facebook’s] two-way communication is really good with that and they really come to the party, but it is up to the consumer. I don’t know if Facebook’s gonna know every single thing with what goes on with their millions of users, unless you bring it to the attention. It’s just not practical, you can’t police the internet.”*

Respondent 6 shares respondent 5’s sentiment: *“... social media is this contradiction because everyone has freedom of speech. In my mind I think there’s a limited amount of things that platforms can do because the more you do that the more you limit people’s right to freedom of speech. ... I think the responsibility lies with the consumer to figure out the real from the wrong.”*

Respondent's 5 and 6 responses touch on a critical debate taking place in the United Kingdom where Computational Propaganda and its effects have led the House of Lords to debate whether social media networks should be held to the same standards to which publishers are held. BBC journalist Amol Rajal (2016) describes Facebook's role from the perspective of publishers succinctly. "The world's biggest platform, increasingly, has the role once fulfilled by news publishers, without the legal restrictions and social obligations." If the UK parliament and publishers succeed with their efforts, platforms like Facebook and Twitter will be held responsible for "[f]ake news, extremist content, online bullying, harassment and copyright infringement that occurs on their platforms" (Brown, 2018).

4.1.4.2 Freedom of speech and censorship

Regulating the creation and spread of misinformation creates a conundrum for social media platforms, especially where users curate and distribute fake news, not out of malicious intent, but out of belief. UN Special Rapporteur on the Right to Freedom of Expression, Professor David Kaye (2018), notes that increased legislation may lead companies to over-regulate their platforms, thereby limiting space for debate, art, politics and other forms of expression. Such regulation could unintentionally galvanise unwitting arbiters of misinformation under the belief that they are being victimised as a result of hidden agendas. Respondent 8 provides a real world example of a similar scenario: "*The whole thing around infowars that helped galvanize the [Far] right against these platforms is because people were asking why are platforms censoring them and not doing the same on the left. There's always a gap between censorship and freedom of speech and it's really hard to find that line.*"

Respondent 8 also points out that political parties like the ANC, risk aiding censorship by reporting accounts they deem to be spreading misinformation. They go on to say that the final decision on whether to remove these reported accounts, should sit with the social media platforms.

4.1.4.3 Conclusion

Mitigating against Computational Propaganda is extremely complex, as noted in the research results. However, respondents in this study suggest that limiting risk is possible, even if there is no silver bullet for solving the problem. Instead, there are preventative measures and defensive measures political parties can take. The chosen route any political party takes must be done while taking social networks' bias for engagement and practices of algorithmic filtering into account. Furthermore, political parties must be cognisant of issues relating to freedom of speech and censorship as some of the suggested defensive measures entail having relationships with representatives at these social networks in order to report them. However, a close relationship may lead political parties to encourage censorship, especially if political parties are government incumbents.



5 . Chapter 5

5.1 Research Findings and Recommendations

The research conducted provides some interesting outcomes with regard to how political parties can tackle computational propaganda online. Social media managers from some of the country's pre-eminent social media teams provided insight into how they believe social media crises should be handled. They also gave insight into how they believe a crisis stemming from Computational Propaganda should be navigated, with Respondents having similar opinions on how to handle orthodox social media crises but divergent opinions on crises resulting from Computational Propaganda. Despite the divergence of opinion, all the social media managers agreed that addressing Computational Propaganda is a complex, nuanced, and multidisciplinary task.

The research provided some guidance on how political parties can try to mitigate against Computational Propaganda, covering four areas political parties can focus on, (1) brand identity; (2) communication alignment; (3) online reputation management ; and (4) communication integration.

The study also illustrates the power dynamics at play with regard to the phenomenon of Computational Propaganda. Events like the Arab Spring were celebrated as social network wins since they seemed to have facilitated a shift of power from incumbent governments to the disenfranchised masses, just as social networks shifted power away from brands and into the hands of consumers. However, events like the Gupta bots campaign and Cambridge Analytica scandals indicate that the same networks that facilitated a shift of power to the masses, have also unwittingly facilitated a power shift to rich and powerful bad actors who are able to mimic mass action with bots and algorithms. Both kinds of shifts in power result from social networks deciding who sees what, which then suggests that instead of shifting power from elites to the masses, power shifted from governments and traditional businesses to social networks. Political parties find themselves playing a balancing act in this context, as they have to navigate a landscape in which they need to appeal to the masses, while protecting themselves against bad actors, all while standing on the shifting sands of social media platforms that have become the world's most popular method of communication. Although this appears to be a daunting task, the research gathered indicates that doing this successfully is possible.

5.1.1 Findings as they Relate to the Research Aims and Objectives

At the outset of this study, the intended aim was to provide insight to political parties on how they could mitigate against malicious online brand attacks. In order to reach this goal, this study explored how Computational Propaganda manifests itself online, what strategies political parties are using to mitigate Computational Propaganda, and which digital brand risk mitigation strategies political brands can employ to mitigate the against consequences of computational propaganda. What follows are answers to these research objectives based on the data gathered.

1. How does computational propaganda manifest itself online?

The research focused specifically on bots as the most easily identifiable form of computational propaganda because the use of algorithms and curation is a lot more targeted and tied to users' beliefs and interests. Computational Propaganda using algorithmic filtering and curation are much harder to identify given their sophistication, as illustrated in the Cambridge Analytica scandal in which victims were only aware of the attack once a whistle-blower exposed Cambridge Analytica and further investigated which Facebook apps had been used (Hern, 2018).

The findings of this research indicate that bots manifest in a multitude of ways for a multitude of purposes, from bots that are used to leak news, to agenda-based bots that reply to specific subject matter, to wide sock-puppet networks popularised during the "white monopoly capital" leaks misinformation campaigns. All but one respondent indicated that they are familiar with bots and have personally come into contact with bots in their work. The research further revealed that other types of digital brand risk are also on the rise, from accounts imitating brands, to account hacks. Surprisingly, it also showed that respondents were aware of curation and algorithms as well as the censorship versus freedom of speech debate, which has inadvertently allowed these more sophisticated forms of computational propaganda to continue unabated.

2. What strategies are political parties using to mitigate computational propaganda risks?

Based on the research, the sample of one political party indicates that an effort is being made to ensure that stringent brand identity policies are being implemented in order to help users identify fake content that is made to look like it originates from the political party. In addition to this, great efforts are being made to ensure communication alignment between the party's various social media accounts and its staff to help users identify misinformation that is not in line with party policies. Unfortunately, although they make a good start, these mitigation strategies only account for specific instances of Computational Propaganda. Based on the interview with the political party respondent one can surmise a level of apathy in the battle of misinformation, but perhaps none of the South African misinformation campaigns were effective enough to warrant defensive action from the party, and this may change.

The political party respondent revealed that agencies are contracted during times of high political activity. These agencies help to manage accounts and may serve as a mitigation strategy in itself, given the systematic crisis communications processes all agency-based respondents employ. Finally, the research indicates that although there is an appreciation of the need to mitigate against Computational Propaganda, there is not a tangible appreciation of how to develop active defensive systems against it.

3. Which digital brand risk mitigation strategies can political brands employ to tackle the brand consequences of Computational Propaganda?

The research uncovered two types of strategies to help mitigate against the consequences of social media. Firstly, preventative measures were considered important. Preventative measures serve to reduce the likelihood of a crisis arising as a result of Computational Propaganda and include brand identity and communication alignment. Brand identity (Keller 2013) measures entail using stringent brand management practices on social media such as ensuring every piece of content abides to the political party's corporate identity rules. In other words the political party must use logos, correct tone of voice, correct language and only distribute content that aligns with the party's values. Communication alignment entails ensuring communication consistency on all media

platforms. For example, it suggests that individual representatives of political parties should not stray too far from the party's policy.

Secondly, defensive strategies were considered relevant; these require action from the political party's social media teams. Defensive strategies include online reputation management espoused by Amigo et al. (2010), which entails the detection, analysis and response to crises. Detection and analysis will help party's to determine what response should be implemented. Tied to response is communication integration as defined by Bruhn (2008), or the use of a wide range of media in a unified manner in order to overcome algorithmic filtering, which may limit the reach of the political party's reactive statement.

While engaging in these defensive measures, it is important for political party social media teams to take context into account. The context will determine the extent to which defensive measures are taken because political parties risk curtailing the freedom of speech of those it deems to be spreading misinformation. Alternatively keeping its messaging to social media platforms risks having only a few people see their reactive statements, additionally, large groups of loyal supporters may have no need for the party to debunk fake news because they trust the party. Therefore, depending on the context and nature of the crisis, political parties must consider media channels beyond social media.

The use of online reputation management and unifying one's message across multiple platforms is by no means new, but highlighting these two avenues as credible strategies which may help inspire political parties implement this low hanging fruit. General consensus amongst social media managers is that the best response to any communications crisis is to have a plan, even if it is not completely fool-proof, it reduces the likelihood of compounded the crisis as a result of inaction. Surprisingly, one potential mitigation strategy that did not emerge from the research is the use of bots and automation to assist in the fight against misinformation. The respondents acknowledged that bots are able to distribute messages widely at great speed, and for this reason it is possible to use bots to flag keywords relating to misinformation and either report them, or tweet to every user that responds to misinformation content, outlining why a piece of content is fake news. The potential reasons why this wasn't suggested may be due to cost, time and technology implications which the respondents may feel, fall out of political party's competency.

5.1.2 Recommendations for Future Research

The research conducted focused on Computational Propaganda and exploring mitigation strategies for political parties in online contexts, based on the outcomes and engagements with political parties. A critical area of research that can be conducted is the investigation into social media crises communications strategies political parties have in place as compared to those in the private sector. In conducting this research report it was found that the value of expertise provided by social media managers was rather limited, which may be a result of Computational Propaganda being a relatively new phenomenon, whereas an established subject like general crisis communication may lead to better transfer of insight on both ends.

In order to achieve this transfer of insight, the study would require a larger sample from political parties, a clear clarification on what constitutes a crisis, and specific scenarios to which the political party and private sector respondent can reply. Thereafter, brand risk mitigation strategies for Computational Propaganda can be revisited with a larger political party sample and specific Computational Propaganda scenarios.

5.1.3 Recommendations for Practice

Based on the research conducted, recommendations for political parties would be to firstly institute preventative measures such as improve party wide compliance to organisational brand identity on official social media accounts. In addition to this, an engagement protocol needs to be established outlining when and how the political party's staff are to respond in terms of reactive and continuous engagement. This protocol must also be contrasted with guidelines on when responses must be escalated for approval. In addition to this, it is advisable that every individual party representative use a playbook designed by the political party in order to guide their engagements. This playbook, while allowing individuals to engage in robust debate, should outline critical policy related subject matter that should not be engaged upon and rather be referred back to more official channels.

Secondly, in order to institute defensive measures, political parties must investigate the manner in which computational propaganda operates whether, be it via bots, curation or algorithms. Doing so will allow parties to identify new ways in which computational propaganda adapts or is manifesting. Following this, it is advised that political parties put in measures to detect increased or anomalous levels of computational propaganda activity, which they can analyse. With regard to analysis, parties need to determine what level of misinformation distribution is negligible, what level requires consistent monitoring and what level requires intervention. In terms of the intervention phase, there should be criteria determining what misinformation activities require a statement distributed on social media, versus what level of misinformation requires an integrated response across multiple media channels. These recommendations can serve as a foundation with which to tackle crises that arise as a result of computational propaganda.

5.1.4 Conclusion

Research indicates that computational propaganda is growing in prominence the world over and measures taken by countries like Italy and their online task team show the importance of dealing with this phenomenon. It is critical that South African political parties are cognisant of this as South Africa draws closer to the forthcoming National Elections. This research study was conducted in order to explore and bring possible mitigation strategies against computational propaganda to the attention of political parties.

Through a worldview of critical modernism (Mumby, 1997), this research explores potential mitigation strategies by using semi-structured interviews (Cohen D, 2006) with social media managers and a political party representative. These interviews were conducted using purposive non-probability sampling (Laws, Harper and Marcus, 2007).

Using thematic analysis (Flick, 2015), the study uncovered four different mitigation approaches, namely; (1) brand identity; (2) communication alignment; (3) online reputation management ; and (4) communication integration. In addition to this, the two contextual considerations of algorithmic filtering and engagement, as well as freedom of speech and censorship were uncovered. While the outcomes of the research may not be entirely groundbreaking, they do outline important areas on which political parties can focus.

References List

5.2 References

Aaker, J. and Chang, V. (2009) *Obama and the power of social media and technology*. Stanford.

Abouzied, R. (2011) *Tunisia: How Mohammed Bouazizi Sparked a Revolution - TIME, Time Magazine*. Available at: <http://content.time.com/time/magazine/article/0,9171,2044723,00.html> (Accessed: 3 November 2018).

Abrahams, D. (2007) *Brand Risk: Adding Risk Literacy To Brand Management*. First Edit. New York: Routledge.

Ahmed, M. A., Lodhi, S. A. and Ahmad, Z. (2017) 'Political Brand Equity Model: The Integration of Political Brands in Voter Choice Political Brand Equity Model: The Integration of Political Brands in Voter Choice', *Journal of Political Marketing*. Taylor & Francis, 16(2), pp. 147–179. doi: 10.1080/15377857.2015.1022629.

Ahmed, M., Kuchler, H. and Garrahan, M. (2018) *How digital footprints paved way to weaponising social media | Financial Times, The Financial Times*. Available at: <https://www.ft.com/content/f369e670-2ac3-11e8-9b4b-bc4b9f08f381> (Accessed: 29 June 2018).

Alvi, M. H. (2016) *A Manual for Selecting Sampling Techniques in Research*. Karachi.

Amigo, E. *et al.* (2010) 'WePS-3 evaluation campaign: Overview of the online reputation management task', in *CEUR Workshop Proceedings*.

ANCIR (2017) *How the Gupta campaign weaponised social media, Times Live*. Available at: <https://www.timeslive.co.za/news/south-africa/2017-09-04-how-the-gupta-campaign-weaponised-social-media/> (Accessed: 15 October 2017).

Andrews, L. (2018) *Why and how to add ephemeral content to your marketing strategy, Bizcommunity*. Available at: <https://www.bizcommunity.com/Article/196/669/175800.html> (Accessed: 4 January 2019).

Arnaudo, D. (2017) 'Computational Propaganda in Brazil: Social Bots during Elections',

pp. 1–39.

Aula, P. (2010) 'Social media , reputation risk and ambient publicity management', 38(6), pp. 43–49. doi: 10.1108/10878571011088069.

Baalen, A. Van and Mulder, D. (2016) *A CONCEPTUAL ANALYSIS OF INTEGRATED COMMUNICATION*.

BBC (2017) 'Woke' and 'post-truth' added to Oxford English Dictionary - BBC Newsbeat. Available at: <http://www.bbc.co.uk/newsbeat/article/40414375/woke-and-post-truth-added-to-oxford-english-dictionary> (Accessed: 21 October 2018).

Beale, J. (2012) *Demystifying Online Reputation Management - Cerebra, Cerebra.co.za*. Available at: <https://www.cerebra.co.za/blog/demystifying-online-reputation-management/> (Accessed: 5 January 2019).

Benkler, Y. (2006) *The Wealth Of Networks: How Social Production Transforms Market And Freedom*. New Haven and London: Yale University Press. Available at: <papers3://publication/uuid/41D6973D-C9DF-4664-9C7A-7DD50EC787B3>.

Benoit, W. (1995) *A Theory Of Image Restoration Strategies*. First edit. New York: University Of New York PR.

Bokor, T. (2014) 'More Than Words - Brand Destruction in the Online Sphere', *Vezetéstudomány/Budapest Management*, 45(2), pp. 40–45.

Boyce, C. and Neale, P. (2006) *A guide for designing and conducting in-depth interviews for evaluation input, Evaluation*. Massachussets. doi: 10.1080/14616730210154225.

Brady, W. J. *et al.* (2017) 'Emotion shapes the diffusion of moralized content in social networks', *Proceedings of the National Academy of Sciences*, 114(28), pp. 7313–7318. doi: 10.1073/pnas.1618923114.

Brown, T. (2018) *Social Media and Online Platforms as Publishers Debate on 11 January 2018*. London.

Bruhn, M. (2008) *Planning Integrated Marketing Communications*. Edited by H. Sievert and D. Bell. Gutersloh, Germany: Verlag Bertalman Stifting.

Butler, P., Collins, N. and Speed, R. (2011) 'The Europeanisation of the British political

marketplace', *Journal of Marketing Management*, 27(7–8), pp. 678–693. doi: 10.1080/0267257X.2011.593540.

Cadwalladr, C. and Graham-Harrison, E. (2018) *How Cambridge Analytica turned Facebook 'likes' into a lucrative political tool | Technology | The Guardian, The Guardian*. Available at: <https://www.theguardian.com/technology/2018/mar/17/facebook-cambridge-analytica-kogan-data-algorithm> (Accessed: 23 September 2018).

Carr, C. T. and Hayes, R. A. (2015) 'Social Media: Defining, Developing, and Divining', *Atlantic Journal of Communication*, 23(1), pp. 46–65. doi: 10.1080/15456870.2015.972282.

Carter, M. (2017) *Legal, disciplinary and reputational risks that stem from social media abuse | Namibia Economist, Namibia Economist*. Available at: <https://economist.com.na/24413/human-resources/legal-disciplinary-and-reputational-risks-that-stem-from-social-media-abuse/> (Accessed: 1 October 2017).

Cheng, Y. (2018) 'How Social Media Is Changing Crisis Communication Strategies: Evidence from the Updated Literature', *Journal of Contingencies and Crisis Management*, 26(1), pp. 58–68. doi: 10.1111/1468-5973.12130.

Choudhury, N. (2014) 'World Wide Web and Its Journey from Web 1 . 0 to Web 4.0', *International Journal of Computer Science and Information Technologies (IJCSIT)*, 5(6), pp. 8096–8100. doi: 10.1186/1471-2105-9-82.

Ciampaglia, G. L. (2017) 'Fighting fake news: a role for computational social science in the fight against digital misinformation', *Journal of Computational Social Science*. Springer Singapore, 1(1), pp. 147–153. doi: 10.1007/s42001-017-0005-6.

Cohen D, C. B. (2006) 'Semi-structured Interviews Recording Semi-Structured interviews', *Qualitative Research Guidelines Project*. doi: 10.1021/la503432x.

Coombs, W. T. (2007) 'Protecting Organisations Reputations During A Crisis: The Development and application of Situational Crisis Communication Theory.', *Corporate Reputation Review*, 10(3), pp. 166, 173.

Coombs, W. T. (2014) *Crisis Management and Communications, Institute for Public Relations*.

Cottica, A., Melançon, G. and Renoust, B. (2017) 'Online community management as social network design: testing for the signature of management activities in online communities', *Applied Network Science*. *Applied Network Science*, 2(1), p. 30. doi: 10.1007/s41109-017-0049-9.

Craig, R. T. (1999) 'Communication theory as a field', *Communication Theory*, 9(2), pp. 119–161. doi: 10.1111/j.1468-2885.1999.tb00355.x.

Creswell, J. W. (2014) *Research design: Qualitative, quantitative, and mixed method, Research design Qualitative quantitative and mixed methods approaches*. doi: 10.1007/s13398-014-0173-7.2.

Downer, L. (2016) 'It ' s the Equity Stupid ! Protecting the Value of the Partisan', 28(1), pp. 22–39.

Elo, S. and Kyngäs, H. (2008) 'The qualitative content analysis process', *Journal of Advanced Nursing*, 62(1), pp. 107–115. doi: 10.1111/j.1365-2648.2007.04569.x.

Facebook (2018) *Removing Bad Actors On Facebook*, *Facebook Newsroom*. doi: 10.1080/01402390.2014.977382.

Farand, C. (2017) *French social media awash with fake news stories from sources 'exposed to Russian influence' ahead of presidential election | The Independent, The Independent*. Available at: <https://www.independent.co.uk/news/world/europe/french-voters-deluge-fake-news-stories-facebook-twitter-russian-influence-days-before-election-a7696506.html> (Accessed: 22 October 2018).

Fitzpatrick, A. (2012) *Is Social Media Playing a Role in a Global Power Revolution?* Available at: <https://mashable.com/2012/05/08/social-media-power-shift/#eGSH2M9F2Gqm> (Accessed: 27 December 2018).

Flaxman, S., Goel, S. and Rao, J. M. (2016) 'Filter bubbles, echo chambers, and online news consumption', *Public Opinion Quarterly*, 80(Specialissue1), pp. 298–320. doi: 10.1093/poq/nfw006.

Flick, U. (2015) *Introducing Research Methodology*. 2nd edn. London: SAGE Publications.

Florea, D. L., Munteanu, C. C. and Postoaca, A. E. (2016) 'Integrating risk literacy into brand management', *Review of International Business and Strategy*, 26(2), pp. 204–218.

doi: 10.1108/RIBS-02-2014-0025.

Galletta, A. (2013) *Mastering the Semi-Structured Interview and Beyond*. 1st edn. New York: New York University Press.

Garcia-Gathright, J., Springer, A. and Cramer, H. (2018) 'Assessing and Addressing Algorithmic Bias - But Before We Get There'. Available at: <http://arxiv.org/abs/1809.03332>.

Garner, M., Kawulich, B. and Wagner, C. (2012) *Doing Social Research A Global Context*. 1st edn. London: Mcgraw-Hill.

Giles, M. (2018) 'Rein In the Data Barons', *MIT Technology Review*, 121(4), pp. 28–36.

Grabner-Kräuter, S. (2009) 'Web 2.0 Social Networks: The Role of Trust', *Journal of Business Ethics*, 90(SUPPL. 4), pp. 505–522. doi: 10.1007/s10551-010-0603-1.

Greenfield, P. (2018) *The Cambridge Analytica files: the story so far | News | The Guardian*, *The Guardian*. Available at: <https://www.theguardian.com/news/2018/mar/26/the-cambridge-analytica-files-the-story-so-far> (Accessed: 24 August 2018).

Griner, D. (2018) 'You Want Me to Write FCK on a Bucket?' *How KFC's PR Crisis Became a Print Ad for the Ages – Adweek, Adweek*. Available at: <https://www.adweek.com/creativity/you-want-me-to-write-fck-on-a-bucket-how-kfcs-pr-crisis-became-a-print-ad-for-the-ages/> (Accessed: 24 January 2019).

Guba, E. G. (1981) 'Criteria for Assessing the Trustworthiness of Naturalistic Inquiries', *Educational Communication and Technology*, 29(2), pp. 75–91. doi: 10.1007/BF02766777.

Haffajee, F. (2019) *How the EFF dominates the disinformation market, Daily Maverick*. Available at: <https://www.dailymaverick.co.za/article/2018-12-12-how-the-eff-dominates-the-disinformation-market/> (Accessed: 4 January 2019).

Harris, P. and Lock, A. (2010) "'Mind the gap": the rise of political marketing and a perspective on its future agenda', *European Journal of Marketing*, 44(3/4), pp. 297–307. doi: 10.1108/03090561011020435.

Hern, A. (2018) *How to check whether Facebook shared your data with Cambridge Analytica | Technology | The Guardian, The Guardian*. Available at: <https://www.theguardian.com/technology/2018/apr/10/facebook-notify-users-data->

harvested-cambridge-analytica (Accessed: 5 January 2019).

Hirschman, A. (1970) *Exit, Voice, and Loyalty: Responses to Decline in Firms, Organizations, and States*. Cambridge Massachusetts: Harvard University Press.

Hofman, C. and Simeon, K. (2013) *Countering Brandjacking in the Digital Age ... and Other Hidden Risks to Your Brand*. First. Edited by S. Zdonik et al. London, Heidelberg, New York, Dordrecht.: Springer.

Hosanagar, K. and Jair, V. (2018) *We Need Transparency in Algorithms, But Too Much Can Backfire*, *Harvard Business Review*. Available at: <https://hbr.org/2018/07/we-need-transparency-in-algorithms-but-too-much-can-backfire> (Accessed: 25 August 2018).

Howard, P. N. et al. (2018) *The IRA, Social Media and Political Polarization in the United States, 2012-2018*. Available at: <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/IRA-Report-2018.pdf>.

Howard, P. N. (2018) 'The Rise Of Computational Propaganda', *IEEE Spectrum*, 55(11), pp. 28–33.

Howard, P. N. and Bradshaw, S. (2018) *WHY DOES JUNK NEWS SPREAD SO QUICKLY ACROSS SOCIAL MEDIA ?*

Howard, P. N. and Kollanyi, B. (2016) 'Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum'. doi: 10.2139/ssrn.2798311.

Howard, P. N., Woolley, S. and Calo, R. (2018) 'Algorithms, bots, and political communication in the US 2016 election: The challenge of automated political communication for election law and administration', *Journal of Information Technology and Politics*. Routledge, 15(2), pp. 81–93. doi: 10.1080/19331681.2018.1448735.

Hupp, O., Robbins, D. and Fournier, S. (2018) 'The Frontlines of Brand Risk', *GfK-Marketing Intelligence Review.*, 10(1), pp. 59–63.

Jenkins, N. (2018) *Mark Zuckerberg Says Cambridge Analytica Acquired His Data | Time*, *Time.com*. Available at: <http://time.com/5236279/mark-zuckerberg-cambridge-analytica-data/> (Accessed: 2 June 2018).

Johannesburg, U. O. (2007) *University Of Johannesburg Code of Academic and Research Ethics, Code Of Ethics*.

Kaplan, A. . and Haenlein, M. (2010) 'Users Of The World, Unite! The Challenges and opportunities of social media', *Business Horizons*, 53, pp. 59–68.

Karolak, M. (2017) 'The use of social media from revolution to democratic consolidation : The Arab Spring and the case of Tunisia', 10(2), pp. 199–216. doi: 10.1386/jammr.10.2.199.

Katzman, A. (2016) *Social Media Is Ubiquitous, Mainstream and Evolving, The Social Media Monthly*.

Kaye, D. (2018) *Commentary: How to 'fix' social media without censorship | Reuters, Reuters.com*. Available at: <https://www.reuters.com/article/us-kaye-media-commentary/commentary-how-to-fix-social-media-without-censorship-idUSKBN1JF34H> (Accessed: 3 January 2019).

Keller, K. L. (1993) 'Conceptualizing, Measuring, Managing Customer-Based Brand Equity', *Journal of Marketing*, 57(1), pp. 1–22. doi: 10.2307/1252054.

Keller, K. L. (2013) *Strategic Brand Management: building, measuring, and managing brand equity, Brand*. doi: 10.2307/1252315.

Khoza, A. (2018) *SA editors launch defamation claim against Bell Pottinger over 'WMC' campaign | News | National | M&G, Mail & Guardian*. Available at: <https://mg.co.za/article/2018-05-21-sa-editors-launch-defamation-claim-against-bell-pottinger-over-wmc-campaign> (Accessed: 2 January 2019).

Kramer, S. (2017) *Identifying viral bots and cyborgs in social media - O'Reilly Media, O'Reilly Media*. Available at: <https://www.oreilly.com/ideas/identifying-viral-bots-and-cyborgs-in-social-media> (Accessed: 2 September 2018).

Krishnamurthy, S. and Kucuk, S. U. (2009) 'Anti-branding on the internet', *Journal of Business Research*. Elsevier Inc., 62(11), pp. 1119–1126. doi: 10.1016/j.jbusres.2008.09.003.

Kroll, A. (2018) 'Cloak and Data. Inside the rise and fall of Cambridge Analytica.', *Mother Jones*, May, p. 23.

Kucuk, S. U. (2008) 'Negative Double Jeopardy: The role of anti-brand sites on the internet', *Journal of Brand Management*, 15(3), pp. 209–222. doi:

10.1057/palgrave.bm.2550100.

Lageman, T. (2016) *Mohamed Bouazizi: Was the Arab Spring worth dying for?*, *Al Jazeera*. Available at: <https://www.aljazeera.com/news/2015/12/mohamed-bouazizi-arab-spring-worth-dying-151228093743375.html> (Accessed: 5 October 2017).

Laws, S., Harper, C. and Marcus, R. (2007) *Research For Development: A Practical Guide*.

Lees-marshment, J. and Lees-marshment, J. (2003) 'Political Marketing : How to Reach That Pot of Gold', *Journal Of Political Marketing*, 2(1), pp. 1–32. doi: 10.1300/J199v02n01.

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

Ligas, M. and Cotte, J. (1999) 'The Process of Negotiating Brand Meaning: a Symbolic Interactionist Perspective', *Advances in Consumer Research North American Advances*, 26, pp. 609–614. Available at: <http://acrwebsite.org/volumes/8329/volumes/v26/NA-26> (Accessed: 5 January 2019).

Liu, B. F., Austin, L. and Jin, Y. (2011) 'How publics respond to crisis communication strategies: The interplay of information form and source', *Public Relations Review*. Elsevier Inc., 37(4), pp. 345–353. doi: 10.1016/j.pubrev.2011.08.004.

Mangalore, U. N. and Shivalingaiah, D. (2014) 'Comparative Study of Web 1 . 0 , Web 2 . 0 and Web', 1(August), pp. 1–9. doi: 10.13140/2.1.2287.2961.

Marshall, C. and Rossman, Gretchen, B. (1999) *Designing Qualitative Research*. 3rd editio. London: SAGE Publications.

Matošević, G. (2019) 'Text Summarization Techniques for Meta Description Generation in Process of Search Engine Optimization', in *Artificial Intelligence and Algorithms in Intelligent Systems*, pp. 165–173. doi: 10.1007/978-3-319-91189-2_17.

Matsakis, L. (2019) *Facebook Cracks Down on Networks of Fake Pages and Groups | WIRED, Wired*. Available at: <https://www.wired.com/story/facebook-pages-misinformation-networks/> (Accessed: 23 January 2019).

McNamee, R. (2018) 'How to Fix Facebook—Before It Fixes Us', *Washington Monthly*, 50(1–3), pp. 33–40. Available at: <http://web.a.ebscohost.com/ehost/detail/detail?vid=0&sid=a3d401b0-ede1-43f7-bbfe-ddc54f11086a%40sessionmgr4008&bdata=JnNpdGU9ZWwhvc3QtbGl2ZQ%3D%3D#AN=126887844&db=a9h>.

Mensah, K. (2017) 'Political brand architecture: Towards a new conceptualisation of political branding in an emerging democracy POLITICAL BRAND ARCHITECTURE: TOWARDS A NEW CONCEPTUALISATION OF POLITICAL BRANDING IN AN', *African Journalism Studies*, 37(3), pp. 61–84. doi: 10.1080/23743670.2016.1220401.

Meredith, S. (2018) *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal*, *CNBC*. Available at: <https://www.cnn.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html> (Accessed: 11 November 2018).

Messing, S. and Westwood, S. J. (2014) 'Selective Exposure in the Age of Social Media: Endorsements Trump Partisan Source Affiliation When Selecting News Online', *Communication Research*, 41(8), pp. 1042–1063. doi: 10.1177/0093650212466406.

Mike Stopforth (2014) *4 Big Myths About Social Media Community Management - Mike Stopforth*, *mikestopforth.com*. Available at: <http://mikestopforth.com/4-big-myths-social-media-community-management/> (Accessed: 20 December 2018).

Miles, M. B., Huberman, A. M. and Saldaña, J. (2014) 'Fundamental of Qualitative Data Analysis', in *Qualitative Data Analysis: A Methods Sourcebook*. doi: 10.5190/tga1948.16.99.

Mirani, L. (2015) *Millions Of Facebook Users Have No Idea They're Using The Internet*, *QZ.com*. doi: 10.1162/inov_a_00223.

Mosseri, A. (2018) *News Feed Ranking in Three Minutes Flat | Facebook Newsroom*, *Facebook*. Available at: <https://newsroom.fb.com/news/2018/05/inside-feed-news-feed-ranking/> (Accessed: 28 June 2018).

Mumby, D. K. (1997) 'Modernism, postmodernism, and communication studies: A rereading of an ongoing debate', *Communication Theory*, 7(1), pp. 1–28. doi: 10.1111/j.1468-2885.1997.tb00140.x.

Murthy, D. *et al.* (2016) 'Automation, Algorithms, and Politics| Bots and Political Influence:

A Sociotechnical Investigation of Social Network Capital', *International Journal of Communication*, 10(0), p. 20.

Neudert, L.-M. N. (2017) 'Computational Propaganda in Germany: A Cautionary Tale', *Working Paper 2017.7. Oxford, UK: Project on Computational Propaganda.*, p. 31. Available at: <http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Comprop-Germany.pdf>.

O'Cass, A. and Voola, R. (2011) 'Explications of political market orientation and political brand orientation using the resource-based view of the political party', *Journal of Marketing Management*, 27(5–6), pp. 627–645. doi: 10.1080/0267257X.2010.489831.

O'Reilly (2006) *Web 2.0 Compact Definition: Trying Again - O'Reilly Radar*, *Radar.oreilly.com*. Available at: <http://radar.oreilly.com/2006/12/web-20-compact-definition-tryi.html> (Accessed: 1 September 2018).

Ornico (2017) *South Africa's top performing brands on social media | Marklives.com*, *Mark Lives*. Available at: <http://www.marklives.com/radar/south-africas-top-performing-brands-on-social-media/> (Accessed: 20 January 2019).

van Otterlo, M. (2018) *Gatekeeping Algorithms with Human Ethical Bias: The ethics of algorithms in archives, libraries and society*. Available at: <http://arxiv.org/abs/1801.01705>.

Pariser, E. (2011) *The Filter Bubble: What The Internet Is Hiding From You*. Penguin Books.

Parliamentary Monitoring Group (2014) *Political Party Representation In National Assembly | PMG*, *www.pmg.co.za*. Available at: <https://pmg.org.za/page/political-party-representation> (Accessed: 9 January 2019).

Pfeffer, J., Zorbach, T. and Carley, K. M. (2014) 'Understanding online firestorms: Negative word-of-mouth dynamics in social media networks', *Journal of Marketing Communications*, 20(1–2), pp. 117–128. doi: 10.1080/13527266.2013.797778.

Portmann, E. (2012) *The FORA framework. A Fuzzy Grassroots Ontology for Online Reputation Management*, *Fuzzy Management Methods*. University Of California.

Qi, J. *et al.* (2018) 'Theories of Social Media: Philosophical Foundations', *Engineering*. Chinese Academy of Engineering, 4(1), pp. 94–102. doi: 10.1016/j.eng.2018.02.009.

- Rajal, A. (2016) *Facebook: Social network, media company - or both?* - *BBC News, BBC.com*. Available at: <https://www.bbc.com/news/entertainment-arts-38333249> (Accessed: 15 January 2019).
- Rost, K., Stahel, L. and Frey, B. S. (2016) 'Digital Social Norm Enforcement: Online Firestorms in Social Media', *PLoS ONE*, 11(6), pp. 1–27. doi: 10.1371/journal.pone.0155923.
- Rust, R. T. and Oliver, R. W. (1994) 'Notes and comments: The death of advertising', *Journal of Advertising*, 23(4), pp. 71–77. doi: 10.1080/00913367.1943.10673460.
- Ryan, Y. (2011a) *How Tunisia's revolution began*. Available at: <https://www.aljazeera.com/indepth/features/2011/01/2011126121815985483.html> (Accessed: 2 November 2018).
- Ryan, Y. (2011b) *The Tragic Life Of A Street Vendor*, *Al Jazeera*. Available at: <https://www.aljazeera.com/indepth/features/2011/01/201111684242518839.html> (Accessed: 1 May 2018).
- Safiullah, M. *et al.* (2017) 'Social media as an upcoming tool for political marketing effectiveness', *Asia Pacific Management Review*, 22(1), pp. 10–15. doi: 10.1016/j.apmr.2016.10.007.
- Salih, K. E. O. (2013) 'The Roots and Causes of the 2011 Arab Uprisings', *Arab Studies Quarterly*, 35(2), p. 184. doi: 10.13169/arabstudquar.35.2.0184.
- Salinas, S. (2018) *Russia had more influence with social media posts than ads*, *CNBC*. Available at: <https://www.cnbc.com/2018/12/17/russias-most-inflammatory-misinformation-posts-were-organic-not-ads.html> (Accessed: 18 December 2018).
- Sanovich, S. (2017) 'Computational propaganda in Russia: The origins of digital misinformation', 3, pp. 1–26.
- Santini, R. M. *et al.* (2018) 'SOFTWARE POWER AS SOFT POWER: A literature review on computational propaganda effects in public opinion and political process.', *The Open Journal Of Sociopolitical Studies*, 2(11), pp. 332–360. doi: 10.1285/i20356609v11i2p332.
- Sheetrit, G. (2017) *5 Social Media Trends That Will Have Maximum Impact in 2018 – Adweek*, *ADWEEK*. Available at: <https://www.adweek.com/digital/guy-sheetrit-over-the->

top-seo-guest-post-5-social-media-trends-that-will-have-maximum-impact-in-2018/
(Accessed: 12 January 2019).

Singh, J. (1990) 'Identifying Consumer Dissatisfaction Response Styles: An Agenda for Future Research.', *European Journal of Marketing*, 24(6), pp. 55–72.

Steenkamp, H. and Rensburg, R. (2016) 'Harnessing stakeholder sentiment on social networking sites: a new conceptual framework for online reputation management', *Communicare*, 35(2), pp. 55–85.

Syme, C. (2014) *Your Social Media Manager Is Your Crisis Frontline | Social Media Today*, *Social Media Today*. Available at: <https://www.socialmediatoday.com/content/your-social-media-manager-your-crisis-frontline> (Accessed: 6 June 2018).

Thompson, N. and Vogelstein, F. (2018) *Inside Facebook's Hellish Two Years—and Mark Zuckerberg's Struggle to Fix it All | WIRED*, *Wired*. Available at: <https://www.wired.com/story/inside-facebook-mark-zuckerberg-2-years-of-hell/> (Accessed: 13 February 2018).

Timothy Coombs, W. and Jean Holladay, S. (2014) 'How publics react to crisis communication efforts', *Journal of Communication Management*, 18(1), pp. 40–57. doi: 10.1108/JCOM-03-2013-0015.

Toko, L. (2012) . Retrieved from: doi: 10.1016/j.ecolind.2009.04.008.

Topping, A. (2018) *'People have gone chicken crazy': what the KFC crisis means for the brand | Business | The Guardian*, *The Guardian*. Available at: <https://www.theguardian.com/business/2018/feb/24/people-have-gone-chicken-crazy-what-the-kfc-crisis-means-for-the-brand> (Accessed: 2 January 2019).

Torp, S. M. (2015) 'The Strategic Turn In Communication Science', in Holthauzen, D. and Ansgar, Z. (eds) *The Routledge handbook of strategic communication*. First. New York, p. 34.

Tudoroiu, T. (2014) 'Social Media and Revolutionary Waves: The Case of the Arab Spring', *New Political Science*, 36(3), pp. 346–365. doi: 10.1080/07393148.2014.913841.

Turner, P. and Turner, S. (1970) *Triangulation In Practice 2 . Triangulation in Presence Research*, *Triangulation In Practice*. Edinbrugh. Available at: <https://www.napier.ac.uk/~media/worktribe/output-220012/triangulationpdf.pdf>

- Unver, H. A. (2017) 'H. Akin Unver', *Journal Of International Affairs*, 71(1), pp. 127–147.
- Veil, S. R., Buehner, T. and Palenchar, M. J. (2011) 'A Work-In-Process Literature Review: Incorporating Social Media in Risk and Crisis Communication', *Journal of Contingencies and Crisis Management*, 19(2), pp. 110–122. doi: 10.1111/j.1468-5973.2011.00639.x.
- Venkatadri, G. *et al.* (2018) 'Privacy Risks with Facebook's PII-Based Targeting: Auditing a Data Broker's Advertising Interface', *Proceedings - IEEE Symposium on Security and Privacy*. IEEE, 2018–May, pp. 89–107. doi: 10.1109/SP.2018.00014.
- Verhoeven, P. and Ihlen, Ø. (2015) 'Social Theories for Strategic Communication', in Zeffass, A. and Holtzhausen, D. (eds). New York: Routledge, pp. 127–135.
- Verwey, S. and Muir, C. (2014) 'MANAGING ONLINE USER-GENERATED BRAND RISK : AN EXPLORATORY CASE STUDY OF SELECTED SOUTH AFRICAN CELLULAR SERVICE PROVIDER BRANDS', pp. 136–155.
- Wagner, C., Kawulich, B. and Garner, M. (2012) *Doing Social Research: A Global Context*. First Edit. Berkshire: Mcgraw-Hill.
- Wagner, K. (2018) *Here's how Facebook allowed Cambridge Analytica to get data for 50 million users - Recode, Recode.net*. Available at: <https://www.recode.net/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data> (Accessed: 11 October 2018).
- Wardle, C. and Derakhshan, H. (2018) 'Thinking about "information disorder": formats of misinformation, disinformation, and mal-information.', in Ireton, C. and Posetti, J. (eds) *Journalism, 'Fake News' & Disinformation: Handbook for Journalism Education and Training*. France: United Nations Educational, Scientific and Cultural Organisation, pp. 43–49.
- We Are Social (2017) *Digital in 2017: Global Overview - We Are Social*. Available at: <https://wearesocial.com/special-reports/digital-in-2017-global-overview> (Accessed: 16 October 2017).
- We Are Social (2018) *Digital in 2018, We Are Social*. doi: <https://wearesocial.com/blog/2018/01/global-digital-report-2018>.
- Wickenden, D. (2018) 'Cambridge Analytica and the Dark Arts of Voter Manipulation | The

New Yorker'. Available at: <https://www.newyorker.com/podcast/political-scene/cambridge-analytica-and-the-dark-arts-of-voter-manipulation> (Accessed: 23 March 2018).

Wood, D., Daley, J. and Chivers, C. (2018) 'Australia Demonstrates the Rise of Populism is About More than Economics', *Australian Economic Review*, 51(3), pp. 399–410. doi: 10.1111/1467-8462.12294.

Woods, A. . and Gaber, K. (2016) *Interpretive and Critical Research: A view through a qualitative lens*. 1st edn. New York: Routledge.

Woolley, S. C. and Howard, P. (2017) *Computational Propaganda Worldwide: Executive Summary*. Oxford.

Woolley, S. C. and Howard, P. N. (2016) 'Political Communication, Computational Propaganda, and Autonomous Agents - Introduction', *International Journal of Communication*, 10, pp. 4882–4890. doi: 1932–8036/20160005.

Yaylagul, S. (2018) 'Skepticism toward Social Media Advertising: A Research on Social Media Users', in Ruggiero, C., Arslan, C., and Icbay, M. . (eds) *Research On Communication*, pp. 177–186.

Zhang, J. *et al.* (2013) *The Rise of Social Botnets : Attacks and*. Arizona, New York City.

Appendixes:

5.3 Appendix A: Social Media Interview Question Guide

1. How long have you been a social media community manager?
2. In your opinion what are key aspects of the work you do?
3. Have you ever experienced a social media crisis?
4. How would one effectively manage a social media crisis?
5. Do you think there are any practices within corporate social media management that political parties could gain from?
6. Are you familiar with communications crises that have been initiated by bot networks or fake accounts? If so, please describe an instance you're familiar with.
7. As a social media/community manager do you believe its possible to influence perceptions of those who come into contact with these misinformation campaigns on social media?
8. As a social media/community manager, how would you recommend political parties mitigate against misinformation campaigns initiated by bots?
9. Do you believe that social networks are doing enough to reduce the impact of these misinformation campaigns?

5.4 Appendix B: Political Party Interview Question Guide

1. How important is social media to the communications performance of your organisation?
2. What do you see as the largest social media threats to political parties?
3. Are you familiar with social media bots?
4. Has your party been affected by misinformation campaigns by political bots?
5. If so, how were you able to identify these attacks?
6. Do you have any plans in place to mitigate against the actions of social media bots and the spread of misinformation?

5.5 Appendix C: Social Media Interview Transcript

Respondent 1 research interview

- ***How long have you been a social media community manager?***

Since 2011, right now my job entails reviewing content, developing content strategy, so messaging strategy, looking at competitors analysis, I do social media audits and paid media analysis. In terms of community management I now do reporting in order to see if we're in line with the communication strategy and I do crisis management.

- ***In your opinion what are key aspects of the work you do?***

I would say the key aspects of the work I do for corporates is finding out where the target market is, because the danger is, if you're not where they are, they're still going to talk about you regardless of whether you have an account or not. So you need to be where they are so you can join the conversation. If they are to post something

that's unfavourable then you have a chance to attend to it before it becomes a crisis. Another thing is that, communication as such, just the whole concept of PR and marketing, it's not about bringing people to a platform, it's about going to where people are, that's the basis of communication. Social media is just a tool, so it shouldn't be seen as a different thing altogether. So if that's where people are...so if they are for example on twitter..so if we do research and found out that your competitors, your target market and the people that you want to reach are on twitter, then be on twitter if they're on facebook be on facebook.. And also what are your objectives? So firstly you decide where they are, then you go there, then you decide why are you there? Are you on there to push product, are you on there to change perceptions, are you on there to join conversations? Uhm, are you on there to be on trend as well, so you have to have a very clear cut goals on why you're on the platforms you're on. Then the last thing is to stick to your values, the danger with social media is that because it's so noisy, you might end up wanting to be a Nando's when you're actually a signature restaurant, you know what I mean? So stick to your values, stick to what your value proposition is. The thing is you're just using this platform to further carry out your business goals.

- **Have you ever experienced a social media crisis?**

Yes I have, lots! Haha! So many. Uhm so, one of the clients I manage is a bank, I'll use this one because it has a nice learning. What happened is that the bank has a technical..what is it..they reset and update their systems, so when this happens, there's a high chance that there will be a black-out, so you won't be able to do online banking, you'll go to certain ATMs and they won't work. So what they do is try to do this late, so let's say, Sunday evening until Monday morning, but there's sometimes a possibility that they go over the time they've allocated, most of the time it's month end, so on a Monday you have people trying to pay employees and they can't because they can't access [they're online banking]. So initially what the bank used to do, is not tell people they're doing system upgrades. They would do it and hope that there won't be any glitches. Everytime there's always a glitch. In previous years when there was no social media, they could get away with it. People would complain wherever they would complain, maybe go to HelloPeter or you know, complain amongst each other, but with the rise of especially twitter, what do people do? Remember our banking behaviour isn't according to set times, there are people partying and want to book an Uber at midnight and they're nothing. Why I say there's a learning. A couple of months later, so we went through that crisis, press releases were sent, journalists were spoken to, tweets went out, systems went back online. A couple of months later we indicated to client that they should inform customers that systems won't be available and we didn't get a much backlash, because people knew to plan around these issues. Communication made such a huge difference.

- **How would one effectively manage a social media crisis?**

First things first, is you need to understand the crux of the crisis, what are people complaining about really? The first thing about a crisis is don't assume what a crisis is, get to the crux of it, what is the issue? Secondly, check where the sentiment is and where most of the complaints are coming from, then acknowledge the issue, but don't ignore while investigating, really do investigate, communicate it and get to the crux of whatever the crisis could be. In that process keep updating people as to where you are in it. If it's an investigation that won't be over a day, you kind of like take people into your confidence as to where you are. Keep people updated otherwise they tend to create their own narrative. Miway are a good example when they had their hoax E-mail situation, they updated step by step, and indicated that they had someone looking into the authenticity of the E-mail, they took us into their confidence every step of the way. Take people through the process because people will create their own narrative. So after acknowledging and taking people into your confidence, give feedback. If there is a long term issue as a result of the crisis don't just rely on social media or PR activity, what are you doing on the ground? What are you doing beyond the affected parties as an organisation? The most important thing is continuous communication, do not flame, do not throw anyone under the bus, especially if it's young junior people managing your accounts. That's nonsense because someone must sign it off. Also don't be too defensive and be too hung up on the legalities. You're dealing with human stuff, so people don't care if you're right in terms of the law if they say you're not being human. Yes you might be right but you're being human. Hence it's important to get to the Crux what is the crisis? Lastly it's important to learn from your mistakes don't repeat

them. One example is outsourcing with their mother's day post only to make the same mistake with a father's day post, H&M is another example. It's important to take corrective action by inking back to what the company does so as to ensure it doesn't happen again. It shouldn't just play out on social media, social media is just another tool.

- **Do you think there are any practices within corporate social media management that political parties could gain from?**

Yes have a strategy and stick to it, Also have a strategy that speaks back to your values. For example the EFF you can see that have community managers If you look at the different accounts the language is pretty much the same And it kind of also feeds back to what the party stands for. When you look at a spokesperson and their leadership the conversation is quite the same. Branding is the same and how they operate is the same they all wish people happy birthday, they're sending condolences to important people's families. What's interesting as it's not just rest in peace to their own members it's rest in peace to other political people. Other great artists and things like that, They obviously have a very strong strategy and don't around for election time. What's smart about them is their press releases are also immediately on social networks. So have a strategy that A speaks back to your values, Stick to your guns on social media if you're argumentative be that, don't change because you're on social media, they act on social media just as they do in parliament. Another thing which is very important, is they need to consider looking at to feedback, also there isn't alignment in their communication which results in them not coming across as authentic. Social is something you can plan, don't be in a hurry to say things or be the first person to say things, no one will care to remember who was the first person or brand to make an announcement, but they certainly will remember if you make a mistake with those announcement. There are no awards for rushed content. Pull each other together, plan content. Parties like the ANC will have one area of the organisation tweet something that's totally out of step with what the entire organisation is saying. It's important to have checks and balances. Also don't have random accounts, the ANC has dormant accounts that aren't being used, they have accounts that are just existing, which ultimately become easy pickings for hackers. Have a content process, an approval process and an alignment with values.

- **Are you familiar with communications crises that have been initiated by bot networks or fake accounts? If so, please describe an instance you're familiar with.**

Yes, currently whenever someone tweets something negative about the EFF, there's a flurry of tweets defending them. There is also an increase in social media accounts with partially incorrect black names that are tweeting against the EFF. There's a lot of that right now, also, another thing is we're headed to election year next year.

- **As a social media/community manager do you believe it's possible to influence perceptions of those who come into contact with these misinformation campaigns on social media?**

Definitely, there are studies that show electronic word of mouth is strong, so if I see an article for example - I once saw an argument between two journalists. The one journalist wrote about how the EFF used to use Adrian Basson, then Jacques Pauw published information on where Malema stays and who bankrolls Malema, then another journalist decided to expose sources so they started having a fight. So now if I'm an EFF supporter who aligns with the EFF because they're pro-poor, honest, aren't corrupt. If I find out they are corrupt and have new "Gupta's" supporting them. If I read that tweet without question, I might not vote for the EFF, that's because people don't read anymore, people don't read articles anymore. People will still argue with you even if you say, read the article this is fake news. People now get outraged very quickly, we don't question. If you look at most of the social media crises that have happened in the past couple of months, some of them have been based on fake news, fake E-mails and things like that. Social media is all about perceptions so you have to fight this. It's important for political parties to know the role fake news plays and also handle and manage it immediately and not say "oh, people won't read that."

- **As a social media/community manager, how would you recommend political parties mitigate against misinformation campaigns initiated by bots?**

It's not about stopping them, teitler have tried to remove fake accounts, so did facebook. It's important to remember that there are people behind these fake accounts making money off them. The important thing, to remember, whetehr its a bot spreading stuff or something being said that wasn't supposed to be said, the internet never forgets. You need to treat it the same way. A you need a strong strategy around your messaging. What content can you put out there to refute claims being made and use different avenues, partnerships and networks to help that message reach as many people as possible. Then also use a media strategy, take the fake news head on and create content that identifies and debunks it. Don't use it as your primary content strategy, your main will be aligned to your brand values, then your secondary approach would be debunking myths - this is where consistency, credibilty and authenticity is important it will help people identify fake news. Don't say what you are, show us. Listen, identify issues, then show in action so people will defend you due to the trust you've built. It's not just about them. Naysayers are everywhere, its just a matter of how you approach, saying something is not true isn't a strategy, show people.

- **Do you believe that social networks are doing enough to reduce the impact of these misinformation campaigns?**

No, they're competing for numbers. Bots are odd. It's good for social networks and bad for them. On one side the it inflates their user numbers so advertisers approach them. Meanwhile they generate distrust towards the social networks. They're not doing enough but they won't do enough because its serves them not to.

Respondent 2 research interview

How long have you been a social media community manager?

I was an online editor which included community management from 2013

In your opinion what are key aspects of the work you do?

As an online editor, my main role was to create and promote both editorial and commercial digital content that would add value to the life of the reader. As a social media and community manager, I needed to grow the social communities and make sure it was an engaged audience and not just a large stagnant one. I also had to answer questions and resolve complaints.

Have you ever experienced a social media crisis?

Yes. Several.

How would one effectively manage a social media crisis?

It depends entirely on the kind of crisis and source of it. If we, as a brand/company, had made a mistake it was easy to resolve. We would apologise earnestly and honestly, say that was should not have done what we did, say that we wouldn't do it again and then let them know what we had done in order to stop that mistake from happening again i.e. what processes are now in place. If the wrongdoing was large enough, we would also donate money to a relevant cause in order to show we were serious about the apology and did not want to profit from it.

If it was a crisis that was unrelated to our behaviour as a brand/company, or, even worse, if it's a company behaviour that management will not agree to change/it's not feasible to change, it's more difficult.

If it's an outside crisis mentioning the brand, then the best way forward it to write the facts in a very clear way, avoiding ambiguous language and explaining why you want to clarify the situation. If possible, include ways for individuals to see for themselves that you're telling the truth.

Do you think there are any practices within corporate social media management that political parties could gain from?

There must be but I'm not familiar political comms.

Are you familiar with communications crises that have been initiated by bot networks or fake accounts? If so, please describe an instance you're familiar with.

When I managed a publishing brand, scammers would create a copy of our website selling a weight-loss product. Once they had credit card details, they'd just keep debiting the accounts until the cards were cancelled. Obviously, this was a disaster for the brand. People were saying we were the scammers or asking us to process their refunds. We couldn't find the scammers as they used international ISPs and we didn't have the tech or legal support to track them down.

As a social media/community manager do you believe its possible to influence perceptions of those who come into contact with these misinformation campaigns on social media?

Yes. Internet users are becoming savvy to fakes and frauds. They notice if logos aren't correct and even grammatical errors. Once we posted screenshots and a warning that we were a publishing site and would only sell magazines and event tickets through secure third parties, people usually had a positive view of us as taking care of them and looking out for them.

As a social media/community manager, how would you recommend political parties mitigate against misinformation campaigns initiated by bots or fake accounts?

They should point out the general ways to spot spam, bots and scammers. Logos that are outdated, incorrect or pixelated. Huge followings with only a few tweets. Links to sites that look like news sites but that nobody had ever heard of. Let them know to check the url. Look at the language. Ask for verification before reposting.

Do you believe that social networks are doing enough to reduce the impact of these misinformation campaigns?

No. They are for-profit companies for whom engagement trumps trust. 20k people fighting over a fake tweet is better for Twitter than hiring more team members to verify accounts.

Respondent 3 Research Interview

- **How long have you been a social media/community manager?**

I've working for 5 and half years, I started out in agency at a junio level firstly as a moderator and creating alot of content for social media pages, I spent alot of time on facebook, on twitter, publishing, researching and writing the content calendars and so forth, that was a year and a half. I've been here at the bank for four and a half years, it's a lot more strategic because we work in the group team a lot of work is focused on how do we help other country departments to setup a presence on social media and best practice tool kits and how they help them in terms of naming conventions and what kind of content to post Android allowing them to do what I need to do and be free but also giving them guidelines on how to operate but still be free and think about what's topical in their world because they would know that bit.

- **In your opinion what are key aspects of the work you do?**

I think to be honest many people say it supposed to be strategic and high level show me the most important things are really the basics so for example, a brand tone and a good moderation plan. So when I speak to you is your approach to reply or not say anything, what kind of plan do you have in place for negative and positive experiences For the positive if you're running a big campaign are you getting all hands on Deck So that you can create lots of engagement You want to speak to people alot or do you want them to ask you questions. Are you starting a conversation or are they When there is a crisis you have FAQs setup with the pr team If you know this is a crisis newsroom have they helped to formulate a statement with legal team so whatever goes out to media is consistent with what you find on social media.

- **Have you ever experienced a social media crisis?**

The easiest one is the downtime that we experience I think it was a month and a half ago, ATMS went down and credit cards went down, people were stuck at restaurants and petrol stations, people bought things and were stuck without the ability to pay. The worse thing for us was wondering if we could have known ahead of time if the downtime was going to happen and could we have planned appropriately. We have seen preventative messaging over the app or via email to say this is going to go down at this time, at least people knew that options that would obviously be a (inaudible) scenario. And if we didn't know that, what were we going to do aside from apologising. Could we have sent money vouchers or done payments on behalf of people so they could claim it back. So those are the types of things that happen when it's a crisis, that's probably the last one we've had this year. The most important thing is to manage the service queries so can people actually make payment or are they physically stuck so they can't do anything. Then the second is obviously the reputational risk, so if you're tracking sentiment, something that could be positive turns very negative This is where I think the moderation and the service aspect comes in to play and people don't want to see copy paste responses that look like a bot that says high tshepiso sorry for the inconvenience but actual solutions, why dont you go to the app and do this, is there someone you can ask to pay so you can pay them back, can we send you voucherts, have you tried the money wallet, you know. Things like that, practical answers

- **How would one effectively manage a social media crisis?**

I think process is the best also because something always happen when you're in the service industry. down time always happens but i think there's no excuse to not have a solid plan so when it hits no one is running around we don't have to wait to get approvals from x y and z before we can go out and make a statement. I think it first definitely have an approved set of people who come together to try and deal with it, who in the social team and who in the PR team, like have a crisis team set up so when things happen you just call on those people everytime, one because they will have experience and know how to handle things, two because they can help the whole process go alot faster. The second thing is to have moderation FAQ document in place, byt now you know what people will ask so you're prepared for those. Then its what positive step you can take afterward to help soften the blow do you send vouchers to say sorry, stuff like that but have that all set up upfront so you're not tryong to run around to sort things out, have all those things defined and then deploy. Also know that there there are resources to answer the calls, monitoring twitter, those sorts of things.

- **Do you think there are any practices within corporate social media management that political parties could gain from?**

Yeah i think because its political people make it very personal, and make it about the person and the one good thing about corporate is that shouldn't necessarily be your personal view but what the brand stands for, the job is the view of what the brand stands for so i know alot of the time is really hard in political campaigning to differentiate the person from the party necessarily especially if you're trying to elect the person you buy into their values but i think its important to define that, is it a personal campaign like Obama in this case you're voting for him and because you buy into what he says or is it something that you're campaigning like Mmusi Maimane does then you're campaigning for the DA so he should sort of take a stance on what the party stands for and not necessarily try to push his personal views. Corporate is quite good at that uhm, what is the view of the company overall so even if my opinion might be different as I'm working on it, it's solid and I understand this is where you draw the line in terms of being overly emotive for example because maybe we can't show that we're being casual and fun because that's not we stand for, we're about heritage and structure and being an old bank in a good way, which means we know what we're doing and we're not going to take silly chances whereas a brand like capitec is really new so they can be fun and playfull, I don't think people would expect them to be serious because it's not who they are so i think yeah its very important to decide if its personal or behalf of a party and if it is on behalf of a party, just have clear rules and maybe content themes and pillars that says when it comes to the people this is what we talk about, when it comes to service delivery we entertain these questions and queries and not others. When it comes to our political messaging, do we use a certain person as a spokesman or do we take the approach of I don't know, like testimonials of people on the ground, like what's the stance, whatever the

message is, whatever your approach, it is consistent, like you're not getting Maxine's view today and Standard Banks view tomorrow, that way people know what to expect.

- **Are you familiar with communications crises that have been initiated by bot networks or fake accounts? If so, please describe an instance you're familiar with.**

I have a personal one definitely, virgin active gym was dealing with a crisis about something happened in their stores, i think somebody was wearing a t-shirt and they told him to leave because they thought it was inappropriate and I remember the sheer volume of queries coming in meant they were unable to handle getting to everyone and I think for them what was most important was to let people know that they were heard. They opted to use a bot for the initial response, to be like, thanks so much, we hear what you have to say, we're working on it we'll release a statement shortly. For them it was important that, say they couldn't get to everyone within a one hour period, they didn't want to wait five hours just because they didn't have enough people because obviously they're not geared up for that stuff because it doesn't happen to them often. Yeah, so that was the one time when I think they used it quite effectively. They know people get irritated when you take time just to like initially acknowledge, they used it for that, where I think it was good though, was that afterwards the follow ups were quite personal so you know it wasn't a bot. So that was a good example of using the bot for initial response to keep people at bay, and then following up with a proper personal engagement. I think it was positive, but i might be biased because I work in social media so I thought that was like a clever way to handle stuff. I guess if you're on the outside and you don't know this stuff you'll sort of be indifferent and it may not make a difference because you'll be irritated regardless. Speaking from a specialist point of view i believe that was a clever way to use a bot, yeah.

- **As a social media/community manager do you believe its possible to influence perceptions of those who come into contact with these misinformation campaigns on social media?**

Yeah definitely, that's why its so important to have your themes and pillars set out initially so your message is clear and you aren't sort of tempted to sway and put your own view in especially when its political if everyones got their own preference and it is difficult at times to remove yourself as the social media person to remove yourself and remember you're speaking on behalf of someone else and speaking on behalf of a brand if you are managing an account say for a company or a political party.

- **As a social media/community manager, how would you recommend political parties mitigate against misinformation campaigns initiated by bots?**

I think its a really hard one, the hardest thing is people can create accounts whether its bots or not, especially with bots faster than you can shut things down so i think in that case the easiest way is to be on really high alert and have all your alerts set up so that you get sort of pinged immediately as soon as a bot, and you would know its a bot because they will probably spit out 20 tweets in two minutes and then you know that's obviously not a person so i think have alerts set up and have a team with enough physical bodies that can sit, report accounts so they can get shut down and i think have a good relationship with the platform partners in whichever country so in South Africa we have facebook africa head office, so for example we don't have a twitter head office, so who's the office rep for twitter? Have them on hand, have their contact details make sure so when you have a crisis you can contact and say here are these five twitter handles that have come up, we've reported them, please help us take them down asap, you know because, of misinformation and propaganda. Other than that, I mean, it's really hard to sort of warn people unless you were gonna send out a tweet saying please be aware of fake news circulating, you know, from these accounts, but if anything that would probably send people to those accounts because the natural curiosity means you want to go and find out what they're saying. So I think a sort of background approach to just try and get them shut down and reported is probably the safest easiest way to attend to it.

- **Do you believe that social networks are doing enough to reduce the impact of these misinformation campaigns?**

I think probably as of 2018 yes, i think before that no, I feel like they didn't really understand especially facebook, didnt really understand the extent to which people were literally putting out sheer nonsense. People were misappropriately using incorrect images and incorrect copy or messages and putting them together uhm and posts were just going viral, but I think ever since then, especially since what happened with cambridge analytica and facebook I think all the social networks, especially facebook, are really on it now, i know that they've actually gone on a whole mission deploying new people and engineers to develop code and have ai algorithms to identify things sooner and faster so they can automatically shut down accounts, delete posts, images and so on, before the public even has a chance to report it as fake. So I think that's going a really long way in the right direction because it teaches the computers not only different languages with copy, but also identify images because I think getting code to read the text and take down is not that complicated in 2018, but i think being able to view a video for example, with terrorist activity with isis, where people were getting beheaded, for video in order to read that and say, oh, here's a person, plus there's plus, plus there's a beheading, oh this probably means its something bad lets remove it. That I think is a really smart move, because all people are gonna do is outsmart the machines and find another way and do funny things in the videos to trick the machine learning to think, oh here's a cute cat and a baby you know, then throw in the horrific scene for example, and let's be honest, human nature is people are curious and they are gonna want to watch it anyway so i think using the tech to do it automatically, before a person needs to report you know something as misinformation is probably the best way, plus they can do it at much greater scale than any human can do, yeah.

Respondent 4 Research Interview

- **How long have you been a social media manager?**

So I've been involved in social media for 9 years since 2009 and that's specifically using it as a social media manager and not from a personal consumption perspective, if its from a personal consumption perspective it goes back to 2005. So my first role was working publicity for a movie franchise and developing an online, a virtual community around that to get generate hype before it got released, but at the same time i was also working extensively with restaurants and cement companies to try and navigate and understand social media from a brand perspective

- **In your opinion what are key aspects of the work you do?**

So in terms of my work let's start let's talk about the day to day and then cover the broader strategic objectives. It is essentially to manage the reputation of the brand I work for and to ensure that there isn't any misinformation around the brand, secondly, where this is negative sentiment, my job is to understand what that is and to see how we can deal with it so that we can give a positive brand experience, not necessarily just for consumers but for all stakeholders. Internal stakeholders, external stakeholders including civil society, uh, advocacy groups, government et cetera. Understanding the brands online reputation whether it has positive sentiment and how that plays out on the line whether it be broadcast platforms online or dialogue platforms online, including social media.

- **Have you ever experienced a social media crisis?**

Yes, I've experienced multiple social media crises over the last 9 years, I'll just rattle off a few from the early days until now. With a pharmaceutical brand, a few years ago one of the challenges we had was that an importer bringing in what can be considered to be grey product and not importing through the proper channels such as getting sabs approvals and selling that product, the problem with that product was that the veracity of the health claims couldn't be proven purely because it did not go through those official channels, so it created a lot of distrust in that product, this was 5 or 6 years ago. For a large retailer, a crisis

i dealt with was hiring practises and preferences and how that retailer dealt with that with regards to transformation. I've dealt with crises in terms of explosions at facilities, where there were damages. Loss of life et cetera.

- **How would one effectively manage a social media crisis?**

Ok, so if we were to define a crisis or any issue, what is a crisis? It is a negative change or a negative disruption in what is assumed to be the norm, so that would be a crisis and it could scale from a bad customer experience to something that might be a little trivial like you bought an expired loaf of bread from a retail outlet, to catastrophic loss of life or property and materially affects a businesses ability to operate, so that's how we would define a crisis the resolution however there are certain commoanlities, the first commonality is being able to understand the context to understand what went wrong and also understand the extent of that damage also to not necessarily contain the message, but be able to focus a singular narrative that comes out of it and that narrative needs to be centralised so part of that mitigation strategy is that the message is controlled from a sense that only certain individuals comment on it, certain platforms comment on it and in the process we eliminate doubt confusion et cetera. So what we've done is all our platforms are centralised and individual operating model entity, say for example, in Gabon cannot just do something or say something without approval which is important because you contain the message. It's also important that our employees are educated to say this is how we manage theses risks because there are safety risks and we don't want to cause undue panic, and that's also important, its important that we dont treat channels separately, so we have a single narrative across channels, so a press release will never contradict a social media update, will never contradict a statement on radio, so its very important that message is consistent, that message is spread across and we try to do as much extensive communication as possible, so that not only do we address the crisis on the platform in which it plays out, but also on ancilliary platforms and that's something I don't think brands take seriously. If there's a crisis for example on twitter they will contain their messaging to twitter, but twitter could be the starting point and extend them to other platforms, so how do you mitigate that?

You might have an issue because of a print ad that plays out in various platforms, like whatsapp groups and you can't monitor that, so you try and spread your message as far as possible and you try and make it as accessible as possible, because you'll never perhaps be able to correct what happens, but you can have a credible voice in there and part of that credible voice is also, before that crisis happens to proactively build credibility within that platform, so when things happen, you do have a voice and this is something we saw from BP, when they had the gulf oil crisis, believe it was in 2010, what happened was, because they had no official presence, they allowed these parody and rogue accounts to come in a create this confusion. It's not something that's stayed in 2010, we see today for example the global citizen concert that happened on sunday and the subsequent problems that ensued at various locations including service stations, there was a parody account for the commissioner of police Bheki Cele, and that parody account was leaving comments and people were thinking that this was the official minister of police leaving official comment on it and that tends to go out of hand, I mean similarly now there's a video circulating of what some say was an angry ex-girlfriend who obstructed a wedding in east london and that footage is going around and now there's a new spin on it where people are saying it was an ANC meeting, so there's obviously a racist and political agenda in terms of depicting this video. That video is from london and its about concert goers who got angry because the artist didn't pitch up, but yet all of this tends to fester and ciruclate and it's sad because we live in what some people term a post truth world. I've seen it happen personally where we had an incident at one of our plants last year. A hydrogen tank ruptured so it was quite a loud noise and a few people were affected by shock because of the noise, but that was the extent of the injuries, people were taking a refinery explosion in Mexico where there was this massive fireball and loss of life and attributing it to the incident last year. When I corrected them, including media agencies, they didnt do anything about it because engagement rates were so high. They didn't care about the truth, they cared about engagement, so that's part of the challenge around it.

- **Do you think there are any practices within corporate social media management that political parties could gain from?**

I think there's a lot of practises the one practice could be the sanctity of the brand and how the brand is depicted so brands understand that we invest a lot in the corporate identity, the Insignia the logo and there's value in that there's equity in that so we're very protective of that and how it is displayed on platforms

And while [political] organisations do have a have a level of branding I do think it not as as uhm heavily invested in from a protection perspective so oftent you might, it's not to say it doesn't happen, the EFF submitted a statement two days ago to distance themselves from people who wear EFF insignia while committing acts that the EFF do not condone so, so there is discussion around it, but brands are more consistent with that. It's the branding practises around civil society and how they could learn from that, I mean simple things like consistent use of a hashtag for example, on something online, i notice that if civil society and advocacy movements were consistent with CI and Branding and empowering their people with those guidelines, that would make for a more empowering conversation especially if you are going to use digital communication to create awareness around a cause, so those are some of the principles I think that uh, political parties can learn from brands. Othwer practises as well is a customer centric aproach [chuckles] to understand constituents needs and deliver on that uh, I saw some interesting research last week that spoke about "what are the top priorities from a polling perspicitve and what are the messages that political parties use" and the disconnect between that, what people value in terms of service delivery, safety et cetera and what party messaging is and that disconnect between that market research and messaging research so I think there's alot of that as well where politcal parties can learn from brands. I do think political parites tend to use social media as broadcast platforms as well if you look at the sa governemnt twitter account for example, it will not share anything except what it publishes or what it subsidiary accounts publish, so theres no sense of engaging and there's no response to comments. So while social media is definitely not representative of a country's sentiment it does capture a part of it. So it would be imortant to consider the dialogue component of social media, if you're asking people to self select their experience and follow you, then give them something that's valid.

- **Are you familiar with communications crises that have been initiated by bot networks or fake accounts? If so, please describe an instance you're familiar with.**

So what happened is we had a tax dispute with SARS last year which we won this year, bassically SARS were saying we owed them R2 billion for oil purchases and uhm, what happend was, some of the WMC bots got hold of that and started pushing their narrative that we're aren't playing [ball] with government, we're white monopoly capital, our CFO is an afrikaner man, so that became a thing and that spread on a bot network including a lot of webssites like WMC exposed, a lot of Gupta Bots stuff, all that is shut down now becuase all their funding is gone there, but for a long time i was dealing with that and how this message was spread out across this bot network and that was kind of scary for a while, but luckily, what we did to counter that was just to be frank, go into traditional media push it out a soon as possible and to also change your SEO strategy quite heavily to combat it. That was a funny experience. So that's one, the other is the conversation around WMC and how that was played out. I've seen the US bots around the US elections spread alot of fake news, and fake news around Obama, Hillary, fake news about Islam as well, I've seen a lot of that and I think that, because I'm close to it from a faith perspective, [the lies] it's so evident. Alot of it is really ridiculous, what's sad is, people's ability to hold on to that and believe it because of what social media does. So a few years ago I was doing an interview on Al Jazeera and the discussion was, is social media subjective or objective and I'm like by its very natures its subjective becuase you self select, because you're using the search parameters to look for what you want to look for, you see what you want to see and it's almost given a platform for like minded individuals to find each other. There were always people who

believed the world was flat, the only difference now is they've found solidarity and some form of uhm, well, other idiots who think the world is flat and that's what social has done, by its very nature it's found like minded people to engage in a virtual community, to share a collaborate and to reinforce beliefs.

So, at Al Jazeera at the time, I was talking about search terms if you search for something you'll find it and it will either confirm a bias or negate the bias, but you don't search for things you don't want to believe in, because you don't want to read stuff that does not confirm the bias, that's harder. If you fundamentally believe that the government is corrupt any misinformation that proves that point you'll take it on, it's the same with farm murders, if you honestly think there is a genocide, if you find a little girl from Louisiana that was slapped, then slap onto and add to say boycott Spur, you will believe that without question. It's harder to question the things we believe than it is to question the things we don't believe.

- ***As a social media/community manager do you believe it's possible to influence perceptions of those who come into contact with these misinformation campaigns on social media?***

It is a difficult job to change perception and change behaviour, because you cannot, especially on a social media platform, if you think..first of all I think people are sceptical of brands and they understand that brands have an agenda as well, brands are not altruistic, they're not just here for the good of society, brands are there because they are pro-profit agencies so they're there to make money, so you should be sceptical when a brand engages you, but at the same time, as a brand we need to consider that just because we might have a version of the truth does not mean that someone will accept that truth so what we need to do is ensure consistency around that truth, authenticity as well as an unyielding commitment to living out that truth because the idea of loyalty is so tainted these days, that your impression of the brand is based on the last impression of that brand. So all the equity a brand might have built up over years, doesn't matter anymore, so a brand has to ensure that all platforms and touchpoints have a level of consistency. So that if some does believe something about your brand, you can prove them wrong.

- ***As a social media/community manager, how would you recommend political parties mitigate against misinformation campaigns initiated by bots?***

It's tough, but I live by three principles whenever I create content for social media, whatever I do has to be credible for the brand and that extends to everything. The second thing is, if we're looking to create content or build relationships, it has to be sustainable, it can't be once off, I'm looking for something we can build over time. The last thing which may answer your question around misinformation, is, whatever content we create must be of value to the user so when we correct someone, is it because of our ego, is it because we're self serving, or is it because it adds value to the person who has this perception of you, and we need to change that perception. To add to that I'd say a deeper level of transparency instead of choosing what you will engage with versus what you won't engage with. I would campaign for transparency I would campaign for openness I would campaign for a demystification of manifestos of opinions, of positions, have an opinion and stick to it until you realise it doesn't work for you. But don't be contradictory and play yourself too often and that's what happens, political parties need to die on their sword in terms of their principles, or they need to be agile enough to adjust and adapt, but the moment you flip flop, the moment you become a foil and don't deal with all your criticism and all your concerns you lose your credibility, that's what I would do. I think clarity of focus is important because you end up alienating more people. Discovery is going through the same thing right now with their bank, with the calls to boycott discovery. The sad thing about that is those who need to empower and enable transformation are the ones with the economic clout to put a barrier to it and that's what's happening. So with the calls to boycott discovery and stuff like that they can't mete out their transformation agenda but at the same time are they doing enough to win over the new customer and the new clients and to change their customer base and that's difficult because if you flip flop you end up losing both sides not just one, because you can't be everything to everyone.

- ***Do you believe that social networks are doing enough to reduce the impact of these misinformation campaigns?***

No, I mean there's a few things they can do very easily, I see good intent, but right now you need a lot more than that, right now you need a deep investment in humans that can fact check, need better integration with uhm, the sort of tools and accounts out there that do fact checking, whether its with snopes or an africa check or something like that ,you need partnerships like that to the point that a social media platform can easily see if something is about to trend and stop it while its gaining momentum, so what happens right now with africa check, it relies on consumers to pose the question in order to initiate the research, whereas if you aggregate this stuff as the network and you have a partnership with these trusted organisations, it will go a long way towards addressing these issues. I mean, twitter has done some work recently to close down some of the bot accounts, but it's one thing to close down an account but its another to address something that's out there. I imagine that if there's a disturbing image going around that's been contested that the platform puts a watermark over it immediately, saying, listen, this is unverified or whatever and that should become the norm, maybe its even to the extent that we want to share something, and if we intend to share, there's a block that comes up saying this is fake news to discourage sharing.

At the moment it's pretty sexy to hate facebook, its cool to hate facebook, it's like when people say facebook is dying, which has been a trend the last four of five years. If anything I think there will never be another facebook, in terms of how ubiquitous it is all encompassing. You get niche platforms that come up and I can accept that, secondly, facebook has transcended social media and become a part of everyday life. We don't celebrate the things anymore, if you look at E-mail, its become part of life, to the point that we don't even notice because we're on it so often. We never articulate that "I am going on facebook anymore" its life, its routine, so I think thats what has happened from what facebook started of being to what it is right now and part and parcel of that is, "are they doing enough?" no one does enough because of you were doing enough it wouldn't be a problem, but I do think they have mechanisms in place which they have invested in to start dealing with this. I think another issue with the problem is, its not just their responsibility, as we see, those who want to propagate fake news will intentionally propagate it. There is this notion that people are unknowingly or unwittingly doing it. Often, we perpetuate it as individuals, so how does a platform react to that, because its always reactionary. Mcquail spoke about this about 20 to 30 years ago, where says technology will lead and regulation will follow and thats what happens, our tech gets developed faster than what regulation can keep up with it that's why right now there's a discussion around whether netflix should pay tax in South Africa. What does that look like, regulation following technology is not new. You will always lead with content, technology then regulation, so the platforms are similar. We as user fo the platform will also dictate the usage of that platform. So recently I readn an article around how teenagers are using instagram to set up events. So we will dictate how platforms will be used, then the platform look at what to upweight in order to monetize it, but when they downweight that, they risk the people not using the platform anymore which is part of the challenge. So instagram took stories from snapchat and twitter changed the favourit to likes because that's what facebook does, as time goes we will see a lot more of that as platforms clamour for eyeballs. At the end of the day the consumers will decide. No matter, how much you invest, the users decide and that's why google plus is now dead which gives me comfort, if google cant get something like that right, then we're ok. Googles clever as well because with most of what they do, they believe utility first then monetisation after, so they have a high product utility rate, gmail, maps and its all free, then later we monetise it.

Journalism has been affected by this, for example the New York times or the Washington Post one of them started capping the amount of words in an article because its a world of engagement and instant gratification and they have to adapt or they will die and that's what's happeneing. There's an interesting article written around 2009 by a guy named Rafiq Copeland and in 2009 the biggest accounts were the media accounts that decided to be on social media because they brought influence from traditional media. CNN brought all their equity and trust, then brought it to social networks. Have you watched this week's episode of The Patriot Act. This weeks episode of the patriot act is great, it covers social networks and how they are problematic because they look for the protection of publishers but they also want to be, because they're content creators, and then

uh, so the entire thing is about how they value freedom of expression and freedom of speech and in doing so they try and distance themselves from the responsibility they have.

So this week's episode is Unbelievable especially when it comes to the historical context of the internet in the early nineties and what legislation was created to protect consumers and how social media platforms are blurring those lines.

Respondent 6 Research Interview

- *How long have you been a social media manager?*

So about 8 years now, I started in a social media agency as a community manager, then just climbed the ranks junior, senior, brand manager and then a social media account lead and now head of department. How the brand manager element works is you're looking after a collection of brands, so that's what brand manager means in our context and in terms of brands we work on pharmaceuticals, Insurance, Banking and Telecommunications

- *In your opinion what are key aspects of the work you do?*

Set of a department a lot of my work is less operational so it's about managing the team support in this team making sure that from day to day they are fine and everything is in order. Healthy. Miss any crisis escalation so I don't really mean that if a client is escalating I mean it from a community perspective. Sophie example today we had an incident with Jack Parow on one of our brands. Helping the team with how do we deal with that and what's the steps and how to liaise with clients and type of stuff I mean I also integrated apartment with the rest of the agency silver lining them with the media guys the analytics guys and the strategy department so basically I'm the bridge between the other teams and my department. I think for all brands whether you've got an active presence on social media or not your audience is on social media. Why they actively be part of that conversation or you can not take part in the conversations. At the end of the day I think for most brands taking part of the conversation cannot control what a consumer things but you can mould and direct the conversation in a certain direction if you're part of the conversation so I think that's the value for most brands. For some brands depending on the brand's identity and the brand's objectives, an active direct involvement in social media may not be the best option, you could use social media purely to monitor reputation or it could be really paid focused and really advertising and focused and you don't really want to build communities. So there's a lot of variables you need to take into account but either way whether it's direct to indirect I think there's a space for every brand on social media, there's a case to be made. But depending on your objectives that determines how entrenched you become.

- *Have you ever experienced a social media crisis?*

Recent example at the beginning of the year on one of our FMCG brands, there was a very topical conversation that was happening in the country and we made a post about it. It wasn't direct commentary but we tried to leverage the situation but then it came over as very insensitive. So yeah, the post went out, we got a lot of negative sentiment and then it was a matter of trying to contain the scenario and trying to contain the brand damage. So it wasn't an issue of a customer complaining it was a piece of content that we as a brand agency were accountable for that was posted out so, in that sense it was around aligning with client so why did the post go out, what was the reason reasoning behind the post and what was the intention, aligning with the PR partner in terms of how do we address this in the social media space, then dealing with questions around do you remove the post do we put out a public statement to do we directly reply to everyone that complained about the content and kind of the recovery process for the brand so now that the incident has happened what do we do to mend the brand reputation. So there's really two types of crises that we deal with the one is that comes from a marketing message where that be a post a billboard or a customer issue that then escalates on social media.

- How would one effectively manage a social media crisis?

I think the funny thing is that most of the social media agencies will tell you that you only need a social media crisis plan when you have a social media crisis. What are the things that we push with clients which is a tricky thing because a lot of clients don't have it in place. Is a crisis comms plan, a lot of the bigger clients will have a crisis comms plan in general. But very seldom in my experience do they have a social media crisis comms plan that aligns with the overall corporate crisis comms plan. So a big thing that we've started with our newer clients before we built communities or we start engaging is to build a social media crisis comms plan. The crisis comms plan leads into a FAQ space so what are the top types of complaints that you get as a brand, what are the standard responses? We ensure that they align with the business, we try to ensure that we reply the same way that someone in a customer care call centre would reply because consistency is very important. But then we also build up for every brand. Case by case scenario so if this happens this is how you should respond to it and if this becomes a crisis what would be step A B and C. So when a crisis hits it's not "oh my goodness what do we do now" it's not a case of we're just running around nobody knows what's happening, Important to know who's responsible for what in that scenario, who is the PR agency, who is the corporate comms person internally and And how do we get messages approved because the last thing you want in that scenario is to get stuck with message approval. So the content not going out because you're not getting the right person approving it timeously, because time is of the essence when it comes to these scenarios. The longer the time you take to respond to a crisis the more unfortunately the consumer infers guilt, on the brand side the longer you're silent the more damage that you do so that's something we always try and prevent.

On my side it's interesting especially on certain channels there's more of a culture around hostility than others so twitter has become notorious as a platform where brands get lambasted and you literally have people that trawl brand pages looking for brands possibly saying something insensitive, with some sort of racial flare there's actually some people that live on this and once they've found those brands they try to make a scene, especially with twitter it happens a lot. It's an interesting thing I don't want to infer that it's a cultural thing. You could align it with people's Obsession with fame and being in the limelight, because of a lot of the time people want that recognition that I'm the one that recognises this brand problem. To be honest a lot of people get a sense of affirmation around it.

On the positive side there's a lot more accountability, there isn't any place for brands to hide anymore so that's the positive side of it, but I do think there needs to be balance, I do think you get some consumers that complain and aggravate the situation for the sake of doing it. But at the end of the day the principle of it, that's the success of social media, for your brand to work you need to be transparent. If you're not you're going to be caught out.

- Do you think there are any practices within corporate social media management that political parties could gain from?

I think if you look at the political party as a brand, at the end of the day it is a type of brand. It's a specific type of brand but at the end of the day they are a brand with a reputation that they need to build and protect. At the end of the day, the things that we do as social media managers relate to protecting brands and creating brand affinity with our audience and at the end of the day that is what a political party is, they want to create brand affinity with an audience so that audience can vote for them. To be honest most of it is applicable to the political space. A variable with political parties is that there are lots of sensitivities and I think there are a lot of topics that they have to be careful of. I think a lot of the time political parties play in the space of commentary and thought leadership, brands do as well but I think with most of the brands that we work with it's less about giving commentary on a particular topic and it's more about we are brand and

this is what we stand for, I think was political parties and maybe a little bit more tricky because they're expected to have an opinion on certain things.

Example Coke there's no expectation that they should have an opinion on everything, Yes there are certain things they do depending on what's related to them, Is check the Sugar Tax as an example, that something is relevant to the brand but the state of the economy is not something that's really want to them. When it comes to a political party they need to have an opinion and a substantiated opinion when it comes to everything, Which I think makes it more tricky Especially from a crisis comms perspective because they really really have to have a well structured structured plan and comment on what is their position on basically every type of topic because politics covers everything.

I'll be honest I don't actually follow any political brands on social media so I'm not sure of the tactics they employ, but I am familiar with the EFF on twitter, I know that they have a very active community on twitter and they're very protective of the brand on twitter. I'm not sure if it's the result of the party's strategy or if its a result of the community, but they've built a strong brand on twitter to the point that if you say something negative, there is this EFF twitter army that will defend them, but I'm not sure if its the result of the audience or actually an active tactic which is tricky. I think would also makes it tricky on social media is that if you're not the target market you won't see it especially if we're talking about advertising. Any brand that's using paid advertising we're not going to see it because we're not that target market. Obviously they're looking at a specific audience that they're trying to build an affinity with which you won't see if you're not part of that audience.

What I do think political parties should be wary of over engaging on social media, that's a general brand practice. Be active with your community and attend to queries, but be wary of spam. Like over communicating, that's a principal we follow with our brands, quality over quantity and have a structure and content strategy where you have three or four posts a week that are very powerful with a lot of substance, instead of twenty tweets a day. Always have a clear idea on why you're there, have a stance and try not to get involved where you haven't figured out your stance, especially if you have trouble aligning it to your overall purpose. If you fail to do so you come across very vague.

- *Are you familiar with communications crises that have been initiated by bot networks or fake accounts? If so, please describe an instance you're familiar with.*

We haven't experienced anything directly, you often hear of accounts that are bots and they're automating content and its fake profiles. From our perspective we deal with a lot of fake account work in the sense that we are often the guys that are escalating the issues to Facebook. Our clients often contact us and say you know these are the four accounts that are imitating the brand Please try to get them shut down, so we kind of, so a lot of the times we're not the victims of it but we see the repercussions of it and we try with the client to kind of solve it.

- *As a social media/community manager do you believe its possible to influence perceptions of those who come into contact with these misinformation campaigns on social media?*

Yes I guess you could but it's difficult right. The problem is that trust has been broken so as soon as people realise that they've been hacked For that the messaging was insincere And then you come back with guys this is what happened this is the situation It's tricky because now you have to rebuild the relationship Before they can trust you again So yes it is possible but it's a long-term recovery that journey that you have to take your customers on.

On a lot of our brands the problem is that Information on the internet is equal value. A consumer doesn't differentiate between what is more true than something else right, and this is a problem, we have a lot of problems with the some of the global brands where they will take content from another region and someone will go photoshop that image and make it come from the local market which is tricky because it look like it comes from the brand, it looks very authentic, it's got the brand name, if you research it you even

see there was some sort of incident but then the local instance was never touched by it. It was never a thing, so doxxing happens.

- *As a social media/community manager, how would you recommend political parties mitigate against misinformation campaigns initiated by bots?*

I think a brand needs to do, a simple thing to do is get all your accounts verified. Sort of like a nice technical thing is to you know, make sure that there's no confusion that you are the brand and that you are seen as the real account so getting that blue tick is a relatively simple thing, to get depending on how big your account is we've never dealt with political parties so not sure if they can get verified I would be my first port of call is to make sure that my account looks as reputable as possible. On an ongoing basis to a search for Imposter accounts report those accounts and try and shut them down And continuously communicate to your audience and community that these are you official channels. These are our official accounts and if you see anything that looks untoward from other accounts it's fake just ignore it. It's very tricky because with social media there's equal power across the board, so the only thing you can do is communicate, we're official, this is not official. I think another tactic that can be used is always refer back to a website, a credible web presence to reaffirm the credibility so say to your community, if this statement is not on our website, then it's untrue, at the end of the day it's a little harder to hack or impersonate a website. Don't be too reliant on your social media presence, try to push it to a website where you can have credible information and your community can also use it as a reference point as the truth of the brand because that is one place where you can control the narrative. A hub basically.

In terms of bots just disseminating information, I think you need to use data to inform your approach. You can use a social listening tool to do this. What a social listening tool does is it can track keywords for a brand so you can put in key sensitive topics as search terms, you analyse that and dependent on the volumes you determine if you want to engage or not. If topics are getting lots of volume and it's negative, then yes maybe I need to respond and attend to those, but if it's a small amount, it might not be feasible to attend to it directly, but the only way is to look at the data, analyse and then determine what you engage with and what you don't.

- *Do you believe that social networks are doing enough to reduce the impact of these misinformation campaigns?*

At the end of the day social media is this contradiction because everyone has freedom of speech. In my mind I think there's a limited amount of things that platforms can do because the more you do that the more you limit people's right to freedom of speech. So I think education is important from a platform perspective. A platform like Facebook needs to educate its community around the potential dangers. At the end of the day I'll be honest I think the responsibility lies with the consumer to figure out the real from the wrong, because I don't think the platform should be responsible for it. It's too big of a job and the more they try to limit that the more defeats the purpose of what social media is.

Respondent 7 Research Interview

- ***How long have you been a social media manager?***

So I've been on social since since 2007 and then my first of a job in social media was in 2010 when I did work for a telecoms company, then I did some work for a paid television service and then some strategy for another telco, mostly social strategy and content strategy. I currently do social media strategy for FMCG brands. Adding all my social media experience together I would say it's 6 for 7 years

- ***In your opinion what are key aspects of the work you do?***

So my current role entails deciphering a client brief then assessing what the current potential market for that client is and what that target market's digital footprint is and then to try plan messages that will reach those people both on a channel level and on an emotional level so whatever we post will resonate.

So on a macro level the key aspects of social media in general, I think one of the easiest answers is customer care on social media, we've become conditioned to think it's now a customer care channel. In general I think just being active and posting if you think of brands a normal person I think social exists as a middle funnel function. it's not quite going to close the deal but it's definitely helps a customer because they've been through and awareness they've now encountered your brand your brand because they follow you for whatever reason and then you sort of transition into harder marketing push onto them.

- ***Have you ever experienced a social media crisis?***

So within my professional work I've been fortunate enough not to experience a crisis but in my personal context I have. Before Twitter became the angry hateful place that it is now, there was a news story that Angelina Jolie had a double vasectomy because she had breast cancer. I was 22 at the time and I tweeted that Angelina without breasts is pointless, an industry colleague saw it and her friend had been diagnosed with breast cancer the day before. I backed down very quickly because the industry colleague was the first one who see it but from there it just spiralled out of control. If it had happened now i would be fired.

In some of my personal work in working in telecommunications I must say that the telecommunications brands are constantly hated on Twitter so it's not as singular crisis but eternal often there's a lot of hate directed towards telecommunications brands on social media and just trying to move that sentiment needle is almost impossible. What we found was there were two decided communities, there was one that would regularly engage every day, we'd put up find the phone puzzle and people would actually wait for it and we give like fifty bucks airtime or twot gigs, you know it was nothing really meaningful as a prize but its something that's better than work. Then you'd get people that would come in for individual issues, hi my phones stolen, hi my phone's dead, hi my phone won't work and it wasn't a finite crisis, but it was just trying to move that needle and up until the account left we never managed to lift the sentiment.

- ***How would one effectively manage a social media crisis?***

So i think initially it really is to understand what really is the problem that's going on here. Is it an employee issue, do people dislike an ad, what's actually the problem. If you're an agency partner then work closely with your client, because your client contact may not be in the department where the crisis emanates from, but it will be important to be close to them because they would have to bring the relevant managers in. Uhm, and then you need to begin engaging with influencers on the platforms as well as media partners to try and mitigate and contain the matter by saying look, this is our side of things and I think if possible engage the offended party possible offline and directly, like look, what actually happened, but in order to do that directly you need not only your marketing contact but also the relevant manager. We have an FMCG brand and one of their brands, which turns out to be a brand that we don't handle, did it incorrectly. They just shut down everything and it's kind of the argument that innocent people don't run but guilty people do, and it really got away from them, they weren't able to say look if you've got product, bring it to these locations, we'll get rid of it. They caught up with that after a week but the initially it got away from them. It also reinforced the notion that they knew that they had screwed up and it seemed like they were careless so they knew something was wrong. If they rather would have been transparent and said, look, we don't know what's happened but we're stopping everything and most times people are ok with that. If you look at the KFC debacle earlier on in the UK this year, they changed suppliers and couldn't meet demand so they had to close all their branches and they kept on putting out messaging like, this is what we know so far, this store has stock, and the one where they turned the whole thing around was when they took out an ad where the bucket of chicken said FCK instead of KFC and the brand manager, it must've been a hell of a thing to sign off an ad where your brand literally says fuck, in brand CI and everyone saw it and first thing they did was take out their phone, tweet it and it goes viral, but everyone came out smiling and the brand emerged

positively. They owned their crisis and they came out and gave an honest, human apology at the end. Social media is not real life, only a small part of the population is on twitter, but those people on twitter are a noisy bunch, they're naturally narcissistic and want to tell people their thoughts so not everything that's a crisis on social media is a full crisis, but if it becomes a full crisis you then need to bring in other channel partners and channel to deal with that. Enterprise is a good example, what they've done now is provide in store flyers showing that they've cleaned the factory. They've a real world crisis that started on social, contained it there eventually and now their messaging is totally in store, I notice that they haven't done it online. So there's room to use other channels, as digital people we rely on digital too much and forgot the real value that a great print advert can do.

- **Do you think there are any practices within corporate social media management that political parties could gain from?**

I think the fundamentals don't change whether you're a person, commercial brand or political brand. So setting up a voice, determining what you stand for and believe then communicate that, uhm, unlike a lot of corporate brands, I don't think political brands need to respond to every single response on social because the nature of that space is inherently emotional and in south africa people will be tweeting nasty things at the eff all day and the account doesn't need to respond to it, they don't need to respond to that, uhm, but I do think they need the same structures in place in terms of, this is who manages the account, this is the structure and hierarchy, and this is who gets involved in terms of a social media crisis. I think one of the things we don't think of and I've only just thought of it now, but a lot of corporates have individual social media policies in terms of how you may act as yourself. I think political parties should set those up as well. What are the holy cows that you may not touch uhm. It's like the DA, there's a guy in PE, Renaldo Gouws, his individual views are always clear, but they don't always align with the DA's views or policies. Its like our most followed people in South Africa are politicians, Razzmatazz is up there, Helen Zille, so what are those people saying, how are they acting, and is it in line with the party? You need a core party strategy and then to think of a strategy and a process for individuals as well.

- **Are you familiar with communications crises that have been initiated by bot networks or fake accounts? If so, please describe an instance you're familiar with.**

Uhm, the one that I've seen recently is the emergence of fake accounts going after individuals, so the one last week or the week before went after the cartoonist jerm, and an anonymous account tweeted work he had done years ago and asked his current employers like guys, how do you employ someone like this and it was pretty distasteful. The perpetrator had been hiding behind a fake account. What I've seen in the last few years is the general social media population wising up to identifying fake accounts and we tend not to react as quickly. There was a time around the trump election era, and then there were articles of the spear artist Ayanda Mamabulu dying in a hail of bullets. You'd have people say no, that's not a real account, look at the link, but still the odd person would still share it. As a population people are a lot better at calling that out, but any crisis stemming directly is not off hand, but one thing I can think of is MiWay, where an assessor allegedly wrote some defamatory comments about a customer who had had an incident and out of anger he basically faked an Email, so not sure where that falls into, but he created a crisis through fake content even though it was through his own identity.

What I've started to notice here is that we haven't had the mass botnets, there's currently a thing where there's BLF supporters and there's a net run from that but its not very sophisticated, the content chos and changes, it's not as sophisticated as the Gupta bots were and people spot it quickly and its multi racial, multi class people that spot it, everyone does.

- **As a social media/community manager do you believe its possible to influence perceptions of those who come into contact with these misinformation campaigns on social media?**

Yes, quite easily. In a post trump era, the first part is the segments that exist. There's this pyramid diagram that show the groups, left and right wing, that different media fall into, I think it has BBC and Bloomberg at the top as most trustworthy and centerist Breitbart in the bottom left and maybe Daily Beast on the bottom right, and people find what it is that sort of agrees with them and lean hard into that, so those silos exist and with social it's very easy to shut out what you don't agree with.

So what I'm not sure of and I know Cambridge Analytica did this, people who are one percent on your side, can you hook them? Because if they're one percent maybe we can move them to a two percent, I'm just not sure if we can nudge people who aren't interested in us as a political brand for sure. Yes I think it's a hard slog but possible, it's just easier depending where I am on the political spectrum in relation to you 'truthful' information, it's just easier for people to fall more and more into the confirmation bias.

- **As a social media/community manager, how would you recommend political parties mitigate against misinformation campaigns initiated by bots?**

I think a lot of it is know your enemy, know what you're up against, if there are short term tactics, like if you come up to a twitter bot network, umh, try and have relationships in place with the platforms so you can say, hey, we've come across these accounts and believe these accounts to be malicious, that enters the dangerous realm of ruling parties shutting down people they don't agree with, but that decision sits with twitter. The other thing that I've seen, and I'm just trying to think back to the trump situation is, and actually I think the Gupta campaign was so hard to defuse because there was a definite Golden Thread ad message that ran through all of it. As the media, rival political parties and citizens, we were fighting all these individuals, but that campaign definitely had a singular golden thread. So I think as a political party it's important to have the one thing you're standing on. We can see it miles away, with the EFF next year it's going to be land and every EFF person in this country, the only thing they will say is we want the land, you can say what you want until you're blue in the face. If you go online, be consistent, have a message and stand by it. If you respond to every troll, you'll never get to why people should think you're interesting and vote for you and your political party brand.

- **Do you believe that social networks are doing enough to reduce the impact of these misinformation campaigns?**

No, that's all you have to write, no. Uhm, twitter has a massive sexual harassment and terrorism problem and they say they're trying. Yesterday the New York Times came out with Facebook's latest screw up and its data leakage to other companies, which allowed marketers to see your personal data and share it on to other companies. The one thing I saw the other day, is the social media companies have all our data and why do they have that data and a google executive off the cuff said, and said, no one said we couldn't have that data. We allowed that data to manipulate us. Facebook have now signed with Africa Check in South Africa, umh but then it emerged recently in the UK that their truth partners were basically only used when there was a crisis and not to consistently monitor for malicious content, so are they doing enough, no. I think Facebook is the worst offender by many miles umh, google tried to clean itself up, but that more of a legal thing than an effort to genuinely clean up its act.

Respondent 8 Research Interview

- **How long have you been a social media manager?**

Community manager specifically, I started out in tech startups in Cape Town, I worked for a couple of incubators but the main one was a 88 mph. What 88 mph does is there look for startups in from Kenya South Africa and they basically operate as an incubator where they bring these startups into residency and they have specialist mentors from sales marketing and I was part of the team handling the social media. So a lot of it was community management some strategy setting up their profiles figuring out how they could

go to market using social media, yeah so I was basically the social media lead during that time. Incubator ended a few of the small businesses stayed on and I was consulting to them on a freelance basis. I was looking to move to Joburg then I found a permanent role at McCann The title for the role was community manager on a large Automotive account. I moved from community management, to social media manager, then senior social media manager and now social media director so int total I've been doing social for 6 years. In total I've worked on automotive, airlines, media a wide amount of industries.

- **In your opinion what are key aspects of the work you do?**

So currently my work revolves around business operations it centres around integration which covers planning it covers things like social media process and governance in addition to scope of work for new and existing clients. Another aspect is figuring out how we expand social into different departments within the agency. Then broadly speaking the importance of social media to customers falls under 4 categories. Data which is reporting and analytics, Strategy which are audits, social media strategies and playbooks. Then Engagement which is social influencers, community management, then you've got Content and production. The crux of it is from a omni-channel perspective and this is how you try to view corporate communications, as a brand you have a story to tell, so it really it lends itself to storytelling because you can reach any individual on their mobile at any given time. Without regurgitating what you've heard before and giving you the same sort of messaging, the honest truth is that social media is contextual advertising because you can serve the right message to the right person at the exact right time. The second thing about social media is these conversations are happening with or without you, so you can choose to participate in them and have some degree of control in that narrative or you could choose to put your head in the sand, but either way that conversation is going to take place. I think any misstep for any brand is about to happen it's just a matter of time, you can be the best brand in the world with the best story but something is going to break down at some point, but if you have an established community and an established reputation online, then I think being able to mitigate any mishaps or miscommunication or crises that come about may be easier. As opposed to O damn they mentioned us on social media we need to get on, let's go set up a profile and and and. So in terms of those two perspectives I think the one allows you to tell your story and the second is about being able to mitigate any issues that might arise for your brand. The thing about social media in corporate communications is that you sort of want to mimic people's native behaviours online. Think about it, if I have a great experience if I go to Old Trafford to watch a game, the first person that I'm going to message about my experience is my wife. By the same token, if I get into a problematic situation I want to get onto the phone and contact someone who's going to help me. It's the same thing if you have a problem, as a brand you can literally tweet something out and it's like sending a WhatsApp to thousands of people, there are 10 million people active online, so you can literally broadcast a message to millions, so if you're a brand like enterprise, you can literally get ahead of an issue by putting your public statement online.

- **Have you ever experienced a social media crisis?**

So yes and no, I've actually been pretty blessed over the past 6 years. It's never been to the extent of something where there's been loss of life. I think the one thing was with a food brand where there were issues with someone's food we got the PR team involved and that was handled fairly well. Another we had just inherited an alcohol brand, and as these brands usually do, they had an event with an instagram booth where people could go in take pictures and share them automatically. What happened was that someone went in with a very misogynist picture which made it look like the brand had generated the content but that was before we had the account handover.

Another issue was a campaign in which we generated a campaign against child and women abuse for 16 days of activism, because we did it for an alcohol brand we had to deal with some blowback in terms of people saying alcohol brands perpetuate abuse, other people also indicated that the campaign money would be better spent actually helping victims of abuse. To mitigate against these issues, which we anticipated, we actually set up a social media war room to check sentiment, have enough community

management hands on deck and have all the necessary people needed for approvals. I think we did fine as our sentiment over the campaign was positive.

- **How would one effectively manage a social media crisis?**

I'm fortunate in the sense that I'm part of a global network so I have a lot of this crisis communication IP that is handed to me and we have an entire chapter that's based on reputation management. How our agency structure works is that we have agencies within the network that support one another, so fortunately we have, or are connected to a PR agency which is one of the best in the world. Our mandate would as a first port of call be to involve our PR agency, but aside from that we have a crisis management protocol which every business should have and this has a number of scenarios which are informed by a frequently asked questions document. The emergency protocol then kicks in whenever something is over and above the FAQ. So I will community managers are able to identify when something is out of the parameters of the FAQ document and then the emergency protocol will kick in. So we've got what we call green, yellow and red level threats, It's a little organogram and it breaks down, If it's green then the community manager responds according to the FAQ. If it's yellow then they respond according to the FAQ but with each within each step they would need to notify and get approval from the client, on our side, those people will be the head of social, the head of client service, then it would be the marketing director and or the PR person, so everyone is notified and monitored over a period of time. In terms of identifying if something is yellow and red, we have a two page scorecard which asks a series of questions and grade the answers. Some questions for example are what is the size of that persons following, what is the severity of the issue at hand, and so you grade each answer and come out with a score and from that you'll be able to understand whether something is green yellow and red. When its red its extremely serious and we have to craft something with relevant stakeholders within two hours regardless of what it is, a response must go out within two hours of identifying the issue. This is something brands get wrong, because they don't communicate, at the end of the day, the more information customers have the calmer they are about situation. So firstly have a recognition of the problem, you don't need to have the answer. You can come in and say thank you for notifying us we have the PR team working on this and will get back to you as soon as we can. The second thing is keep it human, whats wrong with telling someone you have the entire business trying to figure the issue out. Brand will try to be too selective with what they put on social media, when they develop their brand personality and tone of voice, they will say we need to be human and authentic, but when its time to respond to a crisis then all of a sudden you revert to a corporate cold response and people are not idiots, they can pick up when you're not been authentic and I think there is scope for brands to be during crisis. So it's recognise, acknowledge, grade, inform relevant stakeholders which comes in the form of reaching out to the global network to find precedent on existing responses from similar situations, then we would craft the response with PR, legal, client, etc and while this is happening our newroom environment would go into crisis mode where we do live real time listening via the screens on our newsroom walls. So essentially what we do is set up relevant topics to monitor the crisis in real time and depending on the severity of the protocol we will gather the necessary approvals and then we do hourly sentiment reports, has sentiment shifted, what are people talking about and who is talking about it. Then finally you can look at pulling relevant influencers if there are relationships and try to discuss the matter in person with the person affected so they can get clarity or the full story so you can start to get ahead of it. The we can do daily, monthly reports until we're ahead of it. The last thing you want is to sit there and go, now what!?

- **Do you think there are any practices within corporate social media management that political parties could gain from?**

Lot's, Strategy. I don't believe any political party has a social media playbook and I will not take on a social media account with any brand in any country if it does not have a social media strategy and no one knows a brand better than the individuals in it, so we can craft one based on best practice in a collaborative process and you get to an outcome that's the best o of both worlds, and the reason I say this is because I don't believe you can be on social media without having these four five things. The one is a strategic objective,

why are you on social media in the first place, understand the end goal then you understand the means to communicate it. So if it is to generate leads, a lot of what you do will be steeped in paid media, you're making link ads and a lot of it is based on driving traffic to websites, It's all centred around user Journeys and user experiences, closing the feedback loop, and in addition to this you're focusing on customer care and how to bring the cells data in. In other words your end goal basically shapes your approach. So for political parties [your strategy] would be votes, like how do we get votes? There has to be an objective, there can be multiple objectives but the core one would be we need to win the elections and to do that we get people to vote. It can be above the line, billboard, PSA's, radio interviews, there's a whole ecosystem. Then on social one of those components can be buy-in and belief, we need to get people to buy in and believe, so how do they do that if they don't know what it is. The second thing is content themes and content pillars and this will come out of your marketing activity plan, which as a brand you need to have - these are the rallies we go to, these are the times we're on 702 and you map that out for the rest of the year which will help you leverage your bursts on social. Then your actual rally will have its own campaign strat, what are we doing before, what are we doing during and what are we doing after? Mmusi might know what he's doing next tuesday, but does the party as a whole know? It's important to map this out so you have alignment. Third point is tone and persona, so who is the DA what do they sound like, how did they show up online, then you have a consistency of that on their websites. Trick with political parties, and that's why a social media playbook and guide is so important is that it shows individuals how they show up online. In corporate you don't have a problem where employees speak for brands unless they're CEOs, in political parties there are individual representatives. So if Helen believes colonialism helped progress and Mmusi doesn't then they need to have an agreement that she won't bring it up, so you need dos, don'ts and guard rails. Then the last thing is an FAQ doc. To summarise, political parties need those four things and based on what I see online I doubt they have them. Then you can take it further and develop user journeys, how do we take people from awareness, to consideration, to usage and advocacy, then build it into your strategy, because thinking of these things will give you elements within your campaign to think about instead of bulk messages and cold calling.

- ***Are you familiar with communications crises that have been initiated by bot networks or fake accounts? If so, please describe an instance you're familiar with.***

When I know is pizzagate 2016 election Trump is going up against Hillary and Russia is already trying to influence it with their bots a specific piece of information comes out, so they're talking about Hillary's E-mail and how she had private government information hosted on a private server at her home. 2016 the FBI raided a government department and out of that A fake bot pretending to be a Jewish lawyer, leaked that the democratic party was working with certain corporates as part of a human trafficking ring. So these bots took those E-mails and communications and theorised that in the E-mails certain keywords were code for human trafficking ring. One of those E-mails mentioned cheese pizza which was said to be code for a child trafficking ring. It spread like wild fire and you had all these conspiracy websites and infowars publishing it as fact, so you had a whole investigation into democrats E-mails because of this.

- ***As a social media/community manager do you believe it's possible to influence perceptions of those who come into contact with these misinformation campaigns on social media?***

I don't think you can hey. To the point of computational propaganda and bots is to make people who come into contact with it think that there is a much higher proportion of it out there than what it actually is. Social media has an information hierarchy, people are talking about different things so you have a population of a million which is 100% and maybe 5% talking about sports, 10% percent talk about politics and what you do with computational propaganda is you're essentially making a conversation amongst a very small group of people seem a lot bigger than it is. If you can mobilise 3% of twitter to talk about something, it will seem like everyone is talking about it, so I think the bot's mandate is just that. From that perspective I think it's very difficult. You can get ahead of it and put out a factually correct statement, but can you mobilise hundreds of

people to share or change the narrative over time? I think you can do so over time because people forget a week later, they come and go very quickly, You can do is create resources that people can easily access where they can get the correct information and make it readily and easily available to as many people as possible. Then maybe you can work with influences and people with larger statures and get them to help you drive it, or you can make the information available to them and hope they do the right thing and reference it. If a bot comes out and says you're a rapist, and you say you're not, how do you defend against that aside from generating a fact sheet on what has actually happened. The other thing you get is polarisation of political beliefs, people are becoming more and more defensive of their positions - its difficult to change a persons perceptions in person, I'm not sure you can do it online. What happens is, the moment I see something that supports my belief system, I don't want to hear a counter argument, then I want to share it with everyone else to show them I'm right. People really want to share things that prop themselves up. There may be instances where people have been able to nip things in the bud, but I think the only thing you can do is make all the information available and give a link to it like snope, I think snope is amazing and I'm seeing more and more of it in threads where people are using it to debunk misinformation, the only problem then is that people will say snope is owned by the elistist leftist media and you can't get away from that. I do however think a disproportionate amount of these discussions are happening online.

- **As a social media/community manager, how would you recommend political parties mitigate against misinformation campaigns initiated by bots?**

So the points I raised earlier about making the correct information available is important, but what I would do to mitigate against misinformation if I were a political party, would be to bake the facts into every piece of communication that goes out and link to the information portal at every turn. It's important because that's where your media goes, so you just have subtleties in your communications to that debunk the misinformation spread about you. I think its hard for political parties because its easy to hate them online. Its harder for them than for normal brands because Mmusi and Helen have to make you like them and their party. I wan't to believe in Mmusi and then I see Helen and whats going on in Cape Town, there's a disconnect, so its harder for political parties. The other thing is why are political party personalities too personal, why don't they link out to the DA's manifesto at when ever they talk about party issues?

- **Do you believe that social networks are doing enough to reduce the impact of these misinformation campaigns?**

No, absolutely not. I think human verification is absolutely important, I think there is so much they can do, but what they tend to do is cherry pick the things they want to go after. Sort of Tumblr and nudity, on tumblr, they've removed artistic nudity and nipples, but you can get all the white supremacy content you want. The whole thing around infowars that helped galvanize the right against these platforms is because people were asking why are platforms censoring them and not doing the same on the left. There's always a gap between censorship and freedom of speech and it's really hard to find that line. I don't know, there's probably a lot of stuff they can do but there might be a need for more access to more information, you might need a trifecta of verification, information verification, location verification and device verification, but then it means, does twitter get access to your location, but even if you do that, they will find other loopholes to exploit it, like how there are now click farms with hundreds of humans with hundreds of devices and sim cards that are now bypassing two step verification. Apart from that facebook sells eyeballs, reach and frequency, if they have 2 billion people on facebook and five hundred or six hundred million of them are fake, then its not in their best interest to tell you or to get rid of them, so they're conflicted from a business interest point of view. It's never going to be perfect, but they certainly can do more. Big companies are pulling their budget in order to have transparency.

5.6 Appendix D: Political Party Interview Transcript

- **How important is social media to the communications performance of your organisation?**

In recent years we've had to sort of switch to be able to use social media platforms more efficiently and effectively as opposed to your traditional mediums we still do rely heavily on traditional mediums. As head of communications portfolio in the province and my other role and responsibility in the party is what we call the battle of ideas which to discuss and engage with society on critical issues and political discourse both internally and externally, both in the government and party, the goal is to interact with society. So we do engage with society a lot. Over the years we've had to be able to sort of adapt the way in which we engage, so it's almost got to be simultaneous. in the past We would just if you a press statement and be interviewed we now do everything at once so when I issue a written statement I also do a video recording of the main thrust of this statement as I know Society within gauge with it or media would engage with it we then also go to social media immediately and I also do voice recordings and different multimedia. so we've had to adapt the way in which we communicate because it's quick and because it's it's immediate everything has got to go at the same time to everybody. so the way we package our communication is to be able to prepare adequately for responses so possible issues that may come up in whatever we raise. So we sort of do a 360 turn around before we communicate anything, where as in I think in the past it was sort of a wait and see approach and it was because of the time lapse it was easier to prepare. Because there is no time lapse so now it's not as easy, so now you are often faced with things that you are not adequately prepared for. So the media space is changing and the way society engages with content is also changing quite rapidly and I think political parties have got to adapt if they want to stay relevant and I think as ruling party we have more of a responsibility to do it because we're the governing party as well as a political party. It's not always easy to make that distinction but we try to. social media is very critical a large amount of the population engages with social media as opposed to those that engage with traditional forms of media and also it's younger people that engage with social media. SOe let me talk about Gauteng specifically, in Gauteng we have the highest population of the country concentrated in the smallest area space and the majority of those are young people, so if you really want to reach citizens and interact with them and have meaningful public participation at government level, you've got to use it. So we do have a monitoring system we monitor media as a whole and a big part of that is social media so we monitor the reach we monitor the the interactions we monitor the negative, the positive we monitor the issues that come up as people engage. me we and then when there's topical issues outside of relation periods we monitor that as well we do have agencies that assist us depending on the periods that we in so for elections we do because I'm election strategy is based on research so we do have agencies that we use but outside of elections we do make use of agencies but not to the extent that they are responsible for campaigns but during elections they would be.

- **What do you see as the largest social media threats to political parties?**

I think not just in social media but in media as a whole is fake news anybody can create content in anybody publish content, so the security of content Is not really, well there is no security of content really so because of that you have to build your reputation and credibility. Branding and Imagery, PR, your image management becomes very important so that people know by looking they can pickup what is fake and what is not I think we getting better at it so for instance the use of official accounts for content centralising communications has helped so in the ANC you have dedicated spokespersons during elections it does get a bit blurred because of the amount of work that we do on a daily basis but still the communication lines are quite defined in ANC.

So in each structure there's a political head responsible for the content so what's the office of the secretariat so its the secretary and their deputies and the spokespersons so the three of us are responsible for everything that goes out so you would have people at create content with its visual content it doesn't matter but it goes out on approval on approval of the political principles that's really how we do it and where you may have seen or what it doesn't happen and political principals haven't approved it then we're quick to say that this is staff of the organisation or this is whatever. it does create a bit of a PR mess sometimes but but we do this own PR content that's not approved.

in terms of managing political vs party brands we all work in one team so that we have as much energy as possible it's not always easy to do because for instance there would be things that the president as an example

would be responsible for in his official capacity completely so for instance today he's gone to Mozambique and that is his responsibility as the state president the ANC May or may not be aware of it at all and if it is purely because it's there to state it doesn't involve the party at all but we do he's communications teams he doesn't have a presidency communications team in an ANC communications team his communications team or with him 24/7 so we do work together it's just that at times the answer may not be aware of what he's doing. another threat is the Blurred Lines of party position vs personal views year so an official of the party would say something which eye is personal views which he has a right to to do but if they struggle into areas of policy it becomes really difficult so that's always a threat it's not possible to have everyone singing from the same hymn sheet we do have communications protocol it's in black and white it's approved everybody has them but you're not always always able to police human behaviour at the end of it so you find yourself always having to put out fires or reminding people what they can and can't do I think another threat especially for an organisation is because I was is not using or when internal mechanisms are not as effective as they should be you then find members turning to social media to other fuse and Express frustrations and irritations and that sort of thing so the management of of internal conflict is not easy it's always under threat

- **Are you familiar with social media bots?**

I am [laughs] yeah there's quite a lot of them I guess they serve a particular purpose it was certain extent sometimes they say things that people want to say but can't so the anonymity allows them to to say what they want to say what they want to ever they want. that's all I can say about but I think there's always a a fight between big parties saying that the DA has a whole team of of bots they say the same thing about us yes it's of course I mean it's impossible to to trace and police and that sort of thing so people do get away with a lot.

- **Has your party been affected by misinformation campaigns by political bots?**

Not misinformation a lot of stuff that supposed to stay internal finds it's way out through Bots so not really fake stuff [laughs] they actually say lot of true things, and its not stuff that people aren't supposed to know, its information that will come out eventually so it's like leaked.


- **If so, how were you able to indentify these attacks?**

it's the way they operate it's immediate they are issued based and they pick on certain things all the time its easy to identify.

- **Do you have any plans in place to mitigate against the actions of social media bots and the spread of misinformation?**

sure I must say not that I know of if it's there it's top secret high level stuff but I don't know anything about that yeah so I think everybody struggling with it and I don't think anybody is got an absolute answer as to how to deal with them. As a party we don't have any relationships with the social networks, maybe as a state, but not as a party.

5.7 Appendix E: Communication Misalignment




Nickolaus Bauer ✓
@NickolausBauer

Following ▾

“Unity! Maqabane! Unity! Phakama!” @MYANC

[Translate Tweet](#)



Mzwandile Masina
@mzwandileMasina

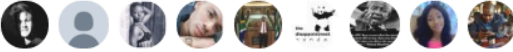
A SARB single-minded focus on inflation, especially in a country like South Africa with high unemployment and underemployment is wrong and unsustainable period.


15:10 · 2019/01/18 · [Twitter for iPhone](#)

13 Retweets 34 Likes

3:48 PM - 21 Jan 2019

6 Retweets 9 Likes






Tito Mboweni ✓
@tito_mboweni

[@mzwandileMasina](#) : ok. Here is the simplified Mboweni idiom: OPEN YOUR BRAIN FIRST BEFORE OPENING YOUR MOUTH! This means for example that don't say things about the SA Reserve Bank before you know what the Bank does! Ok? Helpful? See you at the NEC Lekgotla!!

23:52 · 2019/01/17 · [Twitter for iPad](#)

Tweet



Mzwandile Masina
@mzwandileMasina

I'll argue any day that my brain is always wide awake and I never talk about things I know nothing about [@tito_mboweni](#)

18:43 · 2019/01/18 · [Twitter for iPhone](#)

35 Retweets 129 Likes

4 6 9



Nickolaus Bauer  @NickolausBauer · Jan 21
 “Unity! Amaqabane! Phakama! Phakama!” @MYANC



Tony tornado Yengeni @tyengeni1... · 1d 

Some political prostitutes with huge ambitions believe that they can shut me down here on Twitter..terrible mistake..infact they are urging me on..! I have not even started..this is just the beginning..!

 130

 187

 513



Fikile (Mr Fearfokkol)  
 @MbalulaFikile

Replying to @tyengeni1954

If this was refering to me i will respond decisively.

06:43 · 2019/01/21 · [Twitter for Android](#)

 19

 37

 56



UNIVERSITY OF JOHANNESBURG