Cybertrooping and the online manipulation of political communication in Malaysia: The Barisan Nasional years

NIKI CHEONG
(Peck Beng Cheong)

Thesis submitted for the degree of Doctor of Philosophy

Department of Cultural, Media and Visual Studies,
The University of Nottingham

August 2019

For my mother Tammy,

and in memory of my late father, Alex.

DECLARATION

I hereby declare that this thesis represents my own independent work, except where referenced to others. It was carried out in accordance with the regulations of the University of Nottingham.

I further declare that the work in this thesis has not been previously submitted for any other degree.

Niki Cheong
30 August 2019

ABSTRACT

This study examines the illiberal practice used by state and political actors in Malaysia—known as 'cybertrooping'—to manipulate communication practices and information flow on the internet while Barisan Nasional—the political coalition that had ruled the country since independence in 1957 until May 2018—were in power. It contributes to existing scholarly work on 'computational propaganda', 'astroturfing' and 'trolling', including the many studies that emerged following the political developments globally since the United Kingdom EU referendum and the United States Presidential Elections in 2016. This thesis argues that cybertrooping can be understood as an extension of a political party or state's illiberal attempt at orchestrating a covert operation aimed at gaining or retaining power beyond media control and the threat of legislation, often referred to as the 'chilling effect'. It will argue that cybertrooping extends known methods historically associated with political communication, including propaganda, public relations, spin and psychological operations, aided by internet affordances.

Central to argument developed by the thesis is the analysis of a dataset of 125 pseudonymous emails—many of which were labelled "Online Deployment Strategy"—which consisted of instructions for social media engagement ahead of Malaysia's 13th General Election in 2013. This dataset is likely the first direct empirical evidence of its kind to be studied in a field where researchers face difficulties investigating a covert practice, and have to rely mostly on whistle-blowing and leaks, lawsuits for access to official documentation, investigative journalism, and the use of computational data science methods, to infer knowledge. In addition,

analysis of over 400 news reports helps contextualise the mainstream understanding of cybertroopers, while an analysis of thematic patterns from Twitter data mined during street protests in Malaysia builds on the findings from the emails. These other sets of data—alongside interviews with politicians, journalists and activists—were used in the triangulation process.

On the basis of the analysis that the study undertakes, this thesis will provide an empirically-informed definition for cybertrooping. Given the seemingly increased use of 'sockpuppetry' and 'social bots' in the global political landscape, it is hoped that this definition will contribute to future research into similar practices being used by state and political actors in other parts of the world.

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

This thesis could not have been completed without the mentorship, advice and support of my two supervisors, Jennifer Birks and Andrew Goffey. I have learned so much from both of you over the past four years.

My gratitude to The University of Nottingham for the Vice-Chancellor's Scholarship for Research Excellence (International), which allowed me to embark on this PhD journey. I am also grateful to all the academic, administrative and support staff, especially those at the Department of Cultural, Media and Visual Studies. Specifically, I would like to thank Franziska Meyer who offered much support and pastoral care as Director of Postgraduate Research.

I would also like to thank Tim Jordan and Matthew Allen, who planted and sowed the seed for starting my PhD studies (and have written numerous reference letters over the years).

I was warned to expect a very lonely experience as a doctoral student but my experience has been anything but. A massive thank you to my 'buddies who lunch together': Emma Humphries, Louis Cotgrove, Siqi Wang, Sam Wilkinson, Abi Rhodes, Ivan Markovic and Betti Bodi. I want to especially thank Robert Stenson, David Young and Gareth Shaw for the conversations and constant encouragement.

I am also grateful to my current and former colleagues at the university for their friendship and solidarity: Judit Varga, Victoria Gerstman, Lilia Abadia, Sia Bakhtiar,

Claire Burdfield, Emily Rees, Sungil Ko, Tom Daw and Zhun Gu. Then, there are my colleagues from the Digital Culture Research Network that we set up together.

My gratitude to Giuseppe Sollazzo for his guidance with the computational elements of my study, as well as Alex Bryne, Amelia Johns, Gayathry Venkiteswaran and Paul Byron, all of whom have offered feedback on parts of this thesis.

Moving so far away from my homeland in Malaysia, and taking four years off full-time work, was not easy. I want to thank Vivienne Lee for her generosity of heart and spirit, Low Ngai Yuen for cheering me on, and Ivy Soon for simply having faith in me on the days that I had little. A big thank you to Jason Lioh and Ee Soon Wei for stepping up when I most needed them.

My friends Angeline Cheng, Ryan Lewis, Adam Ivey, Robert Pike, Justin Ling, Alan Ho, Danny Holland, JD Raitt, Justin Khoo, Mike Webster, Nick Carter and Nazri Idzlan offered me a bed and fed me whenever I needed a break and to get away. And to my aunts, Yvonne Nah-Foley and Angeline Taye Jarratt. Thank you all.

To Stephen Dolphin, who has been there at every point of my life over the past four years. I am so grateful, and glad, that we are the best of friends.

Finally, I am eternally blessed for the love, support and reality checks (and the many video calls) from my family: my mother Tammy, my sisters May and Phaik Geok, and my brothers-in-law Mizuan Manaf and Rizal Razman. Then, there are the 'kids'—Sara, Adam, Ali, Isa and Ayub—all of whom shower me with so much affection.

I dedicate this dissertation to the memory of my father, my intellectual hero, who was around when I started but sadly, not here to witness the end of this journey.

LIST OF FIGURES

LIST OF TABLES

ABBREVIATED TERMS
(AND SELECTED GLOSARY)

BN Barisan Nasional (National Front), the ruling coalition in Malaysia since independence in 1957 until May 2018 (originally known as The Alliance)

UMNO United Malay National Party, the largest of the three major parties in Barisan Nasional

MCA Malaysian Chinese Association, another of the three major parties in Barisan Nasional

MIC Malaysian Indian Congress, the final of the three major parties in Barisan Nasional

PH Pakatan Harapan (Alliance of Hope), the ruling coalition in Malaysia since May 2018 made up of several former opposition parties

DAP Democratic Action Party, one of the major parties in Pakatan Harapan

PR Pakatan Rakyat (People's Alliance), the previous opposition alliance during the 13th General Election in 2013

PAS Parti Se-Islam Malaysia (Malaysian Islamist Party), the opposition party that was formerly part of Pakatan Rakyat

PPBM Parti Primbumi Bersatu Malaysia (Malaysians United Indigenous Party), the new party led by current Prime Minister Mahathir Mohamad

RBA Red Bean Army, alleged 'opposition' cybertrooper group DAP denies funding

ISA Internal Security Act 1960, which allows for detention without trial

PPPA Printing Presses and Publications Act 1984

SOSMA Security Offences (Special Measures) Act 2012

ODS Online Deployment Strategy

NOTICES

Note on transcriptions and sources

All quotations derived from the datasets and other online content appear in exact form—including spelling and grammatical errors—as the originals. Quotes in Bahasa Melayu [Malay Language] are italicised, with my English translations[1] provided in square brackets, where relevant. All other emphasis in these quotations—italics, bolds, underline—are noted within the text if they were copied verbatim from the source. Any modifications made by me either appear in square brackets, or noted in text. Where quotes are directly used, they are listed in the list of references. In the case of news reports analysed in Chapter 5, a full list is offered in Appendix I. Emails from the Beruang Biru dataset are cited in text by date received.

The following article includes research presented in this thesis:

Johns, A., & Cheong, N. (2019). Feeling the Chill: Bersih 2.0, State Censorship, and "Networked Affect" on Malaysian Social Media 2012–2018. *Social Media + Society*. https://doi.org/10.1177/2056305118821801

[1] I am fluent in Bahasa Melayu, having studied with the language as my medium of instruction in primary and secondary school (examined up to the equivalent of O' Levels).

Introduction

Enter the cybertroopers

1.1 An invitation to be a cybertrooper

In 2011, an acquaintance asked me out of the blue if I was interested in being a cybertrooper. At that moment, I was not sure if it was a serious offer, but dismissed it immediately. A journalist at that time, my instincts were that it was not the kind of work I wanted to be associated with. Later conversations with mutual friends—active, politically-aware social media users who included former politicians and media practitioners—concluded that it was likely a genuine proposition. Since my refusal of the offer, however, several questions remained in my mind:

What would the role entail?

Who would I report to?

How much can I expect to be paid?

Why do they do the work they are tasked with?

At the time, I was part of the self-labelled Malaysian 'Twitterati'. I was the author of a popular long-standing column for the country's largest English daily, *The Star*, about growing up in Malaysia, and had written one of the earliest full-feature articles introducing Twitter for the newspaper. That, together with the fact that I was an early adopter of social media, meant I was perceived to be part of an elite group of social media users, who were later termed by marketing professionals as 'influencers'. My assumption is that this public profile was what led to me receiving the invitation to be a cybertrooper.

Over a year after that invitation, a seemingly odd series of emails flooded the email address that is listed on my professional website. I was used to receiving unsolicited mail in that inbox, but these emails were different because there were so many of them from the same pseudonym: Beruang Biru (or Blue Bear in Malay). The emails also stood out because they contained content related to politics, with most being in support of Barisan Nasional (National Front), the ruling coalition in 2012. It was also significant because among the list of addresses the emails were sent to include renowned political bloggers in Malaysia. I had previously heard rumours about some of these individuals being pro-Barisan Nasional cybertroopers.

None of my 'influencer' friends reported receiving these emails. Unable to ascertain the reason for my inclusion into the mailing list, I concluded that it was probably the same reason I was offered the cybertrooper role. There was also the fact that the newspaper I had worked for, *The Star*, is owned by the Malaysian Chinese Association (MCA), one of the three major political parties that make up Barisan Nasional. In a country with media restrictions, it was possible that someone working for that newspaper was seen to be an ally. When the Beruang Biru emails started appearing, I was still contributing articles regularly to the newspaper, although I was no longer living in Malaysia, much less employed full-time at *The Star*.

My instincts told me not to delete the emails; instead, I moved them into a folder as I received them over the two-year period where they remained ignored for the most part. I was in the midst of reading for my MA in Digital Culture and Society at this point, a move into academia I had made to help me understand and contextualise—at least academically—the work I had been doing in previous years at *The Star*, focussed on adapting the newsroom for the digital age. One of the biggest issues I

struggled with was the question of how the pervasiveness of social media was influencing news production. My MA dissertation investigated the nature of social ties on Twitter, and the trust issues that emerged from that with respect to the dissemination of news. Media outlets around the world—*The Star* included—were increasingly relying on information online as a source and Twitter trending topics were dictating news cycles. As a journalist who was also an active user of social media, I found the complexities of trusting information online to be fascinating.

The case study I selected as the focus of my MA dissertation research was the Bersih 3.0: *Duduk Bantah* [Sit-In] rally in Kuala Lumpur, which took place on 28 April 2012. Bersih, which means "clean" in Malay, was a significant social movement calling for free and fair elections, and was at the time, changing the landscape of Malaysian politics. The analysis of the tweets mined for the study showed a series of identical posts opposing the Bersih rally sent from different accounts. This behaviour struck me as unusual, but it was not within the scope of the research project to examine this occurrence more fully, and so I noted this finding in the conclusion as a potential topic for further study. Indeed, that little bit of data got me thinking again about the questions I had about cybertrooping mentioned earlier, which led me to writing a PhD proposal on the topic.

It was around this time—October 2012—that an email I received from Beruang Biru stood out among the others I had received before. It was the first email to request an action from the recipients, which was to click on a link that led to a YouTube live chat with then-Prime Minister Najib Razak, and to click on the 'Like' button as many times as possible. Najib was answering questions live online and clicking 'Like' was an attempt to balance out the negative feedback he was receiving. Suddenly, the

Beruang Biru emails became more fascinating, and I wondered if they would help answer some of the questions that had lingered in my mind since receiving those first emails.

I began my PhD studies in 2015, almost three years after receiving that email. By then, the government had clamped down further on freedom of the press and expression. In 2014, politicians, journalists and activists critical of the government were arrested or charged in what has become known as the 2014 Malaysian "sedition dragnet" (Grudgings, 2014). In August 2015, the Bersih movement for free and fair elections held another street rally (Bersih 4) which ran for 48 hours ahead of Hari Merdeka [Independence Day], with the additional call for the resignation of Prime Minister Najib.

I once again mined for tweets during Bersih 4 to see if the data would show similar patterns of cybertrooping I found in the 2012 Twitter dataset. Beruang Biru's emails and these two sets of Twitter data would become the primary datasets for this PhD research project, which will be presented in this thesis to answer some of the questions about cybertrooping I have been asking for years.

1.2 Demystifying the cybertroopers

This PhD research project is a study into the practice of cybertrooping in Malaysia until Barisan Nasional's loss of power in May 2018. It contributes to the expanding scholarly work on manipulation of information on the internet such as literature on 'astroturfing' and 'trolling', among other terms, that have existed for a decade. Previously, less liberal countries were the main subject of study (Al-Rawi, 2014;

Albayrak & Parkinson, 2013; Hung, 2010) but there is an increasing prominence of studies on traditionally liberal countries, and transnational efforts of manipulation, since the United Kingdom EU referendum and the United States Presidential Elections in 2016 (Benkler, Farris, & Roberts, 2018; Bennett & Livingston, 2018; Woolley & Howard, 2017). Academic work referring to Malaysian cybertroopers emerged around the same period (Hah, 2012; Mohamed et al., 2011; Tapsell, 2013), although the earliest public mention of the group dates back to reports in Malaysia's *New Straits Times* in 2004 ("Umno Youth goes on cyber-war footing," 2004).

This thesis (and the findings that it presents) aims to further develop the current understanding of cybertroopers, both historically (reports of cybertrooping in Malaysia pre-date 'social media', as we currently understand it, and included engagement on Yahoo groups, mailing lists, blogs and forums), and presently, by offering an operational definition to better understand this practice seemingly adopted by political parties and states globally. This definition is important because the context in which manipulation occurs differs geographically, and in each situation, different tactics are adopted depending on the use of different platforms (not all of which can be considered social media). It also intends to contribute a way in which scholars can think about this global practice through conceptual, operational and practical frameworks.

In response to the objectives mentioned above, this thesis sets out to investigate the way cybertroopers try to influence and manipulate communication practices and information flow in the Malaysian political sphere, and how they operate as an online extension of the state's control mechanisms to secure or retain power. It does not attempt to examine the reception of cybertrooping practices, but is instead interested

in the operational aspects including the strategies and tactics involved in the production, dissemination and amplification of political information. To answer the research question above, and guide the analyses of the empirical data, this thesis will aim to:

- Examine instances of cybertrooping in Malaysia and identify how cybertroopers are mobilised.
- Explore the activities cybertroopers engage in, and locate these within the current understandings of political communication tools and strategies.
- Use the findings of the case study to understand and contextualise the global phenomenon of online manipulation of political information.

The study is organised around the qualitative analysis of the two major sets of data mentioned earlier in this chapter: the series of emails from Beruang Biru and the two collections of Twitter data from the period of the Bersih rallies held in 2012 and 2015. To support the findings, and to provide further context, this study also includes an analysis over 400 news articles from media organisations in Malaysia and Singapore which discuss, or refer to practices associated with, cybertrooping. Interviews were also conducted with politicians, activists, and journalists; first in 2015, during the early stages of this study, and then in 2018, after Barisan Nasional's historic loss at the general election. Other data collected through internet research methods is also used.

In this thesis, I will argue that cybertrooping is an illiberal practice of online manipulation of information in Malaysian politics, primarily used by Barisan Nasional to retain power. The cybertroopers who engage in this practice are generally

centrally-mobilised, with message directions being passed through a top-down hierarchical structure. Where this practice differs from general persuasive action commonly found in contemporary politics is that the said directed messages are not distributed by accounts linked to Barisan Nasional, nor from any individuals or organisations directly linked to the coalition. I elaborate on this point further in discussions in this thesis about how some emails from Beruang Biru explicitly instruct official accounts linked to the party or government not to distribute certain materials. Alongside the discovery of sockpuppet accounts, these discussions lead me to conclude that cybertroopers can be considered as front-groups for the ruling coalition, allowing Barisan Nasional plausible deniability.

That the political party would engage in such covert activities to dissociate itself from the practice potentially speaks volumes about how insidious they consider practices of online manipulation, considering that the government has long use repressive tactics including controlling the flow of information through arrests, media control and censorship. These covert activities mean that citizens who consume the information are "not informed" of the 'organized persuasive communication' (Bakir, Herring, Miller, & Robinson, 2018, p. 9), and as such, have been subjected to deception.

In the theoretical framework that guides this thesis presented in Chapter 2, I make the case that deception runs through the various activities that existing literature has associated with online manipulation of information. This is also the case with cybertroopers; the strategies they use go beyond just the dissemination of information and include the use of existing information manipulation techniques such as propaganda, public relations, spin and psychological operations. They adopt,

and adapt, these techniques by taking advantage of the internet's affordances and 'mark-up culture' in their attempt to influence, amplify, and manipulate public sentiment in favour of both Barisan Nasional and the government, and to demonise their opponents.

In the Malaysian context, the use of this deceptive practice is significant because for decades, the country has attempted to find legitimacy in the eyes of the world through the veil of democracy being in effect, despite its record of supressing opposing voices being well documented. Cybertrooping—if gone unnoticed—would have allowed Barisan Nasional to get away with its attempts at manipulating the public. The conflation between political parties and the state in Malaysia from having been governed by one entity since independence is also indication of how much more of an assault cybertrooping is as a practice on citizens. This blemish on a country's perceived democratic credentials also allows for the Malaysian case study to be extended into understanding other geographical context, particularly with the more traditionally liberal countries. The risk of being labelled perfidious could explain why governments and political parties in power in countries like the United States and United Kingdom have reacted so strongly against whistleblowers who exposed those countries' adoption of similar manipulative practices, showing them to be less liberal than they have been previously claimed or perceived to be.

In short, I will argue that cybertrooping is a form of what Bakir et al. (2018) would consider 'non-consensual' organised persuasive communication due to the deceptive nature of its operations, setting it apart from online promotional culture and other more known political communication practices presently found in politics, and thus rendering it an illiberal practice.

1.3 The structure of this thesis

In this chapter, I have begun to introduce cybertrooping in Malaysia—the central focus of this research project—and to locate the practice within its local and global context. I have also offered a personal reflection of the journey that has led me to this research project, while detailing the primary datasets that inform the study. This chapter has also set out the research question and aims that guide this research project.

In the next chapter (Chapter 2), I will present a comprehensive review of existing scholarly work surrounding the practice of cybertrooping. The chapter begins with an overview of literature on state-control of online information including censorship, ownership and harassment. This discussion then leads into the instances of online manipulation of information in various contexts, and the debates surrounding the concepts and practices of 'trolling', 'astroturfing', and 'computational propaganda', among others. Following this, the chapter aims to contextualise these practices within understandings of the more traditional practices related to information manipulation in political communication which pre-date the internet. Thus, studies of propaganda, psychological operations, public relations and spin will be canvassed and included. The review will inform the development of a theoretical framework for the analysis and interpretation of the data collected.

Chapter 3 will outline the methodological decisions that were made for the purpose of this thesis. The chapter will also offer a thorough introduction to the various datasets used in this study, including details on the collection of data, method of analysis, limitations of the study and the ethical considerations that were made.

The five chapters to follow directly address the case study. Chapter 4 will provide critical insight into Malaysia's political landscape as well as the country's complex history with information control and political communication. This includes the state's reliance on illiberal practices such as cybertrooping. It will also offer background information on the various political parties which will be discussed in this thesis, as well as on the Bersih social movement, to provide context for the datasets used in this study.

Chapter 5 will be the first chapter to present the findings from the analysis of the various datasets. It will turn to the 403 news articles from media outlets in Malaysia and Singapore to examine the extent of the mainstream understanding of cybertrooping. The news reports also allows for the understanding of how cybertroopers are publicly framed through the analysis of quotes attributed to political leaders on both sides of the divide. This chapter sets up a series of questions related to cybertrooping that can be tested and verified through the analysis of the other datasets, to be presented in the succeeding three chapters.

Chapters 6 to 8 present findings primarily from the analysis of the Beruang Biru emails and the Bersih Twitter datasets. The first of these chapters makes the case linking Beruang Biru to Barisan Nasional, and discusses the dissemination and amplification of information in the dataset, the most readily identifiable tactic mobilised through the emails. Having established such a tactic, the chapter will present similar instances of cybertrooping found in the Twitter datasets. Finally, the chapter will explore the distinctions between cybertrooper (including social bots) and genuine accounts.

Chapter 7 offers two major discussions. First, it presents an investigation into the Beruang Biru emails to argue that cybertroopers are mobilised in a top-down structure, and operate as part of Barisan Nasional's extended communication strategy that goes beyond the digital space. Secondly, the chapter goes on to discuss and characterise other strategies and tactics used by said cybertroopers beyond what was presented in Chapter 6. This includes brigading and spamming, the use of sockpuppetry and memetic signifiers, and the hijacking of hashtags.

Finally, Chapter 8 offers insights into the cybertroopers messaging strategy. It begins by examining the categories of materials provided by Beruang Biru to make the case that cybertroopers are given the option of which 'message style' they would like to use based on their intended public personas. The chapter posits that these categories are used by Beruang Biru to guide recipients of its emails on which topics can be associated with which accounts. This is followed by a discussion—based on the framework presented in Chapter 2—on the different types of messaging strategies cybertroopers use to achieve their different objectives.

Having now presented a clear understanding of how cybertroopers operate and are mobilised, Chapter 9 will conclude this thesis by situating the findings from the Malaysian case study within the existing knowledge discussed in Chapter 2. It will also offer a framework that can be used when thinking about cybertrooping-like activities around the world from operational, conceptual and practical perspectives.

The original contribution of this thesis to knowledge lie in studying online manipulation empirically, especially through a unique dataset in the form of the Beruang Biru emails. The findings will add to the currently-limited empirical studies on the practice used worldwide, particularly in the context of a quasi-democratic

country. This research is even more pertinent considering that there appears to be an increasing reliance on illiberal practices similar to cybertrooping in traditionally democratic nations. In this regard, this thesis will also contribute to the growing literature on methods of control in both 'liberal' countries and semi-democratic states, as well as the growing discourse surrounding disinformation, post-truth politics and the role of 'fake news' globally.

CHAPTER 2

Online manipulation of political information

This chapter will be presented in two parts to situate the research conducted and present the theoretical framework that guides this study. The first part is a discussion of existing literature related to the online manipulation of political information by political and state-linked actors, while the second part presents the framework and tools that will be used to analyse the data to answer the research questions set out in the Introduction chapter.

2.1 Situating the research

This part begins with an overview of the impact that the internet—and social media particularly—has been argued to have on the communication practices and the flow of information, specifically within the context of politics. It then discusses arguments about the ways political actors and institutions control and disrupt the internet to retain power. One of these methods, increasingly addressed in scholarly literature, is the manipulation of political information through practices commonly referred to as astroturfing, trolling and computational propaganda. This will then lead into a brief discussion of cybertroopers—known in Malaysia to engage in the aforementioned manipulation activities—and the manner in which this topic has been tackled by scholars and commentators, which make up the main case study for this thesis. Notably, very few past studies have had access to primary empirical data—this issue of accessibility poses difficulties in researching online manipulation of information—

leading to a general reliance among scholars in the field on secondary data such as news reports to infer knowledge. That said, this chapter acknowledges that relatively new research methods involving big data and computational science have contributed to advancing the way the field is being studied in the absence of more detailed empirical evidence. In the instances that such evidence exists, it often refers to particular geographical contexts. While these studies provide an understanding of practices related to online manipulation of information in different contexts such as country-specific or regime types, they also collectively contribute to the building of a more detailed understanding of online manipulation of political communication.

2.1.1 *The role of the internet in politics*

This section will begin with a discussion of the increasing reliance of political actors on the internet. This will be followed by an exploration of literature suggesting that attempts to control communication practices and the flow of information in online spaces have become part of contemporary political life.

Political actors—be they individuals or institutions—rely on the dissemination of information and engagement with their publics for political survival. This happens across the various spectra of government, from liberal democracies to authoritarian regimes. In the historically more liberal countries, core to the democratic process is political discourse, alongside the freedoms and structures to engage in it. In less liberal countries, such discourse may be stifled although leaders are often cautious to be overtly seen as doing so for fear of accusations of illegitimacy both from the global community as well as domestically from their citizens. After all, history has shown the impact of networked mobilisation of outraged publics (Castells, 2015;

Gerbaudo, 2012), some of which have led to the downfall of authoritarian politicians and regimes including Joseph Estrada in the Philippines, José María Aznar in Spain, and the Communist Party in Moldova (Shirky, 2011). As such, to remain in power, political actors must convince the public that they are the best people to govern and often, this requires them to win the 'information war'. This 'battle' usually relies on the use of creative methods to push through their respective messages, often even at the expense of the very same citizens they seek to win over.

For over two decades, scholars have argued that the internet—and specifically social media—played a key role in this information war. These technological developments have been recognised for their role in changing the political landscape, both in domestic settings and transnationally. Internet technologies have made information increasingly pervasive, leading scholars to argue that communication has become more participatory (Lievrouw, 2011; Rheingold, 2008; Shirky, 2011). Politicians and leaders around the world have been forced to adapt the ways in which they have traditionally engaged with their citizens as a result of this seeming democratisation of communication practices and information. As a result, they have had to learn to manage the ways in which citizens, taking advantages of the ubiquity of internet technologies, are responding to them.

Scholars have explored the many ways citizens have disrupted the political landscape by using the internet, particularly when it comes to responding to state oppression and injustice—perceived or otherwise. The proliferation of websites in the mid-90s, for example, led to the emergence of online news sites, which served as an alternative to, or independent from, mainstream media (Gillmor, 2006; Goode, 2009). Journalists at these sites, in some countries like Singapore and Malaysia, engage in

what George (2006) refers to as 'contentious journalism' as an attempt to resist government control (see also George, 2005; Steele, 2009). The proliferation of blogs, and later social media, following from the use of online forums, saw the emergence of citizen journalism (Gillmor, 2006; Gomez & Chan, 2010; Goode, 2009). Researchers have claimed that the 'participatory culture' of the internet has helped the 'Davids' battle the 'Goliaths', particularly in countries where fighting injustice can be an expensive affair due to civil laws being used by those in power. Through efforts mobilised online, citizens who have fallen victim to the elite, such as in Indonesia and Singapore, have managed to fundraise to support their legal fees or help them pay for court-imposed damages (see Chin, 2016; Lim, 2013). Social media have specifically been hailed as one of the catalysts for the birth and sustenance of many social movements around the world—whether against oppressive regimes, as with the so-called Arab Spring, or economic inequality with the global Occupy movement or the *Indignadas* in Spain (see Castells, 2015; Comninos, 2011; Gerbaudo, 2012; Meraz & Papacharissi, 2013). There has also been, it is argued, a direct impact on party politics, with the emergence of 'digital parties' such as the Pirate Parties and Italy's 5 Star Party (Gerbaudo, 2018). The internet has been said to provide the platform for 'networked resistance' through whistleblowing in the case of Wikileaks (Beckett, 2012; Cammaerts, 2013) or acts of hacktivism, as seen with groups like Anonymous (Coleman, 2015; Jordan & Taylor, 2004; Stoehrel & Lindgren, 2014).

While the scholars cited in the above examples have noted there is much to celebrate about the internet's impact on democracy and politics, the 'successes' in many of those cases were not achieved without significant obstacles. Some observers (see MacKinnon, 2012; Morozov, 2012) have cautioned against perpetuating a techno-deterministic narrative in viewing the internet, contributed in part by the

mainstreaming of social media in the earlier part of this decade. While hardly dystopian in their claims, both Mackinnon and Morozov note the difficulties faced by other publics attempting to replicate such successes within their own geographical context. Among the reasons for this, they argue, is the potential for governments and corporations to adopt these same 'liberating' technologies to erode citizen freedoms. Indeed, political leaders have been conscious about the potential emancipatory role of the internet, and have used the very same technologies to strengthen their control. MacKinnon (2012) argues that governments tend to replicate their problematic behaviours in the online space, adding that this habit is not exclusive to authoritarian regimes. Indeed, the revelations from whistle-blowers such as Edward Snowden highlight the ways in which even some of the most liberal of democracies such as the United States and Britain engage not just in surveillance but also hacking- and propaganda-like practices (Edgar, 2017; see also Greenwald & Fishman, 2015). The Cambridge Analytica scandal involving Facebook and its possible impact on the European Union referendum ('Brexit') in the United Kingdom, and subsequently the victory of Donald Trump in the presidential election in the United States of America—also exposed through whistleblowing—has brought to attention the ways in which social media can be "weaponized" (Berghel, 2018, p. 85).

These cases of whistleblowing have stimulated interest among academic researchers who focus on the illiberal ways institutions in democratic societies are using the internet to oppress citizens and impinge on their rights (Hardy, 2015; Petley, 2014). Previously, literature on these topics tended to focus on countries where mechanisms of control were employed to stifle the flow of information and disrupt communication among their citizens, dating back before the emergence of the internet, as the following examples illustrate. Russia's Soviet past is well-known for

its state-control of the media (Oates, 2007) while Singapore has been clamping down on dissent for decades using tools such as defamation laws, with officials as highly-ranked as the Prime Minister filing such lawsuits against dissenters (Chan, 2003). Thailand has silenced critics using the *Lese Majeste* law, which purports to protect the institution of the monarchy (Streckfuss, 1995), the same way opposition and civil society leaders, journalists and outspoken citizens have been arrested and charged in Malaysia using the Sedition Act and now-repealed Internal Security laws, which allowed for detention without trial (Wong, Chin, & Othman, 2010).

Considering this history, it is not surprising that as heavily-networked digital technologies become more pervasive, scholars have argued that these countries would also attempt to control them for the similar purpose of maintaining power and gaining political leverage over their opponents. As was the case pre-internet, the mechanisms used by governments and regimes are varied, often relying on multiple methods at once or at different times depending on necessity. In many cases, however, it has been argued the goal is to manage communication practices and the flow of information that benefits the status quo. Among the mechanisms identified by scholars is infrastructural control. For example, China's system for online censorship and surveillance, the Golden Shield (more popularly referred to as The Great Firewall of China), has been the subject of many studies over the years (Clayton, Murdoch, & Watson, 2006; Eko, Kumar, & Yao, 2011; Kim & Douai, 2012; Navarria, 2016; Tsui, 2007). The literature also discusses regimes where leaders such as Egypt's Hosni Mubarak and Iran's Mahmoud Ahmadinejab ruled with such a tight grip that they have previously turned off their citizen's access to social media as part of efforts to disrupt citizen protest plans (Howard, Agarwal, & Hussain, 2011).

In countries where governments rely on the veil of democracy as a form of legitimacy, rule of law—that is, through the use of legal intimidation and threats—has also been found to be invoked as a mechanism for control. This is evident in countries like Malaysia and Singapore where citizens are not only arrested, charged and sued by those in power for speaking out, but also tend to remain silent for fear of succumbing to the 'chilling effect' of state power over democratic dissent (Johns & Cheong, 2019; Kenyon, 2010; Liu, 2014; Rodan, 1998). Other countries like Russia are said to use economic means, where direct and indirect ownership of internet companies have been used for internet control (Vendil Pallin, 2017). In countries like Vietnam, efforts are not made to control users directly, but instead influence online behaviour—that is, internet use—through regulating the operations of internet cafés, a means of access for a large number of citizens (Surborg, 2008).

Then, there are the discussions about the more covert attempts by states at disrupting communication practices and information flow through manipulation of political information. Following the events surrounding the 'Brexit' referendum and US presidential elections in 2016, the practices related to the last form of control discussed above have been associated with the terms trolling, computational propaganda, and mis- and disinformation (Bennett & Livingston, 2018; Bradshaw & Howard, 2017; Jack, 2017; Roozenbeek & van der Linden, 2018). Scholars have previously discussed state-linked groups associated with these problematic practices targeted at domestic audiences, in countries such as China, Azerbaijan, Russia and Hungary (Calingaert, 2010; Gero & Kopper, 2013; Hung, 2010; Pearce, 2015), while the current discourse concerning Russian trolls in Europe and the United States

shows that manipulation of political information is now less easily confined within the borders of the nation state than it has ever been before[1].

2.1.2 *Describing online manipulation of political information*

This section will discuss three aspects of what existing literature tells us about online manipulation of political information. It will identify some of the groups of people who engage in this practice, the politicians and institutions mobilising them, and the sort of strategies and tactics they use. It also identifies the gaps in existing literature that motivated the study in this thesis.

In 2017, online manipulation of information on social media was the major trend reported by the US-based Freedom House[2] in its annual *Freedom of the Net* report (Kelly, Truong, Shahbaz, Earp, & White, 2017). The report found that elections in at least 17 countries were affected by state-led manipulation and disinformation strategies, contributing to the decline of internet freedom globally. Freedom House first identified the reliance of states on paid commentators in 2009, and reported that this practice reached a new high in 2017; 30 of 65 countries surveyed were said to have engaged paid pro-government commentators to "feign grassroots support" on the internet (Kelly et al., 2017, p. 7).

In the report, the authors note that evidence of the pro-government online commentators was collected through investigative reporting, leaked government

[1] The US Air Force has also been accused of engaging in these practices in other countries to entrap activists and for pro-invasion propaganda purposes by Anonymous hacktivists (Comninos, 2011) but debates surrounding the issue of manipulation of information beyond national borders only took off significantly post-2016.

[2] Freedom House is a watchdog organisation dedicated to reporting media freedom as a major indicator of states' commitment to human rights and democracy globally.

documents and academic research. Indeed, journalists and scholars have been monitoring this trend for over a decade, long before alleged attempts by Russian trolls to influence democratic practices in the United States and Europe became a mainstream topic. Early literature addressing such manipulation by state (or state-linked) actors focussed mainly on the practice used within domestic politics and within particular geographical contexts (Hopkins, 2014; Hung, 2010; Klotz, 2007). In spite of the extensive analysis offered in the Freedom House report, it is not often clear if such practices are orchestrated directly by governments and political parties or by other actors; often the existence of these actors is in itself inferred. Considering the covert nature of these practices, direct empirical evidence is hard to obtain. This lack of clarity impacts the ability of investigations, such as the one conducted by Freedom House, to generalise a seemingly transnational phenomenon. More empirically-based, context-specific studies are necessary for comparative studies like these to build on. Indeed, the exact nature of this covert practice needs further careful examination, not least because political leaders or institutions engaging in these sorts of manipulation benefit from the murky line between the two, allowing for plausible deniability.

Take for example China's 50 Cent Army, believed to have been established by the Chinese government's Ministry of Education to target college bulletin-board systems dating back to at least 2005, and is seen as part of the Communist Party's (CCP) propaganda apparatus (Hung, 2010). The Chinese government has not officially admitted to having formed the 'army', despite the publication of news reports in the tightly-controlled Chinese media—since removed—of government officers discussing plans to expand its army of 'internet commentators'. In other instances, this blurred line is used to dissociate from the deceptive elements of the practice.

This is the case in Malaysia where numerous media outlets have reported on the reliance of Barisan Nasional—the then-ruling coalition consisting of parties that own said outlets—on cybertroopers[3].

Former Prime Minister Najib Razak makes the distinction between types of cybertrooping. On the one hand, he wrote on his blog that "keyboard warriors, cyber troopers and even news portals have made the online world their 'playground', constructing their own version of 'reality' with click bait headlines that serve their own agendas. This is an unhealthy practice of journalism" (Razak, 2016, para. 3). On the other hand, Najib, as recently as 2017, was quoted to have actively called for their mobilisation: "Members must be ready to defend the party in the cyber and digital world as cyber troopers" (Zakaria, 2017, para. 9). Taken together, the two statements suggest that Najib was claiming that his cybertroopers do not engage in the illiberal activities he attributed to opponents in his blog. Without direct empirical evidence, it is difficult to test claims such as these, not just in Malaysia but in other geographical contexts as well.

Nonetheless, given the implications and ethical consideration of states engaging in such practices, the literature in this field of study continues to grow. To overcome the lack of direct empirical data, researchers have adopted different approaches to studying the practice, with some using computational methods (Ferrara, 2017; Ratkiewicz et al., 2011), and others relying on secondary data such as media interviews and news reports to make inference (Bradshaw & Howard, 2017; Hopkins, 2014; McCauley, 2015) or increasingly, both (Benkler et al., 2018; Saka, 2018; Woolley & Howard, 2017). There have been cases, however, where it has been

[3] I discuss these news reports in greater depth in Chapter 5.

possible to make a direct link between political actors and the practice of online manipulation by virtue of the evidence made available through legal proceedings or leaked documents. For example, the 'internet trolling' by the National Intelligence Agency to interfere with the 2012 Presidential Elections in South Korea was only able to be studied following data released from court proceedings (see Ho & Woo, 2016; Keller, Schoch, Stier, & Yang, 2017). In another instance, King, Pan, & Roberts (2017) were able to conduct a large-scale study on the 50 Cent Army in China following a massive leak of emails sent to, and originating from, the Internet Propaganda Office in one of the country's many districts, allowing the researchers to extrapolate the findings across the country.

The latter study is additionally significant because the data allowed the researchers to "offer the first systematic empirical evidence"—its findings challenging some previously made claims from investigations into China's notorious 50 Cent Army (p. 485). In particular, it was a long-held belief that the 50 Cent reference in the name comes from the amount of money paid to members of the army for posting pro-China and pro-CCP content. In 2012, Chinese dissident artist Ai Weiwei reinforced this belief as a result of an interview he conducted with a self-proclaimed member of the 50 Cent Army for an article in *New Statesman* (Ai, 2012) which has been referenced in scholarly research (Abbott, Macdonald, & Givens, 2013; Bradshaw & Howard, 2017; McCauley, 2015). However, this claim was debunked by the King et al. (2017) study which showed that agents were primarily civil service officers already under the employ of the government. That being said, despite coming to this conclusion, the authors note that "it is possible that other organizations may hypothetically follow different rules and practices […] determining whether it is must wait for new evidence to be unearthed." (p. 495)

The above shows that despite best efforts in research, more direct empirical evidence is necessary to better understand the ways in which these various political actors engage in the manipulation of online information. This sort of data is emerging, however, specifically through leaked documents such as those released in the Snowden whistleblowing reports showing that even the traditionally liberal countries like the United States and Britain engage in similar activities through their respective military units (Greenwald & Fishman, 2015; Petley, 2014). In the meantime, however, researchers are only able to rely on what existing literature suggests, and that is—as with the China example (King et al., 2017)—those who engage in online manipulation activities are made up of different groups of people (and in some cases, multiple groups), depending on their geographical origins. In the Russian context, for example, the common belief is that the 'trolls' are people who have been employed directly to work in a "troll factory" in St Petersburg set up for the dedicated purpose of online manipulation of information (Aro, 2016). The Syrian Electronic Army has been described as 'cyber warriors' linked to the government despite its claims of being independent (Al-Rawi, 2014). In Israel, university students are said to have been recruited in exchange for scholarships, some working at 'The Advocacy Room' on a university campus (Hall, 2014; McCauley, 2015), while in Turkey, the AKTrolls have been identified as social media representatives made up of young party members of the ruling Justice and Development Party, known as AKP (Albayrak & Parkinson, 2013; Saka, 2018).

Names like 50 Cent Army, AKTrolls and Syrian Electronic Army refer to particular groups in specific countries that engage in the manipulation of online information and disruption of communication among citizens, but existing literature suggests that they might not all engage in the same strategies and tactics although overlaps have

been noted. This is another reason why it is important that different contexts are studied, not just relating to geographical boundaries but also the types of governments and regimes. As mentioned, due to lack of empirical evidence, researchers sometimes rely on news reports for an understanding of these groups. However, many of the reports discussing these groups do not outline in detail the practices or tactics the groups may engage in, settling for more general descriptions such as the report of Britain's Conservative party paying an army of Twitterers to "take on" the supporters of opposition leader Jeremy Corbyn (Malnick, 2018, para. 1) or the early Malaysian report on the "cyber war against slander and lies posted on the Internet by the Opposition" ("Umno Youth goes on cyber-war footing," 2004, para. 1).

However, some investigative journalism pieces are more detailed: Adrian Chen's investigative piece in the *New York Times Magazine* on Russia's Internet Research Agency—arguably the most well-known troll factory—describes complex campaigns which spread propaganda and disinformation (Chen, 2015). A report on the practice in Saudi Arabia states that members of its social media army are sent list of people to "threaten, insult and intimidate" (Benner, Mazzetti, Hubbard, & Isaac, 2018, para. 14). Scholarly articles have also attempted to provide insights into these strategies and tactics where possible; the research on Turkey's AKTrolls identified activities including sending threats and insults (Saka, 2018), while the study on China found that 50 Cent Army members mainly engaged in cheerleading, that is, using "expressions of patriotism, encouragement and motivation, inspirational slogans or quotes, gratefulness, discussions of aspirational figures, cultural reference, or celebrations" as a form of distraction (King et al., 2017, p. 486).

Then there are the larger research projects which attempt to paint a transnational picture of online manipulation of information, and to generalise them beyond activities conducted just within geographical borders. The Oxford Internet Institute's (OII) Computational Propaganda Research Project, which has built an inventory of organised social media manipulation across 48 countries, found three ways in which discussions are shaped online:

> (1) Spreading pro-government or pro-party propaganda; (2) attacking the opposition or mounting smear campaigns; or (3) natural strategies that involved diverting conversations or criticism away from important issues, or fact-checking information. (Bradshaw & Howard, 2018, p. 11)

Freedom House also found "three principal aims" of such manipulation:

> (1) feigning grassroots support for the government (also known as "astroturfing");
>
> (2) smearing government opponents; and
>
> (3) moving online conversations away from controversial topics. (Kelly et al., 2017, p. 8)

The two reports discussed above show that both projects generally agree on their respective categories 2 and 3[4]. They also agree on the pro-government orientation in the first category, but the Freedom House version explicitly describes this as astroturfing. Astroturfing is manufacturing expression to "appeal as if it had arisen

[4] The Freedom House report shows that of the 65 countries it identified as having engaged in "disinformation tactics", 37 of them were found to have "paid pro-government commentators" and "political bots". Of these, 29 countries overlapped with the 48 countries in which the Computational Propaganda Research Project identified as engaging in "social media manipulation strategies". Based on these numbers, and descriptions in the documents, it can be argued both reports are referring to similar strategies and tactics but have opted to present them using different terms.

spontaneously from supporters" (Klotz, 2007, p. 3), and as described in the above context infers hidden hands by government-linked actors. Furthermore, while astroturfing does not primarily have to involve spreading propaganda, it could include such practices, as will be discussed in the next section of this chapter.

2.1.3 *Describing online manipulation*

In the discussion above, it has been noted that most of the investigations are country specific, and scholars have attempted to generalise the more common activities into categories. However, media practitioners and scholars alike have not settled on a common way to describe the practice and those engaging in it. Among other reasons, this is likely because the practice is a relatively new form of control that is usually covert, and as such, evidence is only slowly starting to emerge. This section discusses the different terminology associated with the practice of online manipulation of information within existing literature.

As researchers try to make sense of available data, it is not surprising to find them employing different terminology to describe their findings. However, there are three common terms associated with the manipulation of information on the internet: 'trolling' is arguably the most mainstream (see Aro, 2016; Saka, 2018; Zelenkauskaite & Niezgoda, 2017), particularly post-2016 when discussing Russian interference in the US and Europe, while 'astroturfing' has been used by scholars for a longer period (see Comninos, 2011; Hung, 2010; Klotz, 2007; Ratkiewicz et al., 2011). More recently, OII scholars added 'computational propaganda' to the existing lexicon (Woolley & Howard, 2017). Other terms have been used to describe comparable activities, such as George's (2016) 'hate spin'—similarly referring to organised efforts

to manipulate information online—although his study focusses on manufactured outrage in the context of hate speech. Arguably, hate spin is a form than can be found in any of the three mentioned above. 'Disinformation' is another term that has been used (see Aro, 2016; Ferrara, 2017; Pomerantsev, 2015). However, disinformation—referring to intentionally false or misleading information—does not fully capture the breadth of these online manipulation practices because the practice of online manipulation of information involves more than just the spreading of falsehoods (see Jack, 2017, for a thorough unpacking of the lexicon used in relation to problematic information).

It is likely that none of those terms have been whole-heartedly adopted because none accurately capture what researchers are trying to describe. This is especially so when it comes to dealing with particular geographical case studies, considering not all tactics are universally adopted by the various groups worldwide as previously discussed. Other reasons include the complexities in the derivation of these terms. 'Trolling', for instance, has been used with reference to troll farms such as the one identified in Russia. Where a definition has been offered, the understanding of trolling discussed in this chapter has been explicitly linked to political contexts. Zelenkauskaite and Niezgoda (2017, para. 6) describe it as "state-sponsored deviant behaviours online against political opposition in authoritarian regimes", while Saka (2018, p. 163) describes "political trolling" as "state-sponsored anonymous internet political commentators […]".

That these authors make a point to single out this sort of trolling as 'political' is telling; "trolling" as a concept has an extensive, and varied, history in internet cultures, buoyed by anonymity allowing online users to get away with leaving

"deliberately cruel and callous comments that served no purpose other than to hurt, shock, offend and sow discord" (Hannan, 2018, p. 220). In fact, trolling as an online behaviour is still being debated by scholars, and what the term encompasses has developed gradually over time (see Sanfilippo, Fichman, & Yang, 2018). It does not specifically refer to state-sponsored or political trolls, although some of the activities they engage in can be defined as such. Other activities like cheerleading posts in China or dissemination of disinformation and hoaxes like in Russia do not fit well within the earlier understandings of trolling.

The use of the term 'astroturf' also has a similarly complex history, not just in terms of its evolving definition but also in the context in which it is used. Cho, Martens, Kim, and Rodrigue (2011, p. 571), for example, describe astroturf organisations as "corporate version of grassroots social movements". This description can be understood in two ways: first, largely associated with marketing—Gallagher (2014) refers to the practice as false advertising in the 21st century—and secondly, within politics—Lee (2010, p. 73) refers to this as "political action masquerad(ing) as grassroots efforts". However, the understandings above refer to attempts by corporations to misrepresent public opinion in the process of lobbying, in contrast with how astroturfing can be aimed at publics themselves to give a false impression by feigning popularity. Indeed, the use of astroturfing in politics was first noted by United States Senator Lloyd Bentsen in 1985 when he referred to a flood of letters—or what he called "generated mail" (Gallagher, 2014, p. 1)—his office received in favour of the insurance industry's interests, which was written as part of an organised movement by a front group (Klotz, 2007; Lyon & Maxwell, 2004; Zhang & Carpenter, 2013).

As astroturfing became increasingly used on the internet in recent years, scholars attempted to develop definitions specifically to address the practice in its online form. Kovic, Rauchfleisch, Sele, and Caspar (2018, p. 71) offer the term 'digital astroturfing', and define it as "a form of manufactured, deceptive and strategic top-down activity on the Internet initiated by political actors that mimics bottom-up activity by autonomous individuals. Zhang and Carpenter (2013, p. 3) on the other hand offer 'online astroturfing', which they define as "the dissemination of deceptive opinions by imposters posing as autonomous individuals on the Internet with the intention of promoting a specific agenda". Even within their contributions, both papers make distinct points regarding their definition—the latter notes that the motivations for online astroturfing to be more general—"political, commercial or military" (p.3), while the former's definition explicitly refers to political actors. While the typology of Kovic et al. (2018) has developed is well thought out, the authors' choice of the term 'digital astroturfing' as opposed to 'digital political astroturfing', for instance, means that it may be difficult—on the surface at least—to clearly distinguish its political distinction from the more general terms 'astroturfing' or 'online astroturfing'. In fact, the authors note that discourse surrounding this practice has conflated digital astroturfing with trolling, which they warn against because the latter "is not initiated on behalf of political actors" (p. 74). However, this indicates that the aforementioned terms remain ambiguous, and could be confusing for media practitioners and the general public who may not use the terms with the same nuance as scholars.

In recent years, the manipulation of information on social media has also been described as 'computational propaganda', following the release of reports from a large-scale project at the OII. In 2017, the team of researchers released the reports

which included nine in-depth case studies of the "use of social media for public opinion manipulation" (Woolley & Howard, 2017, p. 3). The executive summary for the reports defines computational propaganda as "the use of algorithms, automation, and human curation to purposefully distribute misleading information over social media networks" (p. 6). One year prior, the same authors defined it as "the assemblage of social media platforms, autonomous agents, and big data tasked with the manipulation of public opinion" (Woolley & Howard, 2016, p. 4886). Unlike trolling and astroturfing, computational propaganda is not affected by historical use of the term; it is one that was created in current times to address a current phenomenon.

However, computational propaganda's focus on "autonomous scripts and algorithms" (Neudert, 2017, p. 4) centres the term on the reliance of bots—that is, "computer programs or algorithms controlling accounts on social media" (Murthy et al., 2016, p. 4955). The examples previously discussed of civil service employees in China, troll farms in Russia, and students in Turkey and Israel show that not all known forms of organised manipulation of online information are necessarily automated. In any case, what constitutes a social media bot in itself is ambiguous, particularly when it comes to political bots, no less because of the complexities of distinguishing social bots from cyborg accounts, which are only partially automated (see Gorwa & Guilbeault, 2018, for a comprehensive typology of the social media bot). While it is undoubtedly important to study the increasing disruptions that bots cause, organised campaigns by states into online manipulation may take a hybrid approach to online manipulation, not relying on bots alone. In asking whether or not identifying such bots is sufficient in current research, Grimme, Assenmacher, and Adam (2018, p. 2) propose "identifying coordinated strategies, i.e. orchestrated

activities of multiple (automated, semi-automated or human-steered) accounts". However, putting to one side the question of who the agents are—humans or bots—it is arguable that the term computational propaganda in this context does not sufficiently capture all activities that agents of online manipulation engage in.

2.1.4 *Cyber troops, cybertroopers and cybertrooping*

The Computational Propaganda Research Project had also, in one of its reports, introduced another term in the context of online manipulation of information: 'cyber troops', which is defined as "government, military or political party teams committed to manipulating public opinion over social media" (Bradshaw & Howard, 2017, p. 3). The report found such groups in 28 countries based on news articles—which were subsequently verified by country experts—the earliest from 2010. An updated report in 2018 found such groups in 48 countries (Bradshaw & Howard, 2018). Despite the fact that news organisations had been reporting on Malaysian cybertroopers since 2004 (over 400 such articles are analysed as part of this thesis in Chapter 5), only the 2018 report included Malaysia. The term 'cyber troops' is of particular importance to this study and will be further developed in this thesis—through two other permutations of the term, that is, 'cybertrooping' and 'cybertroopers'—as part of my aim to offer a more comprehensive definition for the activities that are currently gathered under the various terminologies this chapter discusses.

This term is not original to myself or the OII scholars: it has been used in Malaysia as far back as 15 years ago in a news report to refer to pro-Barisan Nasional "cyber activists" taking on the Opposition ("Umno Youth goes on cyber-war footing," 2004, para. 2). It is unique in the sense that the term was crafted for the sole purpose

of referring to centrally-mobilised agents working for a political party in power engaging in cyber warfare. While the news report states that the purpose of the cybertroopers is to correct "lies and 'deluded information"' by the opposition, scholars have long claimed that they deal with manipulated content (Tapsell, 2013a) and virtual harassment (Mohamed et al., 2011), among other tasks. This thesis will explore existing literature on cybertrooping further in Chapter 4 (within the context of other forms of internet control mechanisms adopted by the previous Malaysian government), but what is clear is that lack of more detailed empirical evidence means that existing scholarly work about Malaysian cybertroopers is as limited as studies from different countries discussed in the previous section. This thesis will be the first research into Malaysian cybertroopers to include direct empirical evidence of this scale.

2.2 Framework and tools for analysis

This section discusses strategies, techniques and activities engaged by cybertroopers[5] in more depth to serve two purposes: first, it will further situate this thesis within the field of research that explores information manipulation beyond just digital spaces, and second, develop a more detailed characterisation of existing mechanisms for information manipulation which pre-date the internet to serve as a framework and as tools for the analysis of data in the forthcoming chapters. This discussion warrants deeper consideration to avoid being blinded by the 'digital dazzle', adapting the term coined by ethnographer Robin Fox who cautioned researchers about the

[5] I use the term 'cybertroopers' here to refer to all groups discussed in existing literature engaging in practices of information manipulation (herein referred to as 'cybertrooping') for brevity, pending more detailed characterisation in this thesis's concluding chapter.

'ethnographic dazzle', that is, the preoccupation with superficial differences between groups and cultures (Fox, 2014). After all, the use of technocentric terms like cybertrooping, trolling and computational propaganda gives the impression that the instances of information manipulation discussed earlier in this chapter are unique to contemporary times, seeing as they are mediated on the internet. However, as will be discussed, it is possible that we refer to them now differently solely because they look different when mediated electronically, when they actually share similar characteristics. At the very least, this will be worth discussing because existing literature on cybertrooping from various geographical contexts and periods has included terminology associated with political communication practices which were used by state and political actors for decades before the introduction and popularisation of the internet, such as propaganda, public relations, psychological operations and more.

The following discussion considers the key objectives of cybertroopers, as outlined in the literature, which I categorise as dissemination, defence, demonisation, disruption and distraction. This categorisation builds on the three ways in which discussions are shaped online that the Computational Propaganda Project and the Freedom House respectively highlighted in their reports (Bradshaw & Howard, 2017; Kelly et al., 2017). Based on those reports, *dissemination* and *defence*, for example, would include both the spreading of propaganda and astroturf support for governments, while *demonisation* and *disruption* covers attacks and smear campaigns against the opposition and opponents. Finally, *distraction* includes diverting conversations away from criticism or controversial topics.

2.2.1 *Dissemination and Defence*

The dissemination of information, as a form of online manipulation, has been described by existing literature in different ways. The Computational Propaganda Project's inventory of "organized social media manipulation" described this form of messaging as "spreading pro-government or pro-party propaganda" (Bradshaw & Howard, 2018, pp. 3, 11). This report expanded on a previous one from a year before, which was much more detailed in its description of the practice. In the older report, Bradshaw and Howard (2017, p. 12) identified "content creation" as one approach, noting that "cyber troop teams create substantive content to spread political messages". This content, it said, is distinct from other seemingly similar activities such as leaving comments on social media; it refers to the generation of blog posts, videos and pictures among others to push a particular political message, citing examples from countries such as the United Kingdom and Russia.

Similarly, studies of countries like China, for example, have found that social media posts sent out by members of the country's 50 Cent Army include those categorised as "non-argumentative praise and suggestions" and "factual reporting" (King et al., 2017, p. 498). The former is said to involve "non-controversial valence issues which are hard to argue against, such as improving housing and public welfare; praise of current government officials, programs, or policies", while the latter include "descriptions of current government programs, projects, events, or initiatives, or planned or in progress initiatives" (p. 498). Cybertroopers in Malaysia are also said to engage in similar activities such as dissemination of pro-government information and propagation of particular agendas (Hah, 2016; Liu, 2014).

While terms like content creation, factual reporting, praise and suggestions may come across as relatively innocuous, the examples listed above are presented by scholars within the context of information manipulation and problematic persuasion practices. Indeed, they cannot be studied in isolation from other activities cybertroopers around the world engage in, and from the larger objective of information manipulation. However, even separated from the other activities, there is more to these seemingly harmless activities than meets the eye. Already, Bradshaw and Howard (2018) describe the kind of content created by 'cyber troops' as propaganda, while Kelly et al. (2017) connect the practice with astroturfing, a term associated with deceit. While propaganda did not always have a negative connotation[6], Qualter (1962, p. 6) reflects on the way it was used during World War I as "the first systematic attempt to control public opinion […]". Miller's (2004) book on propaganda and media distortion is tellingly titled *Tell Me Lies*. Jowett and O'Donnell (2012, p. 7) are also clear in their definition: "Propaganda is the deliberate, systematic attempt to shape perceptions, manipulate cognitions, and direct behaviour to achieve a response that furthers the desired intent of the propagandist".

The nature of propaganda remains debated, no less due to what Thomson (1999, p. 2) calls "confusions" as to whether it needs to be deliberately planned or whether persuasion is only propaganda when there is "mistruth and deception or emotional manipulation". After all, not all propaganda is untrue, as scholars have argued. Where convenient, propagandists tend to inject the truth because it is more believable, and thus, more effective in manipulating its audience (Qualter, 1962). Scholars have

[6] The term propaganda dates back to 1622 with the formation of The Office for the Propagation of the Faith (*Congregation de propaganda fide*) by Pope Gregory XV in response to the spread of Protestantism (Jowett & O'Donnell, 2012). Lasswell (1995, p. 13) noted that the term "propaganda" was "given currency" by the church "to refer to the dissemination of its doctrine".

attempted to manage this ambiguity by making the distinction between *white propaganda*—that is, generally truthful but selective and persuasive public communication—and *black propaganda*—which involved lies and deception—although Hiebert (2003, p. 244) notes that "most propaganda is probably partly true and falls into a gray area". Jowett and O'Donnell (2012, p. 20) similarly situate *grey propaganda* in the spectrum between white and black propaganda, describing instances where "the source may or may not be correctly identified, and the accuracy of the information is uncertain." They also further emphasise that while white propaganda is "reasonably close to the truth", it is problematic in the sense that it convinces the public that the propagandist "is the 'good guy' with the best ideas and political ideology", although the intention is often to "build credibility with the audience, for this could have usefulness at some point in the future" (p. 17).

What the above illustrates is that the dissemination of information is hardly a benign act. Consider the links scholars have made between propaganda and military psychological operations (Hiebert, 2003). Psyops, as it is more commonly referred to, is considered part of 'offensive information operations' and can be defined as "operations planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning and ultimately the behaviour of foreign governments, organisations, groups, and individuals" (Whitley, 2000, p. 3). While there is little doubt that psyops can be extremely complex, as will be discussed later in this chapter, one of the ways in which it operates is as simple as the mass distribution of propaganda materials. Miller (2004) found that at the US psyops headquarters at military base Fort Bragg, facilities exist that can produce up to 1 million leaflets in an hour and that since September 2001, over 150 million leaflets produced there have been distributed in both Afghanistan

and Iraq. That information operations generally involves military strategies to weaken an opponent's information system is further indication of how there is more to a simple act of dissemination of information—propaganda—than meets the eye.

It comes as no surprise then that the term propaganda has been adopted to expand on the existing lexicon referring to practices of information manipulation online, such as in the case of computational propaganda (DiResta, 2018; Woolley & Howard, 2016) and networked propaganda (Benkler et al., 2018). Earlier literature in this field also mentions propaganda in describing the objectives of groups identified as engaging in this practice across various geographical contexts. In China, Hung (2010, p. 157), describes one of the aims of China's "Internet administration" as efforts "to systematically develop propaganda on the Internet", while the Syrian Electronic Army has been described as one of President Bashar al-Assad's "propaganda tools" (Al-Rawi, 2014, p. 423). Russian trolls are also argued to be "part of the Kremlin's propaganda system" (Aro, 2016, p. 122).

Existing literature that discusses such manipulation of information online does not only associate the practice with propaganda. Public relations, it has been argued, is a professionalised version of propaganda commonly used in politics (McNair, 2004). As such, it comes as no surprised that scholars have associated it with online astroturfing practices (Sisson, 2017). For example, Al-Rawi (2014, p. 423) argues that the Syrian Electronic Army—a cybertrooper group—"is an organization that clearly exhibits public relations features". The connection between public relations and propaganda goes back to the early days of the former being established. The father of Public Relations, Edward Bernays, conflated the two when he said in an interview that "propaganda got to be a bad word because of the Germans […] using it [in

1914-18]. So what I did was try to find some other words. So we found the words Counsel of Public Relations" (Miller & Dinan, 2008, p. 5). Nonetheless, scholarship surrounding public relations has been mixed when it comes to associating the practice with the pejorative nature of propaganda.

Some scholars who specialise in public relations argue that PR practices are generally non-manipulative (see Bakir, Herring, Miller, & Robinson, 2018, for an extended discussion on PR scholarship), and often focus on the profession and "apolitical technicalities" of the practice (Miller & Dinan, 2008, p. 2). Critics of public relations describe the activities it involves as problematic in different ways. Stauber and Rampton (2004, p. 14) argue that the PR industry functions stealthily, that its "invisibility is part of a deliberate strategy for manipulating public opinion and government policy". Grimshaw (2007, p. 33) similarly notes that the PR industry gains power from the covert way in which it operates, arguing that "without knowing who is spinning *what* messages *where* and *how*, the public is denied a full understanding of how modern political economy functions […]" (emphasis in original). These criticisms could easily be said about cybertroopers, if they are to be considered as groups outsourced by governments or political parties to spread messages on their behalf as part of online manipulation strategies. As Carl Byior, another pioneer of the PR industry, once said: "It is not what a client says about himself that scores, but what another person says about him that carries weight." (Dinan & Miller, 2007, p. 12)

Aside from the lack of transparency, public relations is also considered problematic in scholarly debates because of how its messages are crafted. This harks back to earlier descriptions of cybertrooper groups in China creating pro-government or

party content such as praise and positive suggestions, and even disseminating factual content (King et al., 2017). This sort of content is similar to the white propaganda content Jowett and O'Donnell (2012) argued was problematic, as mentioned above. Among the reasons for this is that information, no matter how mundane, factual or positive, could be the product of 'spin'. Historically[7], spin referred to "the interpretation or slant placed on events" (Esser, 2013, p. 1) or putting a favourable bias or angle on a story (Andrews, 2006; Sumpter & Tankard, 1994). Spin doctors do this by arguing that "truth is relative", which justifies them taking on unpopular clients on the grounds that there are two sides to every issue (Sumpter & Tankard, 1994, p. 22). Miller and Dinan (2008, p. 2) directly link PR tactics to spin, which is "generally thought of as manipulative or deceptive communications". Others, like McNair (2004), consider spinning as a product of political PR. Similarly, Gaber (2000, p. 508) argues that spin includes both the "overt initiatives"—which are more associated to traditional public relations such as speeches, and official announcements and reactions—and the more "covert", mostly associated with spin doctors, which is "as much about strategy and tactics as about the imparting of information".

Indeed, it has been argued that in the same way that propaganda, psyops, public relations and spin can be presented to look neutral to the layperson (although at varying degrees of success), they are also used to respond to criticism from

[7] Andrews (2006) breaks down four ways the term 'spin' has been used: the massaging of how news events are interpreted by the media; a blanket term for anything related to the "black arts" of campaigning; the media operations of political entities; the broadening of the term to include commercial PR (see Esser, 2013, p. 2–3, for a summary of each of these). The first way speaks to the historical technical definition of spin. The second is from the conflation of approaches associated with manipulative and deceptive practices related to political information. Miller and Dinan (2008, p. 2), for example, note that the term "has become the ubiquitous term for public relations tactics" while Andrews (2006, p. 36) argues that spin has "moved from electoral tactic to become synonymous with propaganda".

opponents. Mary Matalin, a political consultant for President George H.W. Bush during his 1992 Presidential re-election campaign against Bill Clinton, described how spinners like herself would be given sheets of paper with talking points following a public political debate before storming into a press room: "our job was to put a positive spin on our guy's performance, and to denigrate the opposition" (Matalin, Carville, & Knobler, 1994, p. 394).

Cybertrooping has also been said to be a defence mechanism in scholarly literature and news reports. This is especially true in situations where the state or political party admits to mobilising cybertroopers, and justifies their cybertrooping as defending themselves on social media. For example, in Israel, student volunteers were allegedly recruited to "counter what is perceived as a false representation of Israel in international and social media through Facebook, Twitter and YouTube" (Hall, 2014). In Malaysia, early literature indicates that the ruling party's cybertroopers existed to counter pro-opposition messages on the internet. For example, Hopkins (2014, p. 12) cites a political leader discussing the defensive role of the ruling coalition's cybertroopers "to counter false allegations, slanders and lies by the opposition". These claims of defence by a politician in themselves can be seen as spinning in action; after all, other scholars have pointed out that Malaysian cybertroopers engage in efforts to "discredit and derail" their opponents (Leong, 2015, p. 60), which is not quite the defence role they claim to take. Even if the claims of taking a defensive role are accepted at face value, scholars such as Gaber (2000) have argued that those efforts can also be considered spin, offering the example of Labour Party's Rapid Rebuttal Unit set up to respond instantly against their opponent's new policy announcements or attacks during the 1997 United Kingdom general election.

In what can also be considered part of a defence strategy, Malaysian cybertroopers are also said to have been set up to manage the image of the United Malay National Organisation (UMNO, the largest component party in Barisan Nasional) on the internet (Ding, Koh, & Surin, 2013), while Liu (2014) argues that one of their roles were to counterbalance opposition forces. Badrul Azmier, Mohammad Agus, and Zaliha (2014, p. 110) also note the role of cybertroopers is to balance "the temperature which has been favourable to the opposition"[8]. This image-building role is a tactic commonly associated by scholars with public relations professions and spin doctors, who sometimes "orchestrate 'structured leaks' of some good news" in advance of major events (Sumpter & Tankard, 1994, p. 22), the same way film companies release trailers and teasers. In the case of US President George Bush's 1992 State of the Union Address, congressional leaders were mobilised in advance "to comment favourably" following the speech (p. 22).

The discussion above regarding the dissemination of information, covering propaganda, psyops, public relations and spin, shows that content can, and has been, created as part of deceptive strategies by state or political actors. It also described how praise, positive suggestions and factual information distributed could be problematic. The content created could have been subjected to spin even while being presented in a neutral or positive way. At the very least, it can give the impression that this content is part of genuine discourse (i.e. astroturfing). What's more, such content is produced as part of a larger information manipulation strategy that includes attacks and diversion, which will be discussed in the next section.

[8] As will be further discussed in Chapter 4, the then-opposition parties were said to have been more dominant on the internet compared to Barisan Nasional, having taken advantage of the 'freedoms' afforded by the internet in a climate where the former-ruling party had controlled of mainstream media.

2.2.2 *Demonisation and Disruption*

Online manipulation activities associated with demonisation and disruption are generally linked to attacks and smearing of others (Bradshaw & Howard, 2018; Kelly et al., 2017). Demonisation can take many forms and target individuals or institutions, be they opposition politicians, supporters of opposition parties or members of the public deemed to be anti-government. As examples, there is literature regarding "state-sponsored harassment" on social media in Azerbaijan (Pearce, 2015, p. 1158), or threats and insults in Saudi Arabia and Turkey (Benner et al., 2018; Saka, 2018). Trolls linked to supporters of the far-right Alternative for Germany (AfD) party have been found to stage an attack on German chancellor Angela Merkel on Twitter during a TV debate (Grimme et al., 2018).

Aro (2016, p. 122) too has noted the "systematic attacks" she encountered by "pro-Kremlin propagandists" in Finland, following her journalistic investigations into Russian troll factories. She claimed that they spread "their own falsified narrative of me and my article", including "lies on fake news sites about me 'persecuting Russians living in Finland and putting together an illegal database of Putin's supporters'" (p. 123). Such description harks back to efforts known as *dezinformatsiya* (which inspired the term disinformation) used by Russian intelligence as part of "coordinated state efforts to disseminate false or misleading information to the media […]" (Jack, 2017, p. 9). However, it is also similar to tactics discussed by Massoumi, Mills, and Miller (2019) implicating the Joint Threat Research Intelligence Group, which is part of Britain's Government Communications Headquarters (GCHQ). The documents noted that the agency's psychological operations involve the spreading of misinformation and use of techniques to discredit opponents on social media

platforms such as YouTube, Facebook, Twitter and blogs (see also Greenwald & Fishman, 2015). While not always the case, demonisation by cybertroopers was traditionally seen in the domestic setting, attacking direct opponents of the state or ruling party, as many of the examples earlier discussed in this chapter illustrate.

That said, there is increasing discussion surrounding a more transnational effort in cybertrooping, particularly with regards to claims of Russian interference in the US and Europe. Following the 2016 US Presidential Elections, the National Intelligence Council mentions the Internet Research Agency—the much-discussed troll factory in St Petersburg—in its report on Russian interference during the elections (Kovic et al., 2018). Woolley and Howard (2017) found in their research on computational propaganda that bots were used in shaping Twitter conversations during the EU referendum in the UK. While the authors did not attribute the campaign to a source, Russian interference in the referendum is currently being investigated by the British House of Commons Culture, Media and Sport Select Committee, as its interim report notes (*Disinformation and 'fake news': Interim Report*, 2018). In these instances, the manipulation activities are seen as an attack on a nation's sovereignty through the disruption of democratic processes.

Ahead of the US midterm elections in November 2018, Vice-President Mike Pence accused China's "covert actors, front groups and propaganda outlets" of interference in media reports, which the country denies ("China denounces 'ridiculous' US claims of election meddling," 2018, para. 13). A few days later, news reports of Taiwan accusing China of the same, linking the misinformation campaign to the 50 Cent Army (Reinl, 2018). While China has denied these accusations, the King et al. (2017, p. 498) study found that even ideology could be attacked, describing a category of

content found in their study as the taunting of foreign countries for being "pro-democracy, pro-West, pro-individual liberties, or pro-capitalist".

Cybertrooper groups are convenient third-party proxies to engage in the aforementioned demonisation activities because those who recruit or hire them are able to disassociate themselves from the attacks or spreading of controversial messages that are being fed to the public, allowing for an element of plausible deniability[9]. According to Maurer (2015, p. 79), the use of "cyber proxy actors" in Ukraine includes the "political incentive to be able to claim plausible deniability[10] as well as incentives for the state to augment their own capabilities by adding those provided by non-state actors". In this context, their activities are reminiscent of another public relations tactic, that is the use of front-groups, mobilised to look like genuine citizen movements to advance the interest of their particular clients (Stauber & Rampton, 2004). Fitzpatrick and Palenchar (2006, p. 203) describe the use of front-groups as:

> Controversial public relations techniques used by organizations to influence public opinion and public policy on behalf of undisclosed special interests. The groups are created to pursue public policy objectives for organizations that disguise their connection (e.g., financial support) with the effort while attempting to appear independent.

[9] Spin doctors too have been known to partake in such attacks; consider the earlier mentioned description by President Bush's political consultant who noted that their job was to "denigrate the opposition" (Matalin et al., 1994, p. 394). In the UK, Prime Minister Gordon Brown's special adviser Damian McBride was dismissed in 2009 after being caught out for proposing a plan to publish personal smears in a blog about some of their opponents (Kenny, 2009).

[10] Cormac and Aldrich (2018) argue that the world currently exists in an era of 'implausible' deniability, partially contributed by the advancement of media and technology. They may not be wrong, but the public do not always have the necessary understanding, skills and ability to discern the nuances of covert activities in general.

Front-groups have also been associated with astroturfing (Cho et al., 2011; Lyon & Maxwell, 2004), in the same way that the manipulation of online information has also been, as illustrated in the earlier discussion on digital astroturfing and online astroturfing (Kovic et al., 2018; Zhang & Carpenter, 2013).

While not always the case, scholars have associated astroturfing on social media with sockpuppetry, that is accounts using false identities. It can be argued that cybertroopers who engage in sockpuppetry are cyber proxy groups, the contemporary siblings of the traditional front groups. Solorio, Hasan, and Mizan (2013, p. 1) describe sockpuppets as "a secondary account created by a user for malicious purposes". To understand them, it is worth emphasising the descriptor "malicious" because the creation of alternative, or 'alt', accounts on social media is very much part of current internet culture (van der Nagel, 2018). It has also long been linked in existing literature to online manipulation of information. Comninos (2011, p. 14), describes sockpuppetry as "armies of fake people" and, in discussing user-generated-content related to the Arab Spring, refers to astroturfing as "sockpuppetry on a larger and more organized scale". Gorwa and Guilbeault (2018, p. 9) further link sockpuppetry to terminology associated with online manipulation of information, noting that "politically motivated sockpuppets" are referred to often as "trolls". Indeed, the leaked documents from the Snowden files, for example, implicated the National Security Agency (or NSA, part of the United States Department of Defense) and the Government Communication Headquarters (or GCHQ, linked to the British Military Intelligence 5) in these activities as well (Massoumi et al., 2019). One of the methods listed referred to a news report that specifically describes "sending spoof emails and text messages from a fake person or mimicking a real person (to discredit, promote distrust, dissuade, deceive, deter, delay

or disrupt)" (Greenwald & Fishman, 2015). Jack (2017, p. 9) too has linked such groups to *dezinformatsiya* strategies, describing the establishment of "'front' organisations or financing opposition political movements" as subversive action.

2.2.3 *Distraction*

Methods and techniques adopted by cybertroopers associated with distraction are generally described in two ways in the existing literature. The first way involves the diversion from a particular topic, which in the context of this discussion, is likely controversial and critical of the government or ruling party. Tucker, Theocharis, Roberts, and Barberá (2017, p. 54) note that one quality of "online trolls" is that they are not usually "interested in argument-based conversation" and as such often "create distractions that refocus online users on another issue or message." It is in this way that distraction differs from defence; as described earlier, the latter addresses the topic or issue head on. Distraction is a "neutral" strategy, which involves diverting or moving conversations or criticisms online away from important or controversial topics (Bradshaw & Howard, 2018, p. 11; Kelly et al., 2017).

Scholars have noted the different ways in which distraction has been used as a strategy online. King et al.'s (2017, p. 499) study on the Chinese 50 Cent Army, for example, shows a high use of what they term as "cheerleading" which involves the voluminous flooding of timelines with positive messages—"encouragement and motivation", "inspirational quotes", "gratefulness"—as a means of distraction. Another way in which the Chinese cybertroopers have been associated with distraction is by intentionally going off topic. The interview conducted by Chinese dissident Ai WeiWei discussed earlier in this chapter quoted the unnamed self-

confessed member of the 50 Cent Army as saying: "When transferring the attention of netizens and blurring the public focus, going off the topic is very effective" (Ai, 2012, para. 27). These two examples indicate a seemingly placid means for distraction. However, not all techniques operate this way. Cybertroopers have also been known to use provocation, detraction and swear words for this purpose (Sanfilippo et al., 2018). This approach is not dissimilar to one used by spin doctors in politics, occasionally referred to as the 'dead cat strategy'. Often attributed to political strategist Lynton Crosby (Delaney, 2016), the approach which involves using a different issue of high news value as diversion, was once described by current British Prime Minister Boris Johnson (2013, para. 2):

> The key point […] is that everyone will shout 'Jeez, mate, there's a dead cat on the table!'; in other words they will be talking about the dead cat, the thing you want them to talk about, and they will not be talking about the issue that has been causing you so much grief.

Other scholars such as Gaber (2000, para. 512) refer to that spin technique as 'firebreaking', which can be defined as "a deliberate constructed diversion to take journalists off the scent of an embarrassing story […]".

The 50 Cent Army member interviewed by Ai WeiWei refers to a similar strategy, citing his job at managing public opinion regarding the oil price increase as an example. He describes his response to public condemnation of the authorities once a news story breaks:

> At this point, I register an ID and post a comment: Rise, rise however you want, I don't care. Best if it rises to 50 yuan per litre: it serves you right if

> you're too poor to drive. Only those with money should be allowed to drive on the roads […] This sounds like I'm inviting attacks but the aim is to anger netizens and divert the anger and attention on oil prices to me […] Slowly, the content of the whole page has also changed from oil price to what I've said. It is very effective. (Ai, 2012)

In this instance, the cybertrooper becomes the story. To some degree, this isn't different from how spin doctors too have often become the story—to the point of becoming "a cultural icon" (Street, 2001, in Andrews, 2006, p. 39)—eventually encountering problems by becoming targeted by the media (McNair, 2004). In this sense, the difference between the cybertrooper above and the spin doctors is that the former operates covertly, and thus, are often not publicly known[11].

The second way in which distraction is used is by taking advantage of the difficult navigation of vast amounts of information on the internet. In discussing information politics, Jordan (2015, p. 50) states that "a founding condition of information life is then the threat of information overload, the fear of being drowned in data". The spreading of disinformation and distribution of junk news—that is, "various forms of propaganda and ideologically extreme, hyperpartisan or conspiratorial political news and information" (Neudert, 2017, p. 16)—can serve as a form of distraction by sowing confusion from too much information. In her report *Lexicon of Lies*, Jack (2017) illustrates how 'problematic information' can sow confusion and lead to distraction. Among other related terms, she describes gaslighting ("used to describe situations in which a person orchestrates and inaccurately narrates events to the

[11] The latter may not want to be noticed but due to the nature of the job, and the profile of the politicians they work for, mean that they are often not able to conceal their identities the way cybertroopers are generally able to.

extent that their victims stop trusting their own judgments and perceptions"), *dezinformatsiya* and the Chinese term *xuanchuan*, that is to "flood conversational spaces with positive messages or attempts to change the subject" (p. 9–10).

While the positive messages Jack mentions likely refer to the content earlier identified as cheerleading, *xuanchuan* describes a specific strategy of spamming in order to flood communication platforms. The term spamming has been used to describe efforts to drown out authentic voices; Verkamp and Gupta (2013, p. 1) argue that spamming on Twitter has been used as a technique to limit political speech by drowning out "voices of protests". Political bots, some of which are knowingly called spambots, are usually attributed to this task and have been found to be used in countries like Russia, Germany and Syria, among others (Neudert, 2017). Not all spamming comes from bots, however, although automation does make the process easier.

Spam has also been viewed in a different way, and attributed to political and military strategies. Jenkins (2009) describes a 2008 *New York Times* article which discusses a media campaign orchestrated by the George W. Bush administration in response to the war against Iraq using former generals as 'message force multipliers' to reinforce government messaging on broadcast news media (see also Barstow, 2008). The campaign, the article claimed, was part of psychological operations through the 'hidden hands' of the Pentagon, which planted a "military analyst […] who could be counted on to deliver administration 'themes and messages' to millions of Americans 'in the form of their own opinions'" (Barstow, 2008, para. 23). Dean (2010, p. 25), in discussing the same article, describes this strategy as "spam for television", and likens these message force multipliers to the role of army troops being deployed into

conflict zones: "it implies adding lots of forces, putting more people on the ground or in the air, just as one would send more troops into a situation". She suggests two ways that message force multipliers are accented: "the force multiplication of messages or the multiplication of message forces" (p. 25).

While this form of distraction can be seen as an attempt at censorship, it can also be seen as an effort to disrupt and divert democratic practices. Johns and Cheong (2019) argue that the use of such multipliers has had an affective impact on a legitimate social movements such as Bersih in Malaysia, dampening the movement's aim at achieving hope and replacing it with helplessness.

2.2.4 *The final 'D'*

Across the five objectives identified and discussed, one additional 'D' persists, and that is *deception*. As this chapter has indicated, some of the activities associated with achieving the aforementioned five objectives could come across as harmless when observed in isolation. However, when considered in the context of information manipulation, deception often runs through them all, even where white propaganda is concerned, as Jowett and O'Donnell (2012) have argued. In addition, there is evidence that the manipulation of information generally involves invisible hands. In one example, court documents showed that the South Korean national intelligence agency had run a covert operation to help the incumbent president and ruling party retain power in the 2012 elections (Ho & Woo, 2016). Add to this the fact that the NSA and GCHQ's strategies would not have come to light if not for whistleblowing, suggests that these operations are run stealthily for a reason: deception. Indeed, in the *New York Times* article cited by scholars (Dean, 2010; Jenkins, 2009), the

Pentagon strategy in addressing the Iraq War was described as orchestrated by 'hidden hands' (Barstow, 2008).

Scholars have noted that these forms of deception benefit those behind these operations in two ways. First, as the public are generally able to recognise blatant propaganda, advertising as a form of political communication is often not seen to be effective. Such communication is often recognised to be biased, no matter if the receiver agrees with the message or not (McNair, 2012). Secondly, unless exposed, political actors behind these operations are able to avoid being linked directly to such problematic practices through plausible deniability (Hopkins, 2014; Maurer, 2015).

However, in addressing deception, Bakir et al. (2018, p. 2) make a distinction between consensual and non-consensual persuasion in their framework for understanding 'organized persuasive communication' (OPC). Non-consensual OPC refers to the involvement of deception, incentivisation and/or coercion, while consensual refers to persuasion with the absence of all the three. This distinction is important to note particularly when addressing the seemingly non-manipulative activities conducted by cybertroopers because the level of deception is not always clear. For example, when used in the right context, spreading of positive propaganda through *xuanchuan*, for example, is not necessarily seen as deceit or distraction, and instead as the process of information dissemination despite the larger objectives of the 50 Cent Army. This then creates a 'grey' area of sorts between cybertrooping practices and other activities associated with genuine grassroots mobilisation or movements. Consider how talking points and rapid rebuttals used within spinning might look like spam (or force multiplication of messages). On social media, this may look no different from pre-formatted tweets prepared as a participatory shortcut by

social campaign organisations as described by Dennis (2019). Bakir et al.'s (2018) framework highlights how using deception, incentivisation and coercion can be a way to measure consent to make this distinction.

2.3 Conclusion

This chapter's synthesis of current knowledge about information manipulation serves the important purpose of establishing gaps in existing literature, within which the research presented in this thesis can be situated. Most significantly identified is a lack of detailed empirical data for researchers to work with in their investigations. While computational science methods have advanced this field of study to address this lack of evidence, it is not sufficient to better understand a practice that is intentionally covert, and whose agents are difficult to identify, either as groups of people or the distinction between human, cyborg or bots. More detailed empirical evidence would also serve to illustrate situated practices, instead of relying on generalisations borrowed from different contexts. This is increasingly important as researchers continue to study what has become a transnational issue. It is equally important to focus on context not often studied; in the case of this thesis, the manipulation of online information within a pseudo-democratic regime, and the first significant study into cybertrooping in Malaysia.

The discussion in this chapter on existing techniques of information manipulation will frame this study, to provide a more nuanced understanding of the different ways in which political information can be manipulated online. While the content may be mediated differently, cybertrooping and other techniques of information manipulation which pre-date the internet share certain characteristics. This will be

further developed in this thesis. To begin with, the following chapter outlines the methodological approach for this thesis, as well as an overview of the datasets that make up the empirical evidence mentioned above.

CHAPTER 3

Designing the research project: notes on methodology

This chapter describes the research process for the study presented in this thesis. It begins with a brief introduction on how the research questions were developed, followed by an overview of the main datasets that make up the empirical evidence for this study. Next, it presents the methodological approach that guided this thesis including a discussion on the methodological decisions that were made. The various datasets are then explored in-depth, focussing on the methods of data collection, the treatment of data in preparation for analysis and the limitations surrounding the data. It concludes with a discussion on the ethical considerations made in the research process.

3.1 Setting up the study

This study is an investigation into how cybertrooping serves as an online extension of the state's control mechanisms to secure or retain power through the influencing and manipulation of communication and information in the Malaysian political sphere. It was guided by the core research questions presented in the Introduction chapter of this thesis, which involved identifying the characteristics and activities of cybertrooping, and exploring the ways cybertroopers are mobilised. These characteristics were then contextualised within existing understandings of political communication techniques, and extrapolated to help understand better the global phenomenon of online manipulation of political information.

This study builds on the recommendation I made in my Master's degree dissertation, which found instances of cybertrooping among collected tweets related to the Bersih street rally in Malaysia in 2012. Analysing the cybertroopers in more depth was beyond the scope of that particular study, and thus, I concluded that further investigations "on astroturfing on online social network services" should be conducted because of its "potential to affect the authenticity of information" flowing through platforms such as Twitter (Cheong, 2012, p. 43). Being in possession of evidence of said cybertrooping seemingly supporting the state in a quasi-democratic country, I was able to develop a PhD project that could address the problems noted in Chapter 2 within existing studies of this field. It was also around this time that I came into possession of a dataset of anonymous instructional emails. Together, these two datasets could be studied to understand what cybertrooping looks like, who may be behind the operations and what they do. It is from these realisations that the research questions were formulated, and decisions on what data was needed for a more in-depth PhD study were made.

3.2 Overview of Data Samples

The aforementioned instructional emails are placed at the heart of this study due to the richness of the dataset; they are likely the first set of data of this kind to offer direct empirical evidence regarding the strategies, motivations and mechanisms for the mobilisation of cybertroopers. In total, there are 913 emails in the dataset, which I received unsolicited between 12 March 2012 and 21 March 2014 from an account

using the pseudonym Beruang Biru [Blue Bear[1]]. Among these are over 100 emails that included some form of instructions for social media engagement, the majority of which were labelled 'Online Deployment Strategy'. These instructions are extremely valuable empirical data considering the difficulties researchers encounter in studying an intentionally covert practice. The fact that these e-mails were received unsolicited from an unknown account adds a layer of complexity in verifying the findings from the dataset.

Having already gathered the tweets related to the Bersih 3.0: *Duduk Bantah* rally calling for free and fair elections held in 2012, I was in possession of data which could be used for the purpose of verification and to support the findings in the emails. This was further confirmed with the emergence of literature on big data and computational methods to identify instances of online manipulation of information. The dataset consists of over 60,000 tweets collected on April 28, the day of the rally. From these, I selected 27,431 for analysis (the selection process will be discussed in more depth later in this chapter). I had also collected tweets in 2015 from the next Bersih rally to be organised both for comparison and to see how cybertrooping may have evolved. This dataset contained over 200,000 tweets. I opted to collect data related to the Bersih rallies for two reasons: first, I was already in possession of the 2012 dataset, and secondly, they represented a very significant social movement that was mobilised in Malaysia in the age of social media[2].

Although previous analysis showed that the tweets could confirm some of the tasks instructed by Beruang Biru (Cheong, 2012), the datasets were not able to answer the

[1] It was not clear from the datasets why this name was chosen, although blue is the colour that Barisan Nasional is most associated with.
[2] I describe the political significance of the movement in Chapter 4.

questions of how cybertroopers are mobilised. To provide this context, I created a corpus of over 400 news reports related to cybertrooping in Malaysia based on the archives belonging to Malaysia's leading English newspaper *The Star*. These reports date back to the first mention of cybertroopers in 2004, and were collected over a series of visits until February 2019. Aside from capturing media representation of cybertrooping over 15 years, the news reports serve as a record of statements made about cybertroopers in Malaysia by politicians and media practitioners. However, aware that newspapers may be a permanent source of information but not necessarily the most accurate or reliable, I also conducted a series of interviews with political leaders, activists and journalists, to seek out answers that the datasets I possessed could not provide, including clarifying some statements that were reported on by the media. A total of nine interviews were conducted over two visits to Malaysia.

All of the data mentioned above were analysed using a mixed-method approach, adopted to reflect the varying nature of each dataset.

3.3 Methodological approach

This study focuses on the production of political information, and the ways in which cybertroopers in Malaysia are mobilised to disseminate and engage with such content. It does not attempt to quantify the impact of such practices but is instead interested in the strategies and tactics involved in the creation and dissemination of information related to Malaysian politics online. However, the analysis of the datasets may include some discussion on motivation and intent—that is, what the cybertroopers aim to achieve by engaging in the identified strategies and tactics—although this does not drive the research agenda. As a result, a qualitative research approach is adopted,

taking into consideration Karpf, Kreiss, Nielsen, and Powers's (2015, p. 1890) argument that "qualitative approaches help us answer the *how* and *what* questions that must be addressed in order to answer the *why* and *so what* questions" (emphasis in original) in political communication research.

The value of the aforementioned approach allows me to maximise the richness of the novel dataset in the form of the Beruang Biru emails. It also addresses the limitations discussed in Chapter 2 regarding the difficulties in identifying strategies from data collected using computational data science methods which focus primarily on quantifying the instances of online manipulation of information. I use some of these computational methods in my attempts at detecting online manipulation as well, although my objective goes beyond quantifying the instances but instead qualitatively analysing the data collected to verify findings from the other datasets. Similarly, the analysis of news reports and the tweets may include quantitative elements (being digital objects, they are by nature quantifiable), but I have framed the results within the qualitative research approach.

This mixed-method approach is also applied to address limitations that may arise from relying solely on one over the other. Benoit and Holbert (2008, p. 622) argue that "a combination of qualitative–quantitative insights can lead to a richer understanding of a given phenomenon because each method provides unique insights that cannot be obtained by the other method". They refer to this as triangulation of methods, borrowing from the concept made popular by Denzin (1978, in Benoit & Holbert, 2008). The latter's concept—which covers the triangulation of data sources, investigators, theories and methods—is also useful in this study. For example, the 2012 dataset of tweets was useful in the triangulation

process to validate some of the findings from the Beruang Biru emails. The 2015 dataset of tweets was also used for this purpose, but it allowed me to compare with the analysis of the 2012 tweets for clarity and consistency. The news reports and interviews served the same purpose not just with each other, but also with the other datasets.

Where the primary datasets—that is, the Beruang Biru emails, Bersih rally-related tweets and news reports about cybertroopers—are concerned, this study adopts the thematic analysis approach. Braun and Clarke (2006) made the case for thematic analysis to be used as a foundational method in qualitative research, as opposed to being among options of methods to be adopted. They define it as a "method for identifying, analysing and reporting patterns (themes) within data" (p. 2, brackets in original). Nowell, Norris, White, and Moules (2017, p. 2) note that some scholars do not consider thematic analysis as a method but as a tool used by other qualitative methods. However, they take the same stance as Braun and Clarke (2006, p. 78) in maintaining that it is indeed a method "in its own right". Nowell et al. (2017, p. 2) point out that scholars consider thematic analysis useful "for examining the perspectives of different research participants, highlighting similarities and differences, and generating unanticipated insights", and that it is useful for "summarizing key features of a large dataset". Considering that this study involves the analysis of a variety of different datasets, both large and small in sample size, thematic analysis was a useful method to adopt. In addition, Boyatzis (1998, in Nowell et al., 2017, p. 2) considers thematic analysis to be a "translator" between quantitative and qualitative analyses, which adds to its usefulness for the elements where quantitative aspects are structured in the analysis within the qualitative frame.

As a study that focusses on political communication on the internet, almost every aspect related to the various datasets rely on digital tools to achieve the aims of the different stages of the research process. With regards to collection, the tools required are often specific to the type of data at hand. In the case of capturing a large collection of social media data, it is likely that one requires the use of purpose-built software. In the absence of knowledge in computer science and programming (as was the case with me), researchers tend to rely on commercial analytics and monitoring software. As such, where the datasets of tweets were concerned, I opted to use the affordable Tweet Archivist systems. I used the desktop version in 2012 because it was free to use, and then the paid web version in 2015, which automated the data scraping process. As for news reports, researchers often have to rely on existing databases. In the case where comprehensive sets of data are not available in the more renowned databases such as Nexis, researchers look for more localised archives. As such, I went to the archive at Malaysian newspaper *The Star*. As for the treatment and analysis of data, specialised qualitative data analysis software can be useful. Having access to a licensed copy of Nvivo from the university meant that I was able to use a high-quality piece of software for this aspect of my research. However, sometimes the more ubiquitous tools such as Microsoft Excel, as was the case with this study in analysing the Twitter data, might be sufficient. I discuss the specifics of the above in more detail when describing each dataset later in this chapter.

Distinct from those described above, this study also made use of other digital tools and processes for the purpose of observation and verification outside of the major datasets. This include manually exploring the Twitter timelines of accounts identified from the datasets of tweets or observing the YouTube accounts listed in the email

dataset. There were instances where some of these websites were no longer accessible or available; in those cases, I relied on tools such as the Internet Archive's Wayback Machine[3], which provides historical data of web pages. This tool has been acknowledged by scholars to be a legitimate methodological resource (Arora, Li, Youtie, & Shapira, 2016). In those instances, I did not capture the data to create additional datasets, but instead, used the observation method and made what Jensen (2002, p. 243) called "reflexive notes, which initiate the process of analysis and theorizing on the basis of observations and other data". To conduct those observations, I borrowed elements from a number of scholars who offer insights into studying digital materials beyond just big data, which Salmons (2016, p. xiii) argues is "broad, but shallow". Instead, she calls for the collection of 'deep data', which can be derived from interviews or observation through "deep exchanges" with the research subjects (p. xiii). Robards and Lincoln (2017) offer the 'scroll-back method' as a way to conduct longitudinal study of social media, which involves scrolling through timelines on these platforms in search of digital traces.

How my approach differs from the last two papers mentioned above is that I did not seek to engage directly with the individuals behind the social media accounts I am studying; instead, I opted to engage with their digital data and footprints. Using Purdam and Elliot's (2015, pp. 28–29) typology of digital data, the notes I made were of 'self-published data' ("data deliberately self-recorded and published" which has been made public such as blogs and online profiles), 'social media data' ("data generated through some public, social process" such as Twitter, Facebook and online games) and 'found data' ("data that is available in the public domain, such as observations of public spaces"). These observational data allowed me to understand

[3] Accessible at http://www.archive.org.

better the individuals behind the social media accounts, developing a profile for them using what Rogers (2009, p. 29) refers to as 'post-demographics', that is "the study of data in social networking platforms, and, in particular, how profiling is, or may be, performed". I use the distinction of 'digital' because of the nature of my note taking and capturing of data (borrowing from ethnography, which involves researchers taking field notes and possibly recording their subjects using video cameras), which relies on digital mechanisms, including taking screenshots and the capturing of links and webpages.

3.4 Data collection and analysis methods

In this section, each of the datasets will be discussed in-depth, covering data collection (where relevant), scope of study, process of analysis, and limitations.

3.4.1 *Beruang Biru emails*

The emails from Beruang Biru were sent anonymously and unsolicited to my public email address[4] between 12 March 2012 and 21 March 2014. The recipients of the emails were visible in the 'To' field of the email for the first few months, before being moved to 'BCC'[5]. In total, the dataset contained 913 emails received from a total of nine email addresses.

[4] This email address was listed on my professional website, and differs from my personal Gmail email.
[5] It is not possible to know if these emails were only sent to this particular set of email addresses. There is a likelihood that several mailing lists exists; online observation shows that there were other recipients of Beruang Biru emails, including some emails which were not found within my dataset.

Table 3.1

The number of emails, and addresses, of those received related to Beruang Biru. The addresses for #7-9 have been anonymised to protect the identities of the recipients who had either replied or also sent a group email.

	Email address of sender	Number of emails	Notes
1	**oneberuangbiru@gmail.com**	141	
2	**satuberuangbiru@gmail.com**	72	
3	**1beruangbiru@gmail.com**	691	
4	**1penabiru@gmail.com**	2	An email received on 22 February 2013 noted that this address was an "option" for Beruang Biru, which would be used at particular times. Only one other email using this address was received.
5	**meera_rin@yahoo.com**	2	Both emails were sent using a mailing list system. One of them was an Online Deployment Strategy, sent using the name "Ah Boon" (see below). Texts from both emails were also identical to two emails sent by Beruang Biru.
6	**ahboon4@ymail.com**	1	This email was sent using a similar mailing list system template as the above.
7	**Recipient #1**	1	
8	**Recipient #2**	1	
9	**Recipient #3**	2	

For the purpose of analysis, the first six email address in Table 3.1 were categorised as emails sent by those operating the Beruang Biru accounts because they generally consisted of similar content. Where the first four are concerned, three of them used a permutation of the same username ('satu' is Malay for 'one'), while the contents in one email from the fourth address ('1penabiru' translated literally: 'one blue pen') explicitly stated that it was an alternative account for Beruang Biru. With addresses five and six in Table 3.1, all three emails were similar to those sent by Beruang Biru. The two emails from meera_rin@yahoo.com had different names attached to them;

one was from Ameera Arini while the second—an Online Deployment Strategy email—was from Ah Boon. The text in the email from Ameera Arini was identical to one of the Beruang Biru emails, and both were sent on the same day (27 March 2013). The email from Ah Boon, on the other hand, was identical to an Online Deployment Strategy email from Beruang Biru also sent on the same day (11 March 2013).

This links the name Ameera Arini, and their[6] email address, directly to Beruang Biru. That the name Ah Boon was used with Ameera's email address connects that email address to the other email from ahboon4@ymail.com, and to Beruang Biru as well. Although in this instance there were no duplicates found, these three emails were the only ones in the dataset to use a similar mailing list system (as indicated by the email template and metadata), further suggesting that they are linked and were set up by the same person or organisation. Where the last three email addresses in Table 3.1 are concerned, the four emails sent were from other recipients of the Beruang Biru email—either as 'Replies to All' or as a new message to the same group (but not in a similar tone or format to the regular Beruang Biru emails)—and as such, not analysed for this study, leaving the dataset at 909 emails.

Content of Emails

Emails in this dataset were selected for analysis based on the content in the body, and type of document attached. Of the remaining 909 emails, 784 mainly contained text or attachments in both text format (.txt files, Word documents) and images (photographs, infographics and illustrations). Most of these attachments were

[6] This pronoun is used to avoid any presumption of gender based on the associated names, especially where sockpuppetry may be involved.

'curated' from various sources—such as mainstream media, blogs, and platforms like Facebook and YouTube—although there was the occasional original material attached. These emails mostly had the word "Artikel" [Article] in the subject line, likely referring to the attached articles, followed by the date the email was sent. In general, they did not include any instructions or comments contextualising the attached articles, although some include a greeting followed by: "For your reference". Due to the scope of the study, focussing on instructions to understand how cybertroopers are mobilised and what the nature of their activities is, I excluded these emails from analysis.

Consequently, the remaining 125 emails (some of which are 'Artikel' emails, but which included a more extensive form of communication or instructions) were selected for the purpose of analysis. Among these emails are 20 that had some kind of communication from Beruang Biru, including the initial email sent on 14 March 2012, explaining the purpose of the mailing list, and the one announcing the commencement of the Online Deployment Strategy series of emails ahead of the general election. There are also five emails labelled 'Ralat' [Error], which includes a recall, or corrections, on material sent out previously. The bulk of these emails, however, included directions for recipients to follow, or calls to action. Among these emails are those marked as Online Deployment Strategy (including several labelled Ad-Hoc) which tend to follow a particular template and often labelled as such (or using the acronym ODS). In most cases, the content of the emails was written in

both Bahasa Melayu [Malay Language] and English, although a minimal number of points in the Online Deployment Strategies were in Chinese language[7].

Thematic analysis

The research analysis software NVivo 11 for Windows was used to conduct a thematic analysis of the 125 Beruang Biru emails described above. NVivo had converted all 913 emails into PDF documents (with functioning links, where applicable) and extracted the attachments into a separate folder. This meant that the few Online Deployment Strategy documents sent as attachments were excluded. I then manually downloaded these ODS attachments[8] from the original emails and imported them into NVivo.

To begin with, I created 11 categories to distinguish the nature of each email. These categories were created mainly from the subject lines of the emails; examples include 'Artikel', Online Deployment Strategy, and 'Ralat'. In other instances where the subject lines didn't necessarily reflect the content of the emails—such as those sent by recipients of the Beruang Biru emails or any that included call to actions but not labelled as Online Deployment Strategy—I labelled them simply as 'Replies' or 'Instructions'. This process was helpful in selecting which emails would be used for analysis based on the decisions explained above.

The 125 emails selected for analysis were then subjected to several rounds of coding, identifying the various themes that emerged from the content of the emails. At the initial stage, I created five analytical categories to record 1) any form of calls to

[7] In all instances, the Chinese points were part of a larger Online Deployment Strategy email, which was primarily in Malay or English. Due to my inability to read Chinese characters, I have excluded these points from my analysis except where translations were included within the emails.
[8] The other attachments are not primarily part of the study, and as such, were not downloaded.

action; 2) type of content; 3) time related, such as whether or not an instruction was urgent, or if it was a response to an event/incident or in anticipation of one; 4) source of linked material, such as blogs, Twitter accounts or Facebook pages; and 5) names of people who were mentioned in the emails. Content from the emails was coded to fit a variety of themes within each category. As an example, the coding of emails in the 'call to actions' category of the Online Deployment Strategy emails identified themes such as requests to 'Like' a particular post online, accounts highlighted for 'retweeting', and the social media platforms identified for action. It is important to note that at each stage, I repeated the process of categorisation and coding several times, as some themes only emerged later in the process and required validation.

Limitations

Due to the pseudonymous nature of the emails, I was not able to identify the true identity of the person(s) or organisation behind Beruang Biru. However, putting aside Beruang Biru's explicit mention of helping "the government" to win the 13th General Election (14 March 2012 email), some of the instructions were directed at those managing official accounts belonging to government ministers, other Barisan Nasional politicians or government agencies. This suggests that the people managing the official accounts were taking instructions from Beruang Biru as well. There are also instances where Beruang Biru has requested recipients to be on standby or anticipate an announcement from either politicians—including the Prime Minister—or the government, which suggests that those behind these emails are part of Barisan Nasional's communication mechanism, or at the very least, privy to inside information. As for the legitimacy of the emails, there is evidence that Beruang Biru's

instructions are being carried out by cybertroopers. A Twitter search on many of the talking points crafted for that platform shows numerous tweets from different accounts using the exact same text. On several blogs, some material is directly attributed to Beruang Biru, either as a credit at the end of the post or the more explicit inclusion of the email text (including metadata such as date of email, Beruang Biru's address, and addresses of other recipients of the emails). I argue that the above is enough circumstantial evidence regarding the authenticity of the emails as a source of instruction, and to link Beruang Biru to Barisan Nasional.

3.4.2 *Tweets during the Bersih rallies*

This section centres on Twitter data collected during the 2012 (Bersih 3.0: *Duduk Bantah*) and the 2015 (Bersih 4) rallies, organised by the Coalition for Free and Fair Elections (Bersih 2.0). For this thesis, I analysed these tweets to highlight the ways in which cybertroopers use platforms like Twitter to perform their roles, identify patterns and trends that emerged, and to establish connections that indicate cybertrooping activity. Tweets from the 2012 rally were collected using the hashtag #Bersih, while those from the 2015 rally were collected using #Bersih4. These hashtags were among several that were found on Twitter during the rallies; however, I only chose to focus on one hashtag each during the collection period due to resources available to me at that time, including limitations of the software.

Data collection

I used commercial Twitter analytics software The Archivist Desktop, available from Tweet Archivist[9], to compile the tweets for the 2012 Bersih 3.0: *Duduk Bantah* rally. The software captured tweets using Twitter's API (Application Programming Interface) containing the hashtag #bersih, the main hashtag used by the Bersih 2.0 coalition in the days leading up to the rally. Over 60,000 tweets were captured over a 12-hour period on the day of the protest (28 April). For the 2015 rally, I used the paid web-version of Tweet Archivist instead. The process of data collection behind this version is more hidden; users can simply type in a search term (in my case, the #Bersih4 hashtag) and the software would continue to capture tweets for each month the paid subscription continues. In this instance, over 200,000 tweets were collected over several months.

Managing the two sets of tweets

The Archivist Desktop provided the #bersih data in two formats—.txt and .xml—which were later converted into Excel format for analysis. The web version of Tweet Archivist allowed for downloading in Excel format directly. Back in 2012, I had intended to use Excel only for the preliminary analysis of the data sample, before searching for a more sophisticated analysis software package. However, Excel proved sufficient to deal with all the requirements necessary to analyse the tweets for the purpose of my study. As such, the same method was replicated for this doctoral study. Although I still had the records of the analysis from the 2012 study, I reanalysed both datasets from the beginning for consistency. From all the tweets captured, I selected four primary categories of the data to be used: username

[9] Available from https://www.tweetarchivist.com.

associated to the account that sent the tweet, date and time, the text in the tweet and finally, the unique ID that Twitter permanently associated to each tweet.

Excel was particularly useful in the removal of any identical tweets[10] that made it into the datasets as a result of the capturing process using the two versions of the software. To do this, I used the tweet ID in the Excel Deduplication process. Any other duplicates left in the dataset following this process would either be retweets or similar-worded tweets sent from different accounts (in some instances, duplicate tweets were sent from the same account, but at different times, overcoming Twitter's restriction on sending the same tweets more than once). Following that, I isolated all retweets (such as those using third-party software or Twitter's own embedded retweet function, or manual retweets crafted by cut-and-pasting original tweets), leaving behind primary tweets to be analysed.

Table 3.2

Number of total tweets in the #bersih and #bersih4 datasets, and after being managed for analysis.

Rally	Total Tweets collected	Duplicates Removed	ReTweets	Primary tweets isolated for analysis
#Bersih (Bersih 3.0: *Duduk Bantah* in 2012)	62,462	7,672	27,359	27,431
#Bersih4 (Bersih 4 in 2015)	203,967	601	132,547	70,819

Analysis

Each dataset—that is, from the 2012 and 2015 rallies respectively—was analysed separately. Taking the cue from the findings from Cheong (2012), a search for

[10] In this instance, I use the term 'identical tweets' to refer to the exact same tweets sent from the same account at the exact same time.

duplicates was performed on the column with text from tweets in each dataset. By this stage, the datasets of primary tweets did not include any technically identical ones and retweets, and as such, the search identified similar tweets, which were mostly sent from different accounts. This meant that each Excel file divided the primary tweets into two sheets: one with the duplicate tweets (Sheet A), and one without (Sheet B). I then conducted a first-level thematic analysis of these tweets to identify which among them were in support and which were against the rallies. This provided an indication of which ones may have been sent from pro-Barisan Nasional cybertroopers. Tweets that were deemed neutral—that is, those that did not take a partisan stance—including those from news organisations, made up a third category.

Following this, I coded all of the tweets based on themes that emerged from the data. For example, in the #bersih dataset from the 2012 rally, there were a number of tweets which began with "joining #bersih" followed by a pejorative attribution associated to the rally organisers. A new sheet in the Excel file was then created for all of these tweets (Sheet 'Joining'). I then performed a search in the sheet without the duplicate tweets (Sheet B) for any tweets with the words "joining #bersih" and added those to Sheet 'Joining'. This ensured that all possible tweets based on the "joining #bersih" theme were captured in the same sheet. I replicated this process for the various themes that were found, some of which were based on hashtags used (e.g. #dearambiga, a reference to then-Bersih chairperson Ambiga Sreenevasan) or types of accounts (e.g. news media), and this too sometimes required several rounds of coding.

These categories and themes from Sheet A allowed me to look for patterns of cybertrooping to identify tweets likely sent out by cybertroopers[11]. To ensure that no tweets from these cybertroopers were left out, a search for tweets in the non-duplicate tweets sheet (Sheet B) was conducted based on each suspected cybertrooper account and added to the various themed sheets described above. This meant that the final theme sheets included all possible tweets from the suspected accounts (across Sheet A and Sheet B). The coding process above was then repeated to include the newly added tweets into the earlier identified themes.

Both datasets, although collected three years apart, contained primary tweets that could be considered cybertrooping, and in some instances, showed similar patterns and behaviours. While nothing in these tweets directly link these accounts on Twitter to Barisan Nasional, the patterns identified matches with what I identified as techniques of cybertrooping. Particularly, in both cases, the tweets sent out looked like they were part of a coordinated top-down strategy.

Limitations

It was not possible to ensure that the data captured are fully representative of all tweets sent out during the period of the two street rallies for three reasons. First, Twitter API rules, as well as unknown algorithms of third-party analytics tools, make it impossible to tell which tweets were collected, what might have been excluded and how many there were in total. To illustrate, the Twitter API only provides access to a random 1% of all public tweets, which has been addressed by scholars as a methodological limitation (see Bruns & Liang, 2012; Gerlitz & Rieder, 2013). Secondly, the respective #bersih and #bersih4 hashtags I collected from are only one

[11] I elaborate on how cybertroopers were identified from the datasets in more detail in Chapter 6.

of several that may have been used to tweet about each of the rallies during those periods (for example, #bersih2, #bersih3 and #bersihreport). Finally, it is possible that Twitter users (including cybertroopers) had opted to tweet without the use of hashtags and as such, those tweets were also not captured. These limitations meant that although the data used in this study showed various instances of cybertrooping that are worth investigating, the analysis of the data cannot be comprehensive. However, considering that I am primarily using these tweets to validate the core dataset—the Beruang Biru emails—in the triangulation process, these limitations should not significantly affect the results of this study.

3.4.3 *News reports related to cybertrooping*

This section discusses the analysis of news reports related to cybertrooping as a practice in Malaysia to understand the ways cybertroopers have historically been discussed in the media. Studying these reports can provide context for the study, especially since the practice is mostly conducted covertly online. These news reports also serve as instruments of record, capturing both the discussions on cybertroopers over the years and quotes from political leaders and government officials discussing cybertrooping.

Data collection

These news reports were compiled from the digital archive at Star Media Group Berhad (which publishes *The Star* newspaper), which is available to its employees for reference (although members of the public can pay a nominal fee for access). Having access to Star Media Group's data was extremely beneficial to this study because it

contained material from so many different localised news organisations. It also appeared to be more comprehensive than those found on other databases such as Nexis[12]. The Nexis database also did not include articles from *The Star*, which made up a significant number of articles in the dataset used for this study. In total, less than 50% of the number of articles in Star Media Group's archive were found on Nexis.

The digital asset management system used by the organisation's information management department is the DC-X Content Hub, which I was familiar with as a former employee of the newspaper. This archive includes all of *The Star*'s past published content, as well as an extensive collection of news reports published by other media organisations. For example, the earliest report in the archive mentioning 'cybertroopers' as related to politics was published on February 25, 2004 in the *New Straits Times* (another English daily in Malaysia).

This dataset consists of 403 news articles containing content from 17 media outlets—both print and online—from Malaysia, and two from Singapore (*Straits Times Singapore* and *The New Paper*)[13]. These media outlets include English and Malay language newspapers as well as English-language online news portals and blogs. These news reports were retrieved over three visits between December 2015 and February 2019 (each retrieval process only collected data which had not been previously obtained based on publication date). Each time, the same search process was conducted using nine search terms: Cyber trooper, Cyber troopers, Cyber

[12] For example, a search of the terms 'cybertrooping', 'cyber-trooping' and 'cyber trooping' on Nexis only produced two articles published in 2018, while the DC-X archive contained articles dating back to 2012.

[13] For context, these 17 news media outlets include all the major national English language newspapers—*The Star, The New Straits Times, The Malay Mail, The Sun* and *The Edge*—and three of the five major Malay language newspapers—*Berita Harian, Utusan Malaysia* and *Sinar Harian*. Is it unclear if the dataset did not include reports from the two other Malay newspapers because the publications did not use any of the search terms, or that the archive did not contain any material from them.

trooping, Cyber-trooper, Cyber-troopers, Cyber-trooping, Cybertrooper, Cybertroopers, and Cybertrooping[14].

Due to the fact that the system did not contain a feature to download the news articles that showed up in the search results (except for those published in *The Star*), I had to archive them manually. Each news report was imported into a Microsoft Word document using the cut and paste function, leaving nine files in total during each visit (one for each searched term).

Managing the data

To analyse the articles, I used NVivo 11 for Windows. Due to the large number of news reports in each of the nine files, I pre-empted potential problems with the coding by creating individual files for each news story (again, using the cut and paste feature in Microsoft Word), naming the respective files by publication date and search keyword (e.g. 2004 Oct 1 Cyber Troopers). In the event that there was more than one article published on the same date (from the same keyword search result), I added a distinctive letter alphabetically to the date (e.g. 2012 July 15b Cybertrooper). All of these were then imported into NVivo for coding and analysis. A preliminary run through of all the files indicated that there were many duplicate articles (this could have emerged from a glitch in the search system and/or the fact that some articles used multiple permutations of the term 'cybertrooping'). Duplicates were removed during the coding process, and this was made easier by my earlier decision to separate each news stories into a standalone file. During the coding process (explained below), there were also a minimal number of news reports which were not related to cybertrooping in Malaysia, which was nevertheless still picked up by the

[14] Searches on the system were not case-sensitive.

search. For instance, an article on gaming used the term 'cyber' and 'trooping' separately and within a different context. These articles were also removed, leaving the dataset to contain a total of 403 news reports for analysis.

Thematic analysis

The process of analysis of these news articles was more straightforward compared to the analysis of the two other datasets previously discussed. I coded aspects such as newspaper title and year of publication alongside the various themes that eventually emerged from the data. Among the themes found included those that referred to particular events (such as the disappearance of the Malaysia Airlines aeroplane in 2014) and references to particular groups (such as accusations against the alleged opposition cybertrooper group Red Bean Army). On a more general level, I was also able to code, for example, instances of admission, accusation, and denial by political leaders related to cybertroopers, the way cybertroopers are described with regards to remuneration (paid, volunteers, gifts and reimbursements), and cases where cybertroopers are seen in a positive or negative light.

Limitations

Relying on Star Media Group's archive meant that I had to use the DC-X system, which was not created for the sole purpose of historical archiving. The limitations of the system meant that much of the retrieval work had to be done manually (such as cut and pasting each news report), leaving space for human error. More significantly, however, is that because the system is linked to *The Star*'s daily publishing process, it can only guarantee that all articles from that specific newspaper are included. While discussions with information officers at Star Media Group indicated that the archive

of material from other news organisations is comprehensive, a search on the websites of some of these newspapers showed that there were articles excluded from my dataset. It is not clear if this was because Star Media Group's archive is not as complete as has been claimed by the officers, or if the reports I found elsewhere online were not published in print versions of newspapers, and as such, not included in the archive. However, I believe that this is the most comprehensive database available where this topic is concerned, and that the resulting set of 403 news reports represents sufficient material for this study, especially when it includes all of *The Star*'s news reports (being the largest English-language newspaper in Malaysia[15]).

One other issue arising from this dataset of news reports, which only became clear during the process of analysis, was that not all 403 news reports included the search terms within the text. This was because the search process also included any articles that were tagged within the metadata fields using at least one of the search terms. I have chosen to retain these reports within the dataset because they all address the focus of this study. This is further supported by conversations with information officers at Star Media Group who felt the same way, hence the tagging of the reports with those keywords from the outset. Additionally, I had already removed any articles that included the search terms but used in different contexts, so all articles in the final dataset are related to cybertrooping-like practices in Malaysia.

[15] Based on annual data on newspaper circulation from Malaysia's Audit Bureau of Circulation (ABC). On its website, the ABC notes that *The Star* is Malaysia's "leading English daily". http://abcm.org.my/members-list-backup-20180813/newspapers-west-malaysia/the-star/

3.4.4 *Interviews*

Although I did not initially design interviews into the study, a total of nine of them were eventually conducted. The first five interviews took place in December 2015, early in the process, to inform the crafting of the research question and help in deciding what sort of data was necessary to be included[16]. Two Malaysian activists working in digital rights and media freedom were interviewed as were three media practitioners. Two of the three (one of whom had left the media industry by the time of the interviews) were technology journalists during the period when Barisan Nasional cybertroopers were believed to have started their operations, while the third had published an article on cybertroopers for an online portal just before interviews were conducted. All of them were asked a series of open ended-questions tailored to their expertise.

In 2018, following the change of regime in Malaysia and as I approached the final stages of my analysis, I decided to interview people involved in the 14th General Election to verify some of the findings from the analysis of the datasets. Three politicians in total agreed to be interviewed, all of whom are from Pakatan Harapan, the current ruling alliance[17]. One, who was involved in their party's communication team, declined to be named and therefore is identified in this thesis as Politician A. The other politician interviewed was Maria Chin Abdullah, the former chairperson of Bersih 2.0 overseeing the Bersih 4 rally, who transitioned from activist to politician at the 2018 general election. The third politician interviewed was Foreign Minister Saifuddin Abdullah, who had been reported discussing Barisan Nasional

[16] As a result, none of these interviews are directly referenced in this thesis.

[17] I had attempted to contact four Barisan Nasional politicians, including those believed to be directly involved with cybertroopers. However, none of them responded. It is not clear if their silence was due to the topic of study, or if this was because I contacted them only a few weeks following their party's defeat at the elections.

cybertroopers while he was part of the Barisan Nasional government[18]. The fourth person interviewed was activist Ivy Josiah, who was part of Maria Chin's campaign team.

Only those affiliated to Pakatan Harapan responded to requests, and as such, the interviews do not collectively reflect the breadth of Malaysia's political scene. However, among those interviewed have been or are part of parties that were accused of engaging in cybertrooping—including one political who was quoted in the news reports analysed—and as such, offered valuable perspective to this study. The open-ended questions asked of them were specific to their respective parties, campaigns and experiences. For this thesis, their responses were used to further emphasise the findings made from the primary datasets, to provide more context, or for triangulation purposes.

3.4.5 *Miscellaneous Data*

Throughout my research period, I spoke to numerous people formally and informally about my investigation. In some instances, these were in a professional setting such as at academic conferences in Malaysia and abroad. In others, many of these conversations happened in social settings with former colleagues, acquaintances and friends. Over the years, many of the people that I spoke to contacted me at various points with information or potential leads that they thought would be relevant to my research. As such, I am in possession of numerous documents related to cybertrooping—primarily linked to the Barisan Nasional government—which I have also included as part of the analysis in this thesis. In all of these cases, the documents

[18] See Chapter 5.

were shared with me on the condition that they are not published or linked back to my source. Where I refer to them in the thesis, I cite them as 'Anonymous Correspondence'. In the one instance where I have included a document, it is because a copy had been posted onto a public forum on the internet, as I go on to explain in Chapter 6.

3.5 Ethical considerations

Considering the sensitive nature of the topic of study, ethical considerations were at the forefront of the research process right from the beginning of my doctoral study. Lee (1993, p. 4) offers a simple definition for 'sensitive research', that is, "research which potentially poses a substantial threat to those who are or have been involved in it". This, according to Lee, refers to the subjects of study, those being investigated as well as the researcher. Considering Malaysia's heavy-handed history of clamping down on dissent, and silencing those they consider to be critics[19], I spent considerable time at each stage of the research process reflecting on the ethical issues that may arise. This practice is consistent with the suggestion by Markham, Tiidenberg, and Herman (2018, p. 6) that the role of the researcher conducting big data research involves "interrogating what is happening along the string of actions that eventually lead to the construction of data, focussing on human practices and nonhuman processes that function interpretively, and reflecting on various levels and stages of possible impact of such actions, constructions and interpretations".

[19] I discuss this further at length in Chapter 4.

Formally, I sought ethics approval from the ethics committee at the University of Nottingham's School of Cultures, Languages and Area Studies. In terms of data collection, ethics approval was granted for the collection of the 2015 *Bersih 4* rally-related tweets before I formally began my doctoral studies[20], due to the timing of the rally. Where the 2012 *Bersih 3: Duduk Bantah* rally-related tweets were concerned, the dataset was already the subject of a completed dissertation. No ethics approval was required from my institution of study at the time because no direct contact was made with any particular individual (and tweets were deemed to be public; no data were collected from private or locked accounts). Ethics approval was also granted for the observation (and data scraping) of online activities of accounts identified through the analysis of the other datasets. I was not required to seek ethics approval for the archive research related to the news reports due to the public nature of published news content; however, I did seek permission from Star Media Group's Chief Executive Officer to access the archive at no cost, making clear my intention of using the data for research purposes.

The ethics approval process was more complex for the use of the Beruang Biru emails in this study. One particular consideration was in terms of ownership of the data: how did I come to be in possession of these emails? The process required me to evidence that these emails were not solicited by me from the sender or any other parties. Proving a negative was a difficult task but this was eventually resolved by providing evidence of another recipient (Recipient #2 in Table 3.1 above) replying to one of the emails we received, asking the person behind Beruang Biru to identify

[20] By this time, I had already been accepted into the PhD programme at the university and had been in touch with my supervisors.

themselves. This email was circumstantial evidence that there are people on that mailing list who received the emails unsolicited, in the same way I made my claims.

As a personal exercise on ethics considerations, I turned to the recommendations for the Association of Internet Researchers Ethics Working Committee published in the Ethical Decision-Making and Internet Research (Version 2.0)[21] document to guide my research. Despite having already gained formal approval for my datasets, I was aware of the growing debate within the field of internet research as to what may or may not constitute as public and private information (Hookway, 2012). I also considered the implications of identifying individuals by their usernames in the analysis of my 'sensitive' study. In some cases, I have opted not to use a pseudonym (as noted in my formal ethics applications). I made this decision for two reasons. First, many of the accounts identified were already pseudonymous (often through sockpuppetry). Second, many of these accounts and tweets are already public. Even if I didn't directly identify them by username, a search of the text I used as examples in my analysis chapters (whether the talking points from the emails or the similar tweets) on Google or Twitter would reveal the identities. Where I am able to de-identify an individual and there is no direct evidence that they are involved in cybertrooping, I have anonymised them such in the same way I did with the recipients of the Beruang Biru emails earlier in this chapter.

On a final note related to the discussion on the 'sensitive' nature of this study, I had, from the start of my doctoral studies, engaged in numerous conversations with my supervisors regarding the possible implications to my personal safety. We had pre-emptively considered a number of ways to address this issue, including the possibility

[21] Available at http://www.aoir.org/reports/ethics.pdf.

of placing an embargo on the submitted version of this thesis so that it remains confidential, or presenting the data in such a way that does not implicate anyone. After more than three years of working on this study, the circumstances have changed. Cybertrooping-like practices are now the subject of mainstream discourse globally, and while many states and political actors still deny involvement, accusations of such engagement has little direct consequence. I also feel that this study, while focussing heavily on Barisan Nasional's cybertroopers, presented findings in a fair manner, and with academic rigour. Most significantly, Malaysian politics have changed notably, with Barisan Nasional no longer in power, providing more confidence to me that the results of this study can be published with little or no consequences to myself as the researcher. Even before this regime change, however, I have also tested the waters, so to speak, by publicly discussing some elements from my study at academic conferences and in media interviews, with no known implications. Perhaps the fear I carried with me was just a product of Malaysia's 'chilling effect' in a previously controlled environment, which I discuss further in the following chapter.

CHAPTER 4

Politics, Pacts and (Illiberal) Practices: Malaysia in context

This chapter will help contextualise the discussions in Chapters 5 to 8 by highlighting the illiberal practices by Barisan Nasional related to curbing dissent and media control. It will provide an understanding of some of the factors that have led to Barisan Nasional's adoption of online strategies such as cybertrooping. It begins with an in-depth discussion of the Malaysian political landscape. This includes a brief background of the country's political parties and pacts, and their relationship to communal politics[1].

The chapter then documents the country's fraught history of control of its citizens before describing how the use of the internet aided efforts of resistance against the state. At this point, a brief history of the Bersih movement, challenges to it by state-linked actors and its reliance on new communication technologies is presented. It then continues with a discussion on the government's efforts in clamping down on dissent on the internet. Building on this, the chapter ends by looking at how the Barisan Nasional governments of the past had used the internet for information warfare, including the mobilisation of cybertroopers.

[1] For the purpose of this thesis, most of the discussion on political parties and ethnic make-up of the country will focus on Peninsular Malaysia (formerly Malaya), where the government is located. Issues from this part of the country tend to dominate the political discourse in Malaysia, much to the displeasure of those from Sabah and Sarawak (located east of the peninsular on the island of Borneo). As such, most of the issues, trends and patterns that emerged from the datasets are framed within the lens of peninsular politics. For example, the Lahad Datu incursion in Sabah (to be discussed in Chapters 6 to 8) played up by cybertroopers tended to focus on the response by Prime Minister Najib or the nation's armed forces, instead of paying attention to local leaders in the state.

4.1 Party, pacts and (ethnic) politics in Malaysia

Malaysia (then known as Malaya) inherited the Westminster model of democracy following independence from the British in 1957, with elections held at regular intervals (within five-year periods) at both federal and state levels. Barisan Nasional (National Front[2], or BN), emerged victorious at each federal general election until May 2018, when an unprecedented shift of power away from a coalition that had essentially[3] governed for over 60 years occurred. The BN coalition was birthed out of consociationalism[4], and claimed to speak for a multi-ethnic Malaysia; the three main component parties which led efforts for independence—the United Malay National Organisation (UMNO), Malaysian Chinese Association (MCA) and Malaysian Indian Congress (MIC)—as their respective names suggest, represent the three major ethnicities[5]: Malay, Chinese and Indian[6] (Ngeow, 2017). Lemière (2018, p. 117) referred to this multi-ethnic coalition as a "façade" for the nationalist UMNO, the dominant party in Barisan Nasional[7]. Due to the embeddedness of Islam in the Malay identity—the post-independence Federal Constitution defines a Malay person

[2] The name National Front should not be confused with the far-right political party in the United Kingdom. The English version of the name should be seen as a translation of 'Barisan Nasional'. Before BN was founded in 1973, it went by the English name, Alliance Party. While nationalism is at the heart of the coalition, and as such, it has been described as being a right-wing coalition, it is worth noting that the main parties that make up BN were formed in the struggle for independence, and in response to colonial rule (Mohamad, 2002; Singh, 1991).

[3] The coalition ran in each election post-independence as the Alliance Party. At the 1969 elections, the regional parties from Sabah and Sarawak—which had formed Malaysia alongside Malaya and Singapore in 1963—ran separately but were aligned to the Alliance. It was only in 1974 that all of the parties formally ran together as Barisan Nasional.

[4] Elazar (1985, p. 18) describes the principal characteristic of consociationalism as when "non-territorial constituent units share power concentrated in common overarching government".

[5] The Malay and indigenous communities make up 69.1% of the population, while the Chinese and Indians make up 23% and 6.9% respectively. Other ethnicities in Malaysia, often referred to as 'Others', make up the remaining 1%. In offering those figures from the Department of Statistics, Wong (2018, p. 766) notes that these numbers do not reflect the complexities of the Malaysian population by lumping "together Malays in the Peninsula and Muslim natives and non-Muslim-natives in Borneo who do not have homogenous experiences and political outlooks".

[6] The Chinese and Indian communities arrived in waves since pro-colonial times, but most significantly in the mid to late 19th century and early 20th century (Gabriel, 2015).

[7] Historically, all of Barisan Nasional's Prime Ministers and their deputies were UMNO leaders.

as someone who professes Islam—religion is often intrinsically linked to issues of ethnicity and Malay nationalism (Lian, 2001).

Indeed, Malaysia is a country deeply ingrained in communal politics, perpetuating the colonial legacy surrounding issues of ethnicity. Noor and Leong (2013) describe how the British divided labour during their rule by ethnicity; generally, the Malays were unwaged while the Chinese and Indians functioned within a capitalist structure. This division was further heightened by the Japanese occupation during World War II, "pitching one ethnic community against the other" (p. 716). While policies promoting multiculturalism have been introduced over the decades due to "ethnic pluralism" from the demographic makeup of the country (p. 715), they have not been able to overcome the underlying tensions from the divide. Among the Malays, the Chinese were seen to be an internal threat, while the non-Malays worry that they would lose their cultural identities by being assimilated into the Malay national identity (Hassan, 2004; Wong & Ooi, 2018). It would come as no surprise that with such deep historical divisions, and political parties in Malaysia situated along ethnic lines, issues surrounding ethnicity would shape the political fabric of the country (see Wong, 2018, for an extended discussion on the communal politics of Barisan Nasional).

Over the decades, the opposition was made up of numerous parties that have by and large operated separately. The two largest parties in Pakatan Harapan (or PH) describe themselves as multi-ethnic, although the Parti KeADILan Rakyat (PKR, People's Justice Party) is generally dominated by Malays and the Democratic Action Party (DAP) is predominantly Chinese (Shiozaki, 2007; Wong, 2018). The other parties in the bloc are generally mono-ethnic or regional.

Table 4.1

List of the main political parties in Malaysia currently, and their affiliation and ethnic make-up. Almost 40 parties contested at the 14th General Election in 2018. Years listed in brackets refer to election years when the respective parties were part of a particular coalition or alliance.

Party	Acronym	Coalition/Alliance	Ethnic make-up
United Malays National Organisation	UMNO	Barisan Nasional	Malay
Malaysian Chinese Association	MCA	Barisan Nasional	Chinese
Malaysian Indian Congress	MIC	Barisan Nasional	Indian
Democratic Action Party	DAP	Pakatan Harapan (2018) Pakatan Rakyat (2008 and 2014)	Multi-ethnic but predominantly Chinese
Parti Islam Se-Malaysia Malaysian Islamist Party)	PAS	Barisan Nasional (1974) Pakatan Rakyat (2008 and 2014)	Malay
Parti KeADILan Rakyat (People's Justice Party)	PKR	Pakatan Harapan (2018) Pakatan Rakyat (2008 and 2014)	Multi-ethnic but predominantly Malay
Parti Pribumi Bersatu Malaysia (Malaysian United Indigenous Party)	PPBM	Pakatan Harapan	Malay
Parti Amanah Negara (National Trust Party)	Amanah	Pakatan Harapan (splinter party from PAS)	Malay

One of these parties is Amanah, a splinter party from the opposition party Parti Se-Islam Malaysia (PAS, Malaysian Islamic Party). The past three elections saw a number of the aforementioned political parties come together[8], first informally as Pakatan Rakyat (People's Alliance) in 2008 and 2013 to weaken BN's grip on power, then taking over government as the formal bloc Pakatan Harapan (Alliance of Hope) in 2018.

[8] The first iteration of this alliance dates back to the 1999 elections when PAS, DAP, Keadilan (now PKR) and Parti Rakyat Malaysia (Malaysian People's Party) formed an electoral alliance with a joint manifesto called Barisan Alternatif (Alternative Front). DAP would eventually leave the alliance in 2001, and the remaining three parties would contest under the same banner in the 2004 elections (Moten & Mokhtar, 2006).

At each of these elections, the opposition parties had to compete not only against incumbent advantages, but also a weak electoral system due to media control, malapportionment and gerrymandering, and money politics (Chan, 2018; Weiss, 2013). Saravanamuttu and Mohamad (2019) also argue that the 'monetisation of consent' is deeply ingrained in Malaysian politics, through the pacification of the public via cash payments targeted at communities with voting potential and subsidies, among other forms. Alongside an increasingly strong opposition force from the late 1990s onwards, a "vibrant" civil society has traditionally worked with the opposition parties attempting to keep the long-ruling Barisan Nasional accountable (Weiss, 2009, p. 742). While the above scenario describes a complex but vigorous political landscape, many scholars do not consider Malaysia truly democratic.

Whether or not the recently-elected Pakatan Harapan government will change opinions is not yet certain, but the BN-led Malaysian governments of the past have been described with such negative terms as "authoritarian" (Slater, 2003, p. 81), "semi-democratic" (Case, 1993, p. 183) and "competitive autocratic" (Yom, 2009, p. 152). Explaining his choice term, Case (1993, p. 186) argues that Barisan Nasional has successfully brought together elements of soft dictatorship, with "the state's tolerating the formation of opposition parties and interest groups even as it closes off electoral routes and lobbying channels to state power" and hard democracy, which involves "the state's scrupulously calling elections while preventing opposition elements from organizing effectively to contest them". After all, Malaysia's political history has been marked by the use of illiberal practices by Barisan Nasional governments to retain power, including silencing opposition voices and electoral irregularities (Hah, 2012; Leong, 2015; Weiss, 2017).

Mahathir Mohamad is perhaps the most notorious of the Barisan Nasional Prime Ministers—traditionally the president of UMNO—and has been criticised for his "authoritarian methods" (Lemière, 2018, p. 115). During his first tenure as Prime Minister, which spanned 22 years between 1981 and 2003, making him the country's longest serving leader, Mahathir has been criticised for weakening democratic institutions such as parliament, the judiciary, and media (Slater, 2003). In 2009—despite not being in office—Mahathir orchestrated the ousting of his hand-picked successor Abdullah Badawi in favour of Najib Razak, the sixth Barisan Nasional Prime Minister (Chin, 2017). The latter began his term as Prime Minister considered by some scholars as a reformist aiming to move his party towards the political centre (Brown, 2013), but his efforts in clamping down on dissent as he began facing a flurry of corruption allegations suggests otherwise (Case, 2017).

In what can be described as irony, it was Mahathir who led the charge against Najib at the 14th General Election on a pro-democracy and reformist platform, causing Barisan Nasional's first defeat since its inception. In 2016, Mahathir had brought together his political rivals from the opposition, alongside civil society leaders and other prominent citizens, to launch a 'Save Malaysia' campaign to call for the resignation of Najib (Kassim, 2016). This event was momentous because it brought together decade-old political foes, including those who have been jailed under draconian laws by the Mahathir regime during his first tenure as Prime Minister. This was a prelude to the formation of Parti Pribumi Bersatu Malaysia (PPBM) led by numerous former UMNO leaders including Mahathir and his son Mukhriz, which together with several other opposition parties, formed Pakatan Harapan that won the 2018 general election.

That so many political parties have roots in Barisan Nasional should not be considered unusual. Due to Barisan Nasional being a coalition, various political parties have at different times in history been affiliated to, or contested against, it. For example, the Malaysian People's Movement Party (Gerakan), which was formed in 1968, had contested as an independent party at the 1969 elections, but eventually joined the Alliance Party three years later. Gerakan stayed as part of the coalition when it became Barisan Nasional until the electoral defeat in 2018 (Ooi, 2017). The Islamic party PAS, on the other hand, contested as part of Barisan Nasional in 1974 (Noor, 2004), but later became part of the Alternative Front and the People's Alliance.

Even in BN's leading party, UMNO, power struggles at various times of its history have led to new splinter parties being formed. In 1987, a faction within the party challenged the results of the hotly contested UMNO elections in court, alleging that there existed illegal local branches of the party that had participated in the polls (Singh, 1991). The High Court ruled that the existence of these illegal branches "rendered UMNO itself as an 'unlawful' society" (p. 716). Mahathir, who led the faction that was victorious, proceeded to register a new party, which is essentially the UMNO that currently exists. The other faction formed Semangat 46, which contested two elections (as part of a pact with various opposition parties including DAP and PAS at different periods). It eventually disbanded in 1996, with many of the core members returning to UMNO. Since then, two other major parties have been formed based on splinters from UMNO: PKR, which is led by former Deputy Prime Minister Anwar Ibrahim, and Mahathir's latest party PPBM. Both these parties are currently in government as part of Pakatan Harapan.

4.2 Draconian laws to clampdown on dissent and control the media

In 1998, Anwar Ibrahim was dismissed from both UMNO and the Cabinet after he refused to resign at the request of Prime Minister Mahathir. Until that point, Anwar was destined to be the next prime minister, having been personally selected and groomed by Mahathir to take over the role. In the days that followed the sacking, Anwar faced a series of charges for sodomy—illegal in Malaysia as part of a colonial law that is still in effect—and corruption. The relationship between the two had already been fractious for several years (Chin, 1997), but Mahathir was increasingly feeling politically threatened by Anwar[9]. Thus, the Prime Minister privately called for his deputy's resignation, in lieu of being sacked and subjected to a "campaign of humiliation" (Case, 1999, p. 5). The campaign is believed to be Mahathir's attempt at damaging Anwar's popularity, which was growing out of the latter's moral and charismatic status (Abbott, 2000).

In 2018—after almost 20 years of claiming his innocence and that the charges were politically motivated—Anwar was released from prison and given a royal pardon by the King, a constitutional monarch. This happened on the recommendation of none other than Mahathir, who had returned to power as Prime Minister, merely days after Pakatan Harapan brought down Barisan Nasional's rule (Ellis-Petersen, 2018). At the time, Anwar was serving a five-year sentence for a second accusation of sodomy—also believed to be politically motivated—while he was opposition leader against BN's most recent Prime Minister, Najib Razak. It may never be known if seeking the pardon was an admission by Mahathir that the 1998 charges were trumped-up, or just part of a political deal between two former foes who have come together to oust

[9] Scholars note that Anwar's pro-International Monetary Fund (IMF) response to the Asian Financial Crisis brought to light his power-struggle with Mahathir (Pang, 2000).

a common enemy in Najib. What is clear, however, is that the events described above show just one slice of Malaysia's history of silencing anyone who poses a challenge to the status quo.

Malaysian leaders have long relied on a variety of legal mechanisms to suppress any forms of resistance through the sustenance and use of laws[10] described as "draconian" (Lim, 2017, p. 211; Wong et al., 2010). For example, the Sedition Act 1948, a broad and vague colonial law, is still in effect and has been used to investigate—and in some cases charge—politicians, media practitioners, academics and activists. In 2015, the law was updated to cover online communication and included a mandatory jail sentence (Leong, 2015). Since then, bloggers, citizens and even satirists have been probed for sedition (Lim, 2017; Tapsell, 2013b); until Barisan Nasional's electoral loss, political cartoonist Zulkifli Anwar Ulhaque had faced multiple sedition charges that could have seen him jailed for up to 43 years, if convicted, for his professional work and for the series of tweets he posted criticising the second jailing of Anwar Ibrahim for sodomy. The charges have since been dropped.

Until 2012, the ruling government also used the Internal Security Act 1960 (more commonly referred to as ISA), which allowed for detention without trial, against its opponents. The law was most famously used during *Operasi Lalang* in 1987, a crackdown to contain ostensible ethnic tensions, set against the backdrop of UMNO's power struggle. Under the directive of Mahathir, the operation saw to the

[10] At the most recent general election, Pakatan Harapan ran on a manifesto which promised to "abolish repressive laws" such as the Sedition Act, Security Offenses (Special Measures) Act (Sosma), and the Peaceful Assembly Act ("Buku Harapan," 2018, p. 61). However, they have yet—as of July 2019—to repeal any of the 10 laws they listed in that section of their manifesto book.

arrest of 107 people across Malaysia, including politicians, activists, and students (Lee, 2008).

When the ISA was finally repealed in 2012 to fulfil a promise made by Najib in his maiden speech as prime minister, it was replaced instead by the Security Offenses (Special Measures) Act 2012 (Sosma) which still allowed for detention without trial. In response to criticisms the new Act was just the ISA in a different form, Najib had promised not to use it for political expediency (Varkkey, 2017). However, just ahead of a rally by Bersih 2.0 (the Coalition for Clean and Fair Elections) in November 2016, which included a call for Najib's resignation, its chairperson Maria Chin Abdullah was detained under Sosma.

The Police Act 1967, which required discretionary police permits for public assemblies, was also repealed in 2012. In its place is the Peaceful Assembly Act 2012, which removed the required-permit provision (with the caveat that the police are notified 10 days in advance). However, this version of the law explicitly considers protests unlawful, thus allowing the Home Ministry and police to declare some street assemblies as illegal before the event even took place (Brown, 2013). Scholars have argued that the newer legislation was more restrictive despite the removal of "headline powers" which were previously subjected to criticism (p. 158). In the past, water cannons and tear gas were used to violently disperse crowds at peaceful rallies which were deemed illegal by the authorities (Khoo, 2014).

When it comes to controlling the media, the Malaysian authorities have often used the Printing Presses and Publication Act 1984 (PPPA), despite the fact that many of the country's most-read newspapers (and a majority of the television stations) are owned either directly or indirectly by the main Barisan Nasional component parties:

UMNO, MCA or MIC. While the Internal Security Act was used on individuals during *Operasi Lalang* in 1987, four publications—*The Star*, *The Sunday Star*, *Watan* and *Sin Chew Jit Poh*—had their licenses, a proviso of the PPPA, suspended. A year later, the Mahathir government tightened the law by requiring mass circulation newspapers to have their permits renewed on an annual basis. This condition was reversed as part of amendments made to the law in 2012 during Prime Minister Najib's tenure, but the Home Ministry still holds the power to issue, revoke or suspend licenses.

The PPPA has had at least two significant effects on Malaysian media and political discussions. First, it placed immense pressure on the print media to toe the government line (Gong, 2011). Decades after *Operasi Lalang*, the spectre of the incident still hovers over the media industry, and alongside the other draconian laws mentioned above, has institutionalised a culture of self-censorship in the media sector (Smeltzer, 2017). In 2006, Information Minister Zainuddin Maidin in a press statement invoked the memories of the 1987 incident, in what some perceived as a veiled threat, by advising the media to learn from Malaysia's journalism history (Mohd Sani, 2009). Indeed, the PPPA was once again used in 2015 on two newspapers—*The Edge Weekly* and *The Edge Financial Daily*—which had their permits suspended for three months after they published a series of articles accusing Najib of corruption[11] (Ramzy, 2015).

Secondly, the PPPA has also been used to directly impact on the opposition's popularity. In 1999, the Home Ministry decided to allow *Harakah*, owned by opposition Islamist party PAS, to publish only fortnightly instead of twice a week as it had previously done after the publication grew in popularity and started eclipsing

[11] As of July 2019, Najib is still defending himself against some of these charges in court.

the circulation numbers of other mainstream newspapers (George, 2007). This follows the arrest of *Harakah*'s editor in 1999 after the general election, when PAS made major gains which allowed them to form two state governments (Shiozaki, 2007).

4.3 The internet as a tool to fight back

When the World Wide Web first came to Malaysia in the mid-1990s, the internet promised to be a godsend for dissenters who lacked access to the mainstream media. This was especially significant because the Malaysian government, under Mahathir's rule, did not opt to put in place any control mechanisms on the internet. George (2006, p. 56) notes that this was unlikely to have been the effect of a "lack of authoritarian imagination", although it is possible that the government had initially failed to appreciate the way that the internet could facilitate the expression of dissent. Officially, it was Mahathir's aim to see through Vision 2020—his goal for the country to achieve fully developed country status by the year 2020—which paved the way for a 10-point Multimedia Bill of Guarantees that includes a no internet-censorship guarantee. The guarantees were used to lure foreign entities to invest in Malaysia's Multimedia Super Corridor—originally envisioned as the Asian Silicon Valley—set up in 1995 to attract IT and multimedia companies (Weiss, 2012).

Many Malaysians took advantage of the guarantee of no censorship, and this led to a proliferation of activities and platforms which served as alternatives to the information that was flowing through the government-controlled mainstream media. Online news site *Malaysiakini* is perhaps the most successful example still operating today; the site and its editors have won several awards internationally for their work

(Steele, 2009). The PAS-owned newspaper *Harakah*—affected by the PPPA—also went online in 1999 and became popular. In the years that followed, blogs became a force to be reckoned with in the Malaysian internet sphere. Sabri Zain's *Reformasi Diary* is considered important documentation from the streets during the Reformasi protests which followed Anwar's sacking, and was eventually compiled into a book (Nair, 2007). Another popular political blog was *Screenshots*, belonging to businessman and columnist Jeff Ooi, which went on to become so widely recognised that Ooi ran for a Parliamentary seat as part of DAP, and won with a significant majority in the 2008 general election.

Such was the impact of blogs on Malaysian politics that Gong (2011, p. 322) found that "running against a blogger (as opposed to a non-blogger) significantly reduces a candidate's odds of winning by 26 percent" and that political blogs played a role in setting the agenda for "social and political discourse" in the country (p. 314). The 'viral' effect that blogs had was immense, especially when it came to news that was not published, or played down, in the mainstream media. In fact, Ooi had started blogging as an "experiment" to "gauge how contagious [the] Internet can be if online content [is] crafted along current issues" (Tang, 2005, p. 7). In 2008, Mahathir Mohamad, then a retired Prime Minister, started blogging because he felt the government-controlled media did not report his opinions during the term of his successor Abdullah Ahmad Badawi (Hounshell, 2008).

That same year, when Barisan Nasional was denied its two-thirds majority in Parliament for the first time since 1969, the use of text messaging and blogs was credited for the damage caused by the opposition parties (Hah, 2012; Liow, 2012; Suffian, 2010). Likewise, the following general election, which saw the BN lose the

popular vote for the first time in its history (although they maintained the majority of seats in Parliament), was dubbed the 'social media elections' not just by scholars but also the then-Prime Minister Najib (Mohd Azizuddin, 2014; see also Nurul Huda, 2014; Tapsell, 2013a). Scholars have noted how social media platforms empowered and connected opposition voices and activists, and helped social movements gather momentum, matching global trends of the past decade (Postill, 2014).

Among the groups that have run successful campaigns on social media are the more partisan Asalkan Bukan UMNO [Anyone But UMNO], and others that claim to be non-partisan such as the Bar Council and Loyar Buruk. The latter two groups are not affiliated to any political parties, but the campaigns they organised are consistent with some of the pro-democratic values of the opposition parties. For example, the Bar Council—the legal body that regulates the profession of lawyers—ran the *Perlembagaanku* (MyConstitution) campaign[12] aimed at simplifying the Federal Constitution to Malaysians. Loyar Buruk, on the other hand, was behind *UndiMsia*! [Vote Malaysia][13], a campaign created to build communities of young people mobilising their peers to vote[14].

While these aforementioned groups (and other like-minded individuals) are not always directly connected to the opposition, they are often united in mutual calls for justice and reform against an oppressive regime—Barisan Nasional. Then, there are movements like Bersih, which relied on social media to mobilise street protests.

[12] Available at https://www.facebook.com/pg/MyConstitution
[13] Available at https://www.undimsia.com/
[14] Ahead of the 14th General Election, 67% of the 3.8 million unregistered voters were between the age of 21 and 30.

4.4 Bersih 2.0 online and in the streets

One of the most successful social movements in Malaysia that contributed to Barisan Nasional's decline over the last 10 or more years is arguably the Bersih movement (see Chan, 2018, for an extended discussion on Bersih's impact in Malaysian politics). With Malaysia's mainstream media outlets being controlled by Barisan Nasional, groups like Bersih relied on blogs, online news sites and platforms such as Twitter and Facebook to mobilise supporters and spread their messages. Bersih specifically benefited from the emergence of new media technologies for both organisation and mobilisation (Pepinsky, 2013). Scholars have noted that Bersih's "embeddedness in social media" (Welsh, 2011, p. 2) allowed for a fostering of a sense of community, often across ethnic, religious and partisan differences, making up what Lim (2017, p. 221) calls "a nation that is a crisscrossing of multiple solidarities online". The movement eventually grew beyond the geographical borders of Malaysia; over the years, a "parallel movement" known as Global Bersih emerged, with rallies held in 85 cities across 35 different countries, organised via Facebook and Google Groups (Lee, 2014, p. 905).

Bersih was originally established in 2005 as the Joint Action Committee for Electoral Reform, made up of opposition political parties, civil society groups and non-governmental organisations. Following its official launch a year later, Bersih organised its first rally on November 10, 2007, mobilising thousands of Malaysians on the ground to rally for electoral reform, something that was reminiscent of the *Reformasi* (reformation) era in the late 1990s, when Anwar loyalists took to the streets to protest his dismissal and subsequent arrest (Postill, 2014). In 2008, the organisation dropped its partisan connections to opposition parties and figures,

changing its name to Bersih 2.0 (The Coalition for Clean and Fair Elections)[15]. However, its demands worked to the advantage of Barisan Nasional's opponents (Welsh, 2011) and Bersih continued to get strong political support over the years from the opposition parties. Bersih's demands included the cleaning up of the electoral roll, reforming the postal ballot process, use of indelible ink during elections, and a minimum of 21 days campaign period; it started out more reformist rather than radical in its political goals. Nonetheless, at the Bersih 4 rally in 2015, it added a call for the resignation of Najib, amid accusations the prime minister was guilty of corruption.

Bersih's reliance on internet technologies was a consequence of having to keep up with contemporary communication practices and to overcome obstacles imposed by the state and state-linked actors, such as the use of security and police laws to arrest leaders associated with Bersih and to declare the rallies illegal. The PPPA was also invoked to ban printed Bersih T-shirts ahead of rallies (Chan, 2018; Khoo, 2014). Barisan Nasional leaders also challenged the Bersih movement on the ground: the *Baju Merah* (Red Shirts)—described by Varkkey (2017, p. 210) as "UMNO's unofficial 'muscle"'—regularly organised counter-rallies in opposition of Bersih. Indeed, a booklet titled *Kebangkitan Baju Merah* [The Rise of the Red Shirts] was distributed at the 2015 UMNO General Assembly by the Department of Special Affairs (or JASA), under the purview of the Communications and Multimedia Ministry, which celebrated the Red Shirt rally, and vilified the Bersih movement. According to a news report, the book listed 14 resolutions, including "exhortations

[15] While the Coalition is officially known as Bersih 2.0, the movement is generally known to the public as just Bersih (Lee, 2014). In this thesis, I use both terms interchangeably.

to 'reject rude rallies like Bersih'; reject racial chauvinism akin to the DAP's; and to reinstate the abolished Internal Security Act" (Kumar, 2015).

In response to the success of Bersih's online approach, the government and authorities began to employ their own social media strategies. Barisan Nasional's official line was that the Bersih rallies were a threat to peace (Pepinsky, 2013). Echoing that sentiment, the Royal Malaysian Police adopted the use of social media platforms in retaliation; in 2011, they released selected videos online and encouraged citizens to report Bersih rally participants in response to accusations of police brutality (Postill, 2014). At the Bersih 3.0 *Duduk Bantah* (Sit-in) rally in 2012, the police released videos on Twitter showing alleged protestors engaging in unlawful activities. Bersih claimed that its website came under distributed denial-of-service (DDoS[16]) attacks in the days ahead of both its 2011 and 2012 rallies.

4.5 Taking back control of the 'opposition playground'

The response on the internet by the authorities to undermine Bersih is not surprising considering efforts by BN to reclaim control of the narrative it had lost due to the freedoms exercised by groups and citizens online. Over the course of the past few elections, it was becoming increasingly clear that the BN—used to being able to control information in the country for decades—was struggling with the online environment. Despite all that, Prime Minister Najib in 2011 committed himself to keeping Malaysia's promise of a free internet (Chooi, 2011) and had while in power organised gatherings such as tea parties to meet his online followers and engage more

[16] A DDoS attack occurs when programmes, or numerous bots, bombard a site server with requests to view the website from multiple locations, making it inaccessible. This is similar to an attack that was inflicted on whistleblowing website WikiLeaks in 2012.

closely with them (Hopkins, 2014). He remains an active user of Twitter and Facebook even after his defeat in 2018. The reality, however, painted a different picture, although Najib was not the first Prime Minister to have reneged on the promise for a free internet. Signs of internet control in Malaysia date back to the days of Mahathir Mohamad, despite his promise for a censorship-free internet when he launched the Multimedia Super Corridor. In 2003, *Malaysiakini* experienced the first of many incidents at the hands of the authorities when its office was raided and computers confiscated for allegedly publishing a letter that was deemed seditious (George, 2006). Since then, there have been several attempts by Barisan Nasional governments to increase control and regulate online activities and behaviours, including the threat of building an internet filtering system. Watchdog organisation Freedom House in 2011 noted that "it remains unclear whether it has been permanently abandoned", although the idea for the filtering system has been reportedly been shelved (Kelly & Cook, 2011, p. 232). That would not be the first time the BN government had made a U-turn on a policy statement; following backlash to a Home Ministry Secretary-general Mahmood Adam statement about including online content in the Printing Presses and Publications Act, then-Home Minister Hishamuddin Hussein downplayed it, stating that the idea was only at discussion stage (Wong, 2011). Not long after, the amendments were made to the aforementioned legislation.

Laws have also been created to control the broadcast media and the internet. The Communications and Multimedia Act 1998 has been used over the years to both threaten and literally suspend online publications, similar to their counterparts in the print media. In 2009, *Malaysiakini* was directed to remove clips deemed "provocative and offensive" by the Malaysian Communication and Multimedia Commission

(Gomez & Chan, 2010, p. 7). When the news outlet declined to do so, all of its staff members were subjected to a three-day investigation. Numerous websites, like how *Malaysia Today* experienced in 2008, have been blocked despite the no internet censorship point in the Bill of Guarantees. In 2016, the UK-based *Sarawak Report*—highly critical of Najib—was also blocked. This led the whistleblowing site to use online publishing platform Medium, which was subsequently blocked after refusing a request from the Commission to remove an article about Najib ("The Post Stays Up," 2016).

The above are examples of direct censorship by the Malaysian government, but the effects are much wider; threats of legal actions led to self-censorship not only within the media but also among individuals. While *Operasi Lalang* continues to haunt institutions, regular citizens do not have such a history to remind them of the potential consequences of speaking freely. To expand its control, the BN governments have targeted ordinary citizens for investigation and arrests over their comments and conversations on social media platforms and on chat apps such as Whatsapp (Johns & Cheong, 2019). Tapsell (2018) offers an example of how the repressive laws has resulted in social sanctioning to silence opposing views even among friends or colleagues; one user shocked members of his Whatsapp chat group by informing them that he was going to file a police report on materials shared in the group.

4.6 Barisan Nasional's pro-active information war

Critics of Barisan Nasional believe that there are other methods and devices for controlling the internet that were used by BN governments and which are not

publicly known. In its 2012 report on Malaysia, Freedom House suggests that the extent of the Malaysian government's efforts in surveillance is not clear, but there exist laws which allow them to carry such activities out, including the draconian security offences (Sosma) law, which allows for "the interception of communications without judicial order, at least in cases involving security offenses" (Kelly, Cook, & Truong, 2012, p. 362). News reports have also suggested, based on leaked information, that the Najib administration had paid for services from hackers in Europe servicing the Malaysian Anti-Corruption Agency, the Malaysian Intelligence Department and the Prime Minister's Office (Rozario, 2015).

At the very least, as the Bersih discussion above noted, the Royal Malaysian Police was monitoring social media activities. A former-Inspector General of Police had sent warnings out from his personal Twitter account while in that position and a Minister of Communications and Multimedia had threatened action against people who insulted the government (Kumar, 2016). The media had reported that the Police Cyber Investigation Response Centre had publicly alerted users on social media—mainly activists—that they were being monitored and warned users to be more careful with their activities online ("PM left red nosed by censorship protest," 2016).

Besides Bersih, other organisations too have accused the Barisan Nasional of DDoS attacks. During the 2011 Sarawak state election, *Malaysiakini* was hit by cyber-attacks on April 12. Its co-founder and chief editor Steven Gan believed that the attacks were linked to its reporting on the campaigning of the Sarawak elections ("Malaysian news portal crippled by cyberattacks," 2011). This alleged attack came three days after Britain-based *Sarawak Report*, which was then critical of now-retired Sarawak Chief Minister Abdul Taib Mahmud, suffered the same attacks ("Sarawak Report

suffers massive cyber attack," 2011). A few days later, on April 14, the online edition of PAS-owned *Harakah Daily* also claimed to have come under a DDoS attack ("Cyber attack on Harakahdaily; A message to readers.," 2011).

While no individual or organisation has taken responsibility for them, the timing and the nature of all three attacks have led to speculations that they were the work of the ruling party Barisan Nasional. The international organisation Committee to Protect Journalists released a statement stating that, "Malaysian authorities used to tout their commitment to a censorship-free Internet, but their silence over these cyber-attacks have been deafening" ("Ahead of election, cyber-attacks cripple online media," 2011, para. 3). Then there is also Barisan Nasional's mobilisation of cybertroopers, which is the focus of this thesis.

4.7 Enter the cybertroopers

Mentions of Malaysian cybertroopers in academic literature do not offer a particular definition or in-depth investigation into the phenomenon. In most instances, cybertroopers are presented as groups belonging to Barisan Nasional, although some scholars have argued that such groups exist on both sides of the political divide[17] (see Hopkins, 2014; Leong, 2015; Suffian, 2008; Tapsell, 2013a; Weiss, 2009; Willnat, Wong, Tamam, & Aw, 2013). However, only Barisan Nasional leaders have admitted to running operations involving cybertroopers, based on news reports and interviews conducted by researchers. Due to the covert nature of their activities, it is difficult to understand cybertroopers comprehensively. How cybertroopers are engaged, for

[17] I discuss further Barisan Nasional leaders accusing their opponents of also having teams of cybertroopers based on news reports in Chapter 5.

example, is not clear in the literature: some scholars refer to cybertroopers as paid agents (Hah, 2012; Hopkins, 2014; Tapsell, 2013a) while others argue that they are volunteers (Kasmani, Sabran, & Ramle, 2014; Lim, 2009; Mohd Azizuddin, 2014), although there has been no discussion on whether volunteers can be paid. Some simply refer to them as either having been "recruited" (Suffian, 2010) or "trained" (Ufen, 2015). That said, it is possible to generalise some of these to craft a typology of Barisan Nasional cybertrooping activities into three broad categories:

4.7.1 *Monitoring and defence*

Most of the earlier literature notes that the cybertrooper's role was to counter pro-opposition messages on the internet. In some instances, a distinction was made between the role of 'volunteers' from UMNO (the dominant party in Barisan Nasional) who scoured and countered what they considered to be rumours and misinformation, while Gerakan (a BN-component party) had teams tracking blogs specifically (Lim, 2009; Weiss, 2009). Both teams are believed to be monitoring online sentiments. Specifically, Mohamed et al. (2011, p. 19) note the defensive role of BN cybertroopers "to fend off attacks and respond to political attacks". However, they also refer to the actions of cybertroopers as "virtual space harassment", indicating a shift to a more pro-active approach (p. 18).

4.7.2 *Balance*

Some of the studies found that cybertroopers were used to balance the sentiments on the internet, which had been dominated by pro-opposition voices. Ding et al. (2013)

refer to cybertroopers as units set up to manage UMNO's image on the internet, while Liu (2014) argues that one of their roles were to counterbalance opposition forces. Badrul Azmier, Mohammad Agus, and Zaliha (2014, p. 110) also describe the role of cybertroopers to balance "the temperature which has been favourable to the opposition". Nevertheless, they also point out that cybertroopers had been "adopting provocative-style writing and communication which were in contrast to the friendly image of leaders" (p. 109).

4.7.3 *Content creation/Attacks*

The general consensus among scholars is that Barisan Nasional cybertroopers exist as part of information warfare (Leong, 2015; Nurul Huda, 2014; Zakaria, 2011). These attacks may take the form of content generation (Muhamad, 2015) and publication of materials (Liu, 2014), which Tapsell (2013a, p. 45) believes exist to "slander" their opponents. Linking it to other known pro-Barisan Nasional groups, Azlan (2018, p. 24) argues that where the "Red Shirts disrupted Bersih's performativity in the material public space, cybertroopers were disrupting protest exchanges on Twitter".

This typology of the roles of cybertroopers shows a chronological shift in Barisan Nasional cybertrooping activities. It began with a defensive approach, followed by attempts at creating balance in the narrative, and finally a more aggressive approach. However, it is unclear if these are strategic shifts or just a form of evolution of behaviour, in line with how patterns of communication have changed on the internet.

4.8 Conclusion

The discussions in this chapter are important because they set the scene and provide a useful context to the data analysed in Chapters 5 to 8. An understanding of the political affiliations of the various parties, for example, will be useful to follow the discussion of news reports related to cybertrooping in Chapter 6. It also illustrates the multi-pronged approach that Barisan Nasional takes to achieve its political goals, relying on both online and offline techniques. The discussion on Bersih, and the attempts to challenge it by state-linked actors, provides the necessary foundation for the analysis of the two Bersih rally-related dataset of tweets.

This chapter has provided a historical and contextual overview of Malaysian politics and the illiberal efforts by the former ruling coalition at controlling the media and suppressing dissent. It described how internet technologies have helped the opposition parties, civil society groups and the public to overcome these government-imposed obstacles. The chapter also showed the ways in which the Barisan Nasional governments adopted strategies using social media to counter their opponents. One of the ways they do this is through the use of cybertroopers, the subject of analysis in the next four chapters of this thesis.

CHAPTER 5

How cybertroopers are reported in the media: An analysis

Early use of the term 'cybertroopers', used in the political context, can be traced back to Malaysia. Both English and Malay[1] language newspapers in the country mentioned the term as early as 2004[2], before the emergence of platforms currently referred to as social media. In three articles published in the *New Straits Times* that year, 'cybertroopers' was not used to describe a particular practice but instead was attributed to a specific group of people engaged in a "cyber war" against "the Opposition" (News Straits Times 25 February 2004; 19 March 2004; 1 October 2004).

This chapter will develop an analysis that is focussed on a dataset of 403 news reports published in Malaysia and Singapore—from both print publications and online news portals—to look at how cybertroopers (and the practice of cybertrooping) has historically been presented to the public. The analysis in this chapter considers these reports in terms of two main functions. First, they reflect the representation of the cybertrooper groups and their operations by media practitioners. Secondly, they provide access to descriptions and quotes by political leaders discussing cybertroopers. With that understanding of these two functions,

[1] It is important to note that in many cases, the term "cybertrooper" (or a permutation of that term) was used within a direct quote attributed to a source. I make this distinction to eliminate doubt that the term was used by reporters descriptively (although this was the case in the earlier news reports). This is a significant observation to eliminate any doubt that where interviews were conducted in Bahasa Melayu, articles written in English did not simply use "cybertrooper" as a translated term. In fact, even some Malay language newspapers used the term in inverted commas suggesting that there is not an acceptable or common alternative in that language. It is only when referring to the Red Bean Army (to be discussed later in this chapter) that most of the Malay language articles use the term "*pasukan tentera siber*" [cyber army].

[2] This is based on not just the earliest articles in my dataset but also on searches conducted on databases such as Nexis. Scholarly literature has suggested that cybertroopers were likely to have been part of UMNO strategy as far back as 1999 (Hah, 2016).

this chapter has three general aims. First, it provides the historical and evolving understanding of the Malaysian use of the term cybertroopers. The chapter also discusses the extent to which the news reports can be considered documented evidence for the existence of these groups and their practices. This discussion is important because not all of the quotes and media representations can be taken at face value due to issues of ownership and legislation of the media[3]. Instead, these issues of media control can provide a sense of the spin that Barisan Nasional engages in; in certain instances, some of the remarks from politicians appear to be more revealing than intended, especially where there is no clear advantage to the party or coalition in the admission. Finally, this chapter will also provide a background to public claims made by political leaders in Malaysia about their relationship with cybertroopers, allowing it to be used as a means to test the datasets that will be discussed in Chapters 6 to 8.

5.1 UMNO, Barisan Nasional and the 'original' cybertroopers

Discussions about the origins of cybertroopers begin with the United Malays National Organisation (UMNO), the largest and most influential component party in Barisan Nasional (BN). The party has not just been the one most commonly associated with cybertroopers in Malaysia, but its leaders have consistently—in news reports owned by the party no less—admitted to operate or train such teams as part of their online strategies. For example, former UMNO Youth Secretary-general Abdul Rahman Dahlan confirmed the existence of the party's cybertroopers dating

[3] Most of the major news outlets in Malaysia are owned by parties within Barisan Nasional (for example, the *New Straits Times*, *Berita Harian* and *Utusan Malaysia* are owned by UMNO, while *The Star* is owned by MCA), and as such, the party mechanism would pay close attention to how they are reported on and portrayed.

back to at least 2003, in an article reporting on UMNO's online preparations ahead of the 12th General Election (New Straits Times 17 February 2008). More specifically, UMNO Youth and Puteri UMNO—the party's youth wings for men and women respectively—have been reported as having been responsible for cybertroopers, at least in the early days. The first three articles in the dataset, dating back to 2004, noted that cybertroopers were made up of members from the two wings, alongside "cyber activists". This is consistent with later accounts in the news: in 2012, Puteri UMNO chief Rosnah Abdul Rashid Shirlin described its formation of "Cyber Troopers"—which includes 532 trained bloggers—as an example of the wing's effort in helping the party address its technological needs (Utusan Malaysia 10 May 2012).

> *"Pergerakan ini telah menubuhkan Cyber Troopers yang mana pasukan ini bukan sahaja dilatih bertahan daripada serangan pembangkang tetapi dajar teknik menyerang pembangkang."*
>
> [Our movement has created a Cyber Troopers team where members are not just trained to defend the party from opposition attacks but also taught the techniques to attack them.]

It is not clear why Rosnah would choose to divulge this information, considering the negative perception of cybertroopers. It is likely that her intentions were just to play up the role of the wing in UMNO in a question-and-answer style article focusing on Puteri UMNO's contribution to the party. However, the quote does not just confirm UMNO's mobilisation of cybertroopers but suggests that cybertrooping activity is akin to top-down astroturfing practices. It also contradicts other claims by party leaders that UMNO cybertroopers merely take on a defensive role against alleged lies and slander from the opposition. Cybertroopers were reportedly trained in "writing

the truth" and provided with facts needed to defend Barisan against "rumours" (New Straits Times 19 March 2004), including "informational bullets[4] with which to use as ammunition against anti-establishment forces" (The Edge 25 February 2008). Then-UMNO and BN Youth chief Khairy Jamaluddin reportedly said in a different report that his new BN Youth Cyber Team would be provided with "enough facts and information in response to whatever issues or questions raised by the Opposition" (The Malay Mail 9 August 2012).

Although it isn't clear if they genuinely believe this to be true or that these claims are a product of spin, these descriptions show that party leaders are willing to present cybertroopers as part of the party's communications mechanism. In addition, the descriptions are consistent across numerous news reports. In a different article, UMNO Youth's former Executive Secretary Shahrul Zaman reportedly likened the top-down structure to multi-level networking:

> Shahrul Zaman says the number of cybertroopers is confidential but reveals that they are organised in a similar fashion to multi level networks, with team leaders and down lines. (The Edge 25 February 2008)

Where the quote does not correspond with other news reports is Shahrul Zaman's secrecy on the numbers of cybertroopers. Aside from Rosnah revealing the number of trained cybertroopers in Puteri UMNO, there have been several media reports about the size of BN-linked cybertrooper teams. For example, a group of Barisan Nasional supporters calling themselves Perak[5] Cyber Troopers claimed to have built up a team of 220 members since it was founded in 2008 (New Sunday Times 20 May

[4] This is important to note because the Daily Deployment Strategy emails from Beruang Biru which will be analysed in the next three chapters include content which can be considered informational bullets.
[5] Perak is one of 13 states in Malaysia and was, in 2012, run by a BN state government.

2012). While this claim did not come from an UMNO leader specifically, the news report was about the group's launch event being officiated by Perak Chief Minister Dr Zambry Abdul Kadir, which can effectively be considered an endorsement by the party. In this case, the report was not about a group's contributions to the party like in Rosnah's case but instead more focussed on the existence of cybertroopers specifically. Having a launch event is public relations in practice, likely organised in an attempt to 'flex their muscles' in a show of strength. In a different article ahead of the 13th General Election, former Deputy Minister Saifuddin Abdullah placed the number of cybertroopers in Barisan Nasional at 10,000 (The Edge Financial Daily 12 November 2012). Similarly, it is also unclear if Saifuddin's numbers specifically includes groups belonging to other component parties in the coalition; UMNO is not the only party within Barisan Nasional that has admitted to having teams of cybertroopers. Leaders from major parties like Malaysian Indian Congress and regional parties such as Parti Rakyat Sarawak (Sarawak Peoples' Party) and Sarawak United People's Party have reportedly spoken about their respective teams of cybertroopers (The Star 6 February 2010; 22 March 2012; 4 July 2012). Nonetheless, the contradictions between claims about the size of teams and Shahrul Zaman's note on confidentiality suggest that those numbers cannot be accepted at face value. As products of PR exercises and spin, the sizes claimed could have been inflated to play up their ability to take on the opposition.

Aside from the links to the youth wings of UMNO, the early articles from 2004 also mention that not all cybertroopers are members of the party. The implicit suggestion is that the "cyber activists" who are not part of UMNO Youth or Puteri UMNO are all supporters of the party. At the times when it is explicitly addressed in the reports, cybertroopers are often described as volunteers or supporters of the party (Sunday

Star 9 June 2013; The Edge 25 February 2008; The Edge Financial Daily 12 November 2012). What is unclear from the news reports is whether or not cybertroopers work[6] (or 'volunteer') for the party or individual leaders within the parties, or both. Saifuddin Abdullah claims that both instances exist within his former party UMNO (S. Abdullah, personal communication, July 14, 2018). This could be one reason why news reports in the dataset feature party leaders lamenting factional fighting among cybertroopers, consistent with scholarly literature arguing that various teams attack each other internally within the party or coalition (Hah, 2016). One such person reportedly claiming as such is former deputy prime minister Ahmad Zahid Hamidi who said in an interview:

> But our cyber troopers are attacking each other when we should be attacking the opposition's cyber armies and become a shield for Umno. (New Straits Times 16 August 2015)

Other parties within Barisan Nasional have also raised the issue of factional fighting in media reports. Ong Tee Keat, the former president of the Malaysian Chinese Association (MCA)—one of the larger parties in Barisan Nasional—had reportedly complained about falling victim to "cyber-attacks" at the instruction of other leaders within his own party (New Straits Times 19 December 2013). He had previously claimed in the media that his successor Chua Soi Lek had formed a team of cybertroopers (Sinar Harian 22 February 2011). It is not possible, however, to tell if these accusations reflect the reality within the party or if they are being used merely to attack opponents, in the same way Barisan Nasional and their opponents accuse

[6] Scholarly literature is mixed as to whether or not cybertroopers are paid agents, as mentioned in Chapter 2.

each other of bad cybertrooping practices[7]. Given the indiscrete admission of internal competition, it is possible that teams' show of strength—for example, size of teams or extent of training—is not just directed at the opposition parties but also within the coalition or respective parties in Barisan Nasional.

The infighting may also explain why there were accusations in news reports of BN and UMNO leaders calling out their own party's cybertroopers, accusing them of unsavoury practices. In 2012, Kadir Jasin, a close advisor to Mahathir Mohamed[8] who was then still with UMNO, described the behaviour of BN's cybertroopers as "crude and infantile" (Malaysia Business 16 August 2012). When Saifuddin Abdullah was still in UMNO, he had reportedly condemned the adversarial nature of cybertrooping (The Star 12 April 2013). Considering how the reputation of cybertroopers has deteriorated in the media, these condemnations could also be part of efforts to distance the party from these teams. After all, reports also include other attempts at dissociating certain practices from cybertrooping, such as Khairy Jamaluddin making the point of differentiating the formation of the BN Youth Cyber Team from cybertroopers (Financial Daily 9 August 2012). The distinction Khairy made was that cybertroopers were involved in a "head-to-head war" against the opposition, while the Youth Cyber Team is a centralised group aimed at spreading pro-government information and countering the attacks from the opposition. Considering that the latter is how his fellow BN-leaders have previously described their respective cybertroopers to the media, the distinction Khairy makes is

[7] The dataset shows that DAP was the first to associate UMNO cybertroopers with bad practices. That UMNO had previously admitted to having teams of cybertroopers perhaps made them an easy target for such attacks from the opposition. This is discussed in more depth in section 5.3.2 of this chapter.

[8] Kadir Jasin was Group Editor of *New Straits Times*, the UMNO-owned daily, from 1988 to 2000, during Mahathir's first tenure as Prime Minister of a BN government. At the 14th General Election, Kadir publicly supported Pakatan Harapan and served as spokesperson for the new government's Council of Eminent Persons following the bloc's victory. He is also a Supreme Council member of Mahathir's new party Bersatu.

questionable at best. It is arguable that in practice, the BN Youth Cyber Team are cybertroopers by a different name. By using this convenient frame in the news reports, Khairy is able to distance Barisan Nasional from the activities and increasingly damaged image of its cybertroopers, portraying them as outliers. This is consistent with his attempts as dismissing what he refers to as "hardcore cybertroopers":

> Not all cybertroopers are under the payroll of political parties. As such, the opinion of a fanatic Barisan Nasional supporter should not be taken or viewed as the party's stance. (Khairy, as quoted in The Malay Mail, 14 February 2012)

One reason why Khairy might have taken this approach is because the party felt that it had lost control of their cybertroopers, particularly when we consider the admission of infighting discussed above. It would explain Saifuddin's frustration with their approach—that they are no longer able to be controlled centrally—and that of UMNO veteran Sanusi Junid who, following the 13th General Election, spoke to the media about the UMNO cybertroopers as young supporters of the party who were encountering obstacles at the division and branch level of the party[9], and thus, decided to act on their own (Utusan Malaysia 19 May 2013).

All of these criticisms and setting up of more official—or at the very least different—networks of cybertroopers appear to also include an element of spin, allowing the party to distance themselves from the negative perception of cybertrooping. This reframing of cybertroopers in the media was a convenient way to

[9] Divisions and branches of the party are a significant part of Malaysian politics. Leaders are usually voted up at each level, so the support of divisions and branches is important to a politician's ascent into high-level politics.

deal with the fact that they have been increasingly been demonised following the 12th and 13th general election in 2008 and 2013 respectively. This was when the opposition parties significantly affected BN's majority in Parliament, which scholars have partly attributed to the impact of the internet and social media (Mohd Azizuddin, 2014; Pepinsky, 2013; Weiss, 2012).

5.2 The Red Bean Army and the imagined cybertroopers

In 2013, the Democratic Action Party (DAP)—at that time, still an opposition party—was facing a barrage of accusations by its former members, Barisan Nasional leaders, non-governmental organisations, and the media, that it had spent 1.5 million Malaysian Ringgit (over £290,000) on a team of full-time cybertroopers called the Red Bean Army. The party vehemently denied through the media that it engaged in such practices, claiming that these allegations were a figment of Barisan Nasional leaders' imagination. Liew Chin Tong, the party's political education director, told *The Star*:

> They are funding their own Ikan Bilis Army or whatever, and they are using their own model to imagine that the other side runs on the same basis. We have no funding for such endeavours. (Liew, quoted in Sunday Star 9 June 2013)

Ikan Bilis is the Malay term for anchovies, and that statement was likely a sarcastic response to the accusations playing on the food reference in the term 'Red Bean'; there is no evidence of the existence of an Ikan Bilis Army. However, Liew's quote is noteworthy because of his claim that the accusations were formed on the basis that

the alleged Red Bean Army functions in the same way that Barisan Nasional cybertroopers do, as paid-agents covertly using social media to demonise their opponents. Not long after, DAP veteran Lim Kit Siang reportedly said, in his denial of the allegations, that it was part of a narrative created by UMNO cybertroopers to request more funding from their own party to take on a "fictitious Red Bean Army" (Malay Mail 3 July 2013). While Lim did not provide any evidence for his own accusation, the analysis of the news reports shows that there was almost an obsession among media outlets with DAP's alleged team of cybertroopers. Indeed, 80 of the 403 articles in the dataset mentioned the Red Bean Army were published by outlets owned by BN parties. This includes the 30 published in *Utusan Malaysia*[10] and over 20 in the *New Straits Times* (both UMNO-owned), and 10 articles in *The Star* (MCA-owned).

Reports of the Red Bean Army first emerged in the days ahead of the 13th General Election in May 2013. One news article took on a bizarre tone to warn readers about the dangers of the Red Bean Army, and included very specific descriptions attributed to unnamed "media analysts":

> Beware of the DAP-sponsored cyber troopers, known as the Red Bean Army, who are ready to wreak havoc in the cyberworld. The core group was said to comprise of between 2,000 and 3,000 members who could easily reach 60,000 people by sending out postings via social networks. The members were said to be employed full time with a salary of between RM3,000 and RM8,000 [per month, £590 and £1560] each and they have

[10] While *Utusan Malaysia* has discussed 'cybertroopers' using that term (there is no Malay equivalent), it only refers to the Red Bean Army as a cybertrooper team in one article. In all other instances, it refers to the group as "*tentera siber*" [cyber army]. However, all English-language articles in the dataset refer to the Red Bean Army as cybertroopers.

> been told to launch attacks on pro-government websites and social networks, spreading lies about the government and prevent any effort to connect with the people via the net.
>
> Media analysts said the group, which was formed between four to six years ago, were also directed to "kill off" pro-government comments in alternative media and disrupt programmes that lent credit to the government. (New Straits Times 2 May 2013)

A day later, reports published in different newspapers attributed accusations of the Red Bean Army's existence to two different former-DAP members. In the first instance, former DAP vice-Chairman Tunku Abdul Aziz Ibrahim[11] claimed that the Red Bean Army was responsible in the push for public participation in the Bersih 3: *Duduk Bantah* rally (New Straits Times 3 May 2013), while the other one quoted DAP's former Klang[12] youth chief Shen Yee Aun discussing the alleged cybertrooper group (The Star 3 May 2013). A different article published on the same day refers to the "widely reported" Red Bean Army, although these were the first sets of news articles referencing them in the dataset (however, blogs had previously referred to them).

In many of the reports, particularly in the English-language dailies, DAP leaders have been quoted denying direct association with the Red Bean Army. One of the most common defence was that they do not have access to the millions of Ringgit

[11] The article also mentioned that Tunku Aziz is against street rallies, and that his tenure as Senator—unelected positions in the Malaysian senate—was not renewed by DAP because of his public objections to street protests.
[12] A constituency in Malaysia.

allegedly funding these cybertroopers, as has been reported[13]. *Utusan Malaysia* had linked the funding of the Red Bean Army to a Taiwan-based Malaysian businessman (1 June 2013), who denied the allegations amid police investigations and threatened legal action against those who have linked him to the cybertroopers[14] (The Star 4 June 2013). This is not to say that DAP does not have a team working on their online campaigns. In the same news report quoted at the start of this section, DAP's Liew said that the party did not pay cybertroopers. Instead, he was quoted as saying that the party had "supporters (who come) forward as volunteers to help our online campaign. They are people who want to see change and voice out their opinions. They are using their own names and their own accounts, not fake accounts or names" (Sunday Star 9 June 2013).

Claims that the Red Bean Army is fictitious stand in contrast to findings in scholarly literature which suggests that DAP leaders acknowledge its existence. For instance, Tapsell (2013a, p. 46) noted that DAP social media officer Medaline Chang described the Red Bean Army as "angry Chinese young men who were active online, writing anti-government stuff on social media"[15]. Other media reports suggest a certain consistency in the party's messaging line with Chang's statement; member of Parliament Jeff Ooi discussing pro-DAP "cyber activists"—but not explicitly speaking about the Red Bean Army—was quoted as saying: "We don't discount the fact that there are some who speak on our behalf without our consent …"

[13] In an interview with a DAP leader conducted for this thesis, the lack of funding and resources was also cited as one of two reasons why the party had not developed cybertrooper-like networks. The other reason, the interviewee said, was due to "leadership disapproval". (Politician A, personal communication, July 27, 2018)

[14] There has been no indication of any lawsuits related to this in the dataset, suggesting that the accusations against him have died down following his threats.

[15] This description of "angry" young men is reminiscent of descriptions used to describe the 'cybernats', the people believed to be behind the abusive online activities of Scottish nationalist during the Scotland independence referendum. Macwhirter (2014, p. 18), in arguing that the cybernats are not members of any political party, described them as: "sad social misfits, sitting in their bedrooms getting a buzz from abusing public figures".

(Sunday Star 9 June 2013). The distinction that Liew was making in the above quote is perhaps more an issue of semantics; to the DAP leaders, cybertroopers are paid agents who engage in sockpuppetry. In this vein, the Red Bean Army are not DAP's cybertroopers because they are not on the party's payroll, and are a separate entity from the volunteers who are centrally mobilised.

Nonetheless, UMNO New Media Unit's head Tun Faisal challenged Liew's claim in the same article stating that DAP's alleged cybertroopers had to be paid—implicitly suggesting that the Red Bean Army reports to the party—because they react so quickly on the internet:

> "If these people are volunteers, they'd be like those in Barisan and UMNO – we cannot respond promptly because we don't sit in front of the computer 24/7. We have to do other work." (Sunday Star 9 June 2013)

Relying on the suggestion that teams can only be efficient if they are paid is perhaps not the strongest argument. In addition, this claim also contradicts the quote from Khairy Jamaluddin that alluded to the fact that some cybertroopers were on UMNO's payroll. In light of this, Tun Faisal's response is likely another use of spin to distance themselves from the negativity attached to the cybertrooping he is accusing the Red Bean Army of engaging in. To further his point, Liew also responded to Tun Faisal's accusation:

> Barisan (Nasional) simply does not understand participatory politics. They cannot conceive how people can voluntarily get involved in a participatory campaign. (Sunday Star 9 June 2013)

This statement returns to the claims of UMNO's limited imagination—allegedly in their own image—about how cybertroopers are mobilised.

It is worth noting that neither Tun Faisal nor anyone quoted in the 80 new reports that mentioned the Red Bean Army provided any evidence that directly linked the group to DAP. The closest mention was in one report that stated that a Red Bean Army page on Facebook existed, although its creator reportedly claimed that the name was merely a title for the page and that it did not represent any organisation. The report states that the creator Li Shuang spoke of the page[16] as a platform for political discourse and that the page "had never issued any comments to provoke racial hatred", responding to accusations that DAP's alleged Red Bean Army stoked racial flames among other things[17] (The Star 6 June 2013). Despite these denials, most of the BN-linked newspapers continued to report on them. In fact, only one article in the dataset said otherwise. Published in *The Edge*, one of the few newspapers not controlled by Barisan Nasional[18], columnist Kam Raslan echoed DAP stalwart Lim Kit Siang's description of the Red Bean Army as fiction. Although he offered no evidence, Kam made an unequivocal denial when he discussed attacks on social media aimed at a female DAP politician:

> When it became abundantly clear that nobody was falling for the false, clumsy and misogynistic smear attack, the response from *Utusan Malaysia* was that BN's bloggers had been 'trapped' into spreading the photo by the

[16] The article does not mention the URL of the page. A search on Facebook shows several such pages, but it is not possible to identify which is the one being referred to. It is also possible that the page has been deleted.

[17] As mentioned in Chapter 4, DAP is a multi-ethnic party but its predominantly Chinese membership base has been used as a rhetorical strategy against them. Politician A (personal communication, July 27, 2018) offered the example of accusations leading up to the 14th General Election that an ethnically-Chinese leader of DAP would become Prime Minister if Pakatan Harapan was to win, despite the fact that Mahathir had been announced as the Prime Minister candidate.

[18] This is the same newspaper that was later suspended by the Najib administration for running stories linking the Prime Minister to corruption.

> notorious 'Red Bean Army' (DAP's cybertroopers). Unfortunately, this argument is completely self-defeating because it uses the BN bloggers' own stupidity as their defence. And also, there's no such thing as the Red Bean Army. It's complete fiction; and it doesn't matter how many times the fiction is repeated, it's still a fiction. (The Edge 26 May 2014)

The point made by Kam above regarding the manner in which the alleged Red Bean Army is being used as a scapegoat, alongside the claim by Lim Kit Siang that the "fictitious" story is perpetuated to help BN cybertroopers demand for more funding, is worth further consideration. This is because efforts by those in power to identify and take action against RBA based on news reports have not been successful. This lack of action is unusual by Barisan Nasional standards; Najib has shown that he would arbitrarily use draconian laws to investigate and arrest those causing his regime problems. More significant is the fact that all of these complaints about the Red Bean Army were reported as having been brought to the attention of the higher levels in government. Based on one report, a group claiming to represent 130 non-governmental organisations had submitted a memorandum requesting a Royal Commission of Inquiry into the Red Bean Army and its funding source to then-Minister in the Prime Minister's Department, Shahidan Kassim, who then brought the issue up to the Cabinet (New Straits Times 3 July 2013). A Member of Parliament too had raised the issue, calling for a "special court" to address cybercrimes such as the Red Bean Army (The Sun 3 July 2013). In response to questions from MPs in Parliament asking about what kinds of police action will be taken, then-Deputy Prime Minister and Home Minister Zahid Hamidi responded stating that the alleged cybertroopers could face both criminal and civil charges (New Straits Times 11 July 2013). Prior to that, Zahid had accused the RBA of

disseminating content deemed seditious, threatening action. None of these have been reported to have been followed through based on dataset of news reports, which could indicate a couple of possibilities: first, that there is no any evidence to be used against DAP for action to be taken, or secondly, that Barisan Nasional was using these accusations as spin, and benefitting from keeping this story going.

5.3 The weaponisation of cybertroopers

Over the years, both the ruling and opposition parties[19] would exchange accusations in the media, blaming each other's cybertroopers for online attacks and engaging in bad practices. This would keep happening despite the fact that DAP and other then-opposition parties would deny having cybertroopers, while Barisan Nasional component parties would generally insist that their teams only existed to defend the party and counter lies. Both sides, in news reports, refer to volunteers or decentralised supporters who they are unable to manage. In the case of Barisan Nasional parties, so much control has been lost that teams within the same parties would take on each other, presumably targeting different factions.

The analysis of this dataset cannot confirm or deny with any certainty any of the allegations both sides are throwing at each other. However, they do provide some insight into possible ways in which cybertroopers can be used for political gain. The data allows for an interpretation of this weaponising of cybertroopers in two ways. First, the news reports include descriptions of some strategies and techniques adopted by cybertroopers. Some of these are more credible than others, but in

[19] While DAP was the opposition party that was mostly targeted, many of the news reports had generically referred to "opposition" or "Pakatan Rakyat" cybertroopers when discussing attacks on Barisan Nasional.

general, they can provide a sense of how cybertrooping is constructed as representation to contrast with the more direct empirical evidence in this study. Secondly, the analysis of the news report also allows for an inference about the way that the narrative of cybertroopers perpetuated by newspapers has been used by its owners—the political parties within Barisan Nasional—as a frame of attack to discredit their opponents.

5.3.1 *Instances of cybertrooping*

In 2007, political blogger Raja Petra Kamaruddin was investigated under sedition laws for comments allegedly condemning the King and Islam which were posted on his website, *Malaysia Today*. A report in *The Sun*, a newspaper not owned by any BN party, reported Raja Petra's statement to the police that accused UMNO cybertroopers[20] of leaving said comments to get him into trouble:

> These people are Umno "cybertroopers", there are about 25 of them paid RM2,750 each a month to raid and invade malaysia-today.net. They flood my website with about 500 to 600 unwanted and sensitive comments daily and I lose sleep every night cleaning this mess up by deleting them from my site. (Raja Petra, as quoted in The Sun 26 July 2007)

The case above touches on two aspects of cybertrooping. First, it identifies blogs[21] as a possible platform that cybertroopers may target. Since then, reports from the

[20] Describing the police questioning, Reja Petra wrote on his website that the 25 cybertroopers were working under the orders of UMNO supreme council members Azalina Othman and Norza Zakaria. Both of these people were associated with UMNO's youth wings that set up cybertrooper teams mentioned in the 2004 articles; Azalina was previously chief of Puteri UMNO while Norza was quoted in one of those articles talking about UMNO Youth's cybertroopers (New Straits Times 19 March 2004).

[21] It is worth noting that the incident described happened at a time when social media was in its infancy.

dataset have suggested that cybertroopers are found on various platforms including Facebook and Twitter, and more recently, turning to the chat apps such as WhatsApp[22]. Secondly, it suggests that one of the cybertrooping activities that takes place on these platforms is the posting of "sensitive comments". The Raja Petra claim raises the issue that these are not just comments aimed at challenging or disagreeing with him, pretending to engage in political discussions; his accusation is that these comments are planted specifically to get him into trouble. This is consistent with reports accusing cybertroopers of engaging in more than just trolling[23] or spouting abuse online. For example, DAP's Lim Guan Eng has accused Barisan Nasional cybertroopers of creating 'fake websites'—including one called *Lim Guan-Eng Blog*—which included posts that led him to being probed for sedition (The Star 26 January 2010). Not unlike Raja Petra's case above, the accusation here is that content—whether as a comment or a blog post—is posted to get someone in trouble with the authorities.

These allegations regarding fake sites can be understood alongside accusations of sockpuppetry—the creation of fake accounts—among BN cybertroopers. Even DAP's Liew Chin Tong had referenced this when he mentioned how his party's team of volunteers use their own names and accounts, implying that BN cybertroopers use fake accounts to engage in their activities (Sunday Star 9 June 2013).

[22] In his study on the role of smartphones at the most recent general election, Tapsell (2018) noted that WhatsApp was a crucial campaigning tool.

[23] DAP's Jeff Ooi had a rather considered approach about the roots for some of the actions by these "cyber activists". He reportedly told the Sunday Star (9 June 2013) that "all abusive, threatening, defamatory and utterly senseless comments online are extensions of the chatroom culture which was prevalent in the 1990s".

In the 2007 incident mentioned above, Raja Petra described the commenters on his website as cybertroopers masquerading "as Chinese (to) whack the Malays and Islam". In his *Malaysia Today* article, he continued:

> Then other cyber-troopers would respond and whack the Chinese. The Umno cyber-troopers are the ones behind this racial and religious bashing in Malaysia Today. Then they make a police report alleging that Malaysia Today insults Islam and stirs racial sentiments. (Malaysia Today 26 July 2007)

In the same way UMNO's Tun Faisal did not offer evidence to support his accusations related to the Red Bean Army, the likes of Raja Petra and the DAP leaders too did not offer proof in their accusations. Nonetheless, trends identifying strategies and tactics such as sockpuppetry are worth raising to be further developed in this thesis, considering the fact that Tun Faisal had admitted to the creation of fake Facebook accounts, as evidenced in scholarly literature (Hah, 2016).

The quote above from Raja Petra also highlights another trend that was evident from the dataset, that is the stoking of racial and religious issues. A year later, he would again raise this issue by claiming that Facebook administrators and cybertroopers from UMNO Youth's New Media Unit—which scholars note to be responsible for the mobilisation of cybertroopers (Hopkins, 2014)—were "attempting to poison the minds of young Malays and Muslims about the threat to the Malays and Islam" (Malaysia Today 11 January 2010).

The then-UMNO owned *Utusan Malaysia* also once called for the retention of the Internal Security Act that Prime Minister Najib had promised to repeal, citing racial tensions as one of the reasons:

> *Cukup jelas, dalam suasana sekarang—cybertroopers yang terang-terang tanpa rasa bersalah membangkitkan soal rasis, perkauman dan kaum masing-masing—ISA amat-amat diperlukan.* (Utusan Malaysia 29 July 2009)
>
> [It is clear that in the current climate—with cybertroopers blatantly playing up issues of race and ethnicity—that the ISA is much needed]

Considering the newspaper's tendency to stoke racial tensions among the Malays and non-Malays (Yang & Ishak, 2012), it is likely that they are referring to sentiments that challenge Malay superiority. Indeed, the newspaper had earlier that year also published a commentary piece that mentioned how cybertroopers are attacking bloggers who defend the 'Malay institution' (Utusan Malaysia 25 March 2009). As such, although the quote above does not identify whose cybertroopers they are accusing, it is arguable that the author was referring to those whose views do not represent the Malay nationalist party UMNO. It is not possible to tell whether or not the cybertroopers in question are genuine or if they are the sockpuppet accounts raising the issue of race as part of a masquerade, the way Raja Petra alleges. This can be said to be comparable to what George (2016) refers to as hate spin, that is, the manufacturing of mass righteous indignation against minorities. It would appear then that race and religion—a dominant discourse in Malaysian politics—are also themes that cybertroopers are believed to take advantage of and engage in.

5.3.2 *Framing cybertroopers as a means to discredit and distract*

Raja Petra's early allegations aside, it was only in 2009 onwards that news reports would start taking a negative tone in discussing cybertroopers. For example, the media has described cybertroopers as "mud-slingers" (New Straits Times 22 August 2009) and accused them of "spreading rumours" (Sinar Harian 20 September 2010). Reporters at *The Star* grouped them together in a list of what they called "internet bullies" including "cyberbullies, keyboard warriors, flamers, trolls, etc." (12 April 2013), and a columnist of that newspaper associated cybertroopers with "disinformation and propaganda" (The Star 5 June 2013). While the cause of this shift is not entirely clear, the gains that Pakatan Rakyat made against Barisan Nasional at the 12th General Election in 2008 likely played a part. Scholars have noted the role of communication technologies—SMS (Short Messaging Service) and blogs specifically—as having contributed to BN losing its two-third majority in Parliament for the first time in history (Lim, 2009; Liow, 2012; Ndoma & Tumin, 2011).

Interestingly, the dataset shows that it was not Barisan Nasional leaders who first started attacking opposition cybertroopers. In fact, news reports in 2010 showed that DAP leaders were the first to accuse the ruling coalition's cybertroopers of bad practices. However, it did not take long before the tables were turned, and it is possible that this reversal was amplified due to Barisan Nasional's ability to control the media narrative through its direct ownership and control of mainstream media publications. The same way that the existence of BN's cybertroopers can be accepted with certainty due to the numerous admissions by different political leaders, it is likely that attacks on cybertroopers (especially allegations of DAP's Red Bean Army)

were a deliberate attempt at using media framing and priming strategies to discredit the opposition. In 2012, MCA's Wee Ka Siong was reported in an UMNO-owned newspaper describing the job of opposition cybertroopers to "twist your words, put in their own words, pluck from here and there, out of context, and they start to attack you" (New Sunday Times 1 April 2012). This quote—effectively describing spin—is ironic considering that Barisan Nasional commonly adopts this form of propaganda technique, and that UMNO leaders have admitted in newspapers owned by their party that their cybertroopers were trained to attack the opposition. Another article also likened the Red Bean Army to terrorist groups like al-Qaeda and extremist Islamist group Jemaah Islamiah[24], arguing that the threat the cybertroopers pose is worse than that of the violent incursion that occurred in Lahad Datu in the state of Sabah involving 235 militants in February 2013 (Utusan Malaysia 1 May 2014).

Besides just being used to tarnish the opposition's reputation by describing the alleged cybertroopers in negative terms—consider the ways in which the Red Bean Army were described: a national threat, cause of racial tensions, seditious—newspapers also acted as a mouthpiece for third-party actors to demonise the RBA. The analysis of the 80 news reports referring to Red Bean Army in the dataset also showed a pattern with regards to complaints from non-governmental organisations[25]. In 2013 and 2014, the media discourse surrounding the Red Bean Army appear to have been aided by strong condemnations by non-governmental organisations, particularly through articles published in *Utusan Malaysia* and *New Straits Times*. For a

[24] The Jemaah Islamiah group is based in Southeast Asia, and is perhaps most notoriously remembered for the 2002 bombing in Bali, Indonesia.

[25] I have already discussed the mutually beneficial relationship that UMNO has with some pro-government groups such as the 'Red Shirts' in Chapter 4.

month between May and June 2013, *Utusan Malaysia* ran seven articles featuring at least 15 NGOs—each article mentioned two to three organisations—calling for action against the Red Bean Army. The next year, between March and April, 14 NGOs were featured in 11 news reports in the same newspaper. Generally, most of these articles were written based on a similar template. Around this same period, *New Straits Times* followed suit, with seven articles featuring a total of six different NGOs, one of which was headed by former PKR leader (3 May 2013). Attacks on the RBA by former opposition members is a particular trend in the *New Straits Times reports*; besides the aforementioned article, three others were published featuring former PKR members criticising the RBA (12 March 2014; 30 March 2014; 3 April 2014).

In one instance, *Utusan Malaysia* ran a series of reports focusing on one particular NGO that claimed to have submitted names of 800 members of the Red Bean Army to the Home Ministry for further investigation (3 April 2014; 4 April 2014; 12 April 2014). Its head Ramesh Rao Krishnan was quoted in one article stating that he had been told a special squad in the Royal Malaysian Police has been set up to investigate the group. However, just like the threats previously mentioned in regard to police investigations and Royal Commissions of Inquiry, nothing appears to have come out of these investigations. All of these reports were in addition to the ones mentioned earlier in this chapter covering the memorandum that the group of 130 NGOs had submitted calling for a Royal Commission of Inquiry that the minister had brought to Cabinet but was not followed up on. The lack of action from the government suggests that it did not consider the Red Bean Army as the big threat they were made out to be, or believe the group even existed. The media narrative however was useful in discrediting and demonising the political opponents of Barisan Nasional, particularly with regards to their online strategy that had been fêted as being superior.

Besides amplifying this narrative to discredit their foes, such multi-pronged attacks—using both offline and online media means, including third-party groups—can also be seen as a distraction strategy by Barisan Nasional, not unlike the 'dead cat strategy' discussed in Chapter 2. Malaysia has its own term often used in political circles to describe hidden hands and performative acts as a cover, or *wayang* (which means 'theatre'), a well-known version of which is the *wayang kulit* or shadow puppet performance.

This tactic could explain why attacks on the Red Bean Army—from politicians, the media and the NGOs—peaked on the two occasions when Barisan Nasional faced immense pressure from the public: first in 2013 following the 13th General Election, where Barisan Nasional formed government despite not winning the popular vote that led to accusations of electoral cheating and gerrymandering, and secondly, in 2014 when the Malaysian Airlines flight MH370 plane disappeared. In both instances, the media attacks died down within a couple of months, despite the issue having been investigated by the police, raised in Parliament and at a Cabinet meeting, and the aforementioned calls for a Royal Commission of Inquiry. It is worth noting again that the majority of news reports in question—over 50 out of 80 articles which mention the Red Bean Army—were published in *Utusan Malaysia* and the *New Straits Times*, both newspapers at that time owned by UMNO. That there were similarities in the structure of the articles reporting on the NGO complaints—not just within the same newspaper but across both papers—further suggests that Barisan Nasional, the NGOs and the media were possibly working together on an astroturfing-like campaign, not unlike some known cybertrooping activities.

5.4 The myth of the cybertroopers

In the months leading up to the 14th General Election in May 2018, the media ran a number of stories looking at the role that the new communication technologies—the internet, social media and artificial intelligence—would play during "the silly season" to quote one columnist (The Star 20 March 2018). Unlike the instances described earlier in this chapter, the rhetoric surrounding cybertroopers had become more muted. Direct attacks on the Red Bean Army, for instance, mostly ceased from 2015 onwards. Both sides of the political divide continued to criticise each other's cybertroopers—real or imagined—but there were significantly less attempts at calling out the parties for mobilising cybertroopers in the first place, at least by the standards seen in the news reports from the preceding years.

This could be attributed to several reasons. First of all, Barisan National—and UMNO specifically—have spent a number of years ahead of the elections managing accusations of corruption against Prime Minister Najib related to the state-owned investment corporation, 1Malaysia Development Corporation (1MDB). The extent of the accusations meant that the coalition was not merely fending off criticism online, which they could easily dismiss as the work of opposition cybertroopers. Instead, attacks were coming in from both online and print news sites (which led to the suspension of *The Edge*), both locally and internationally. So intense was the scrutiny that websites like *The Sarawak Report* and platforms such as Medium were banned. Investigations into the scandal were opened in countries such as the United States, Singapore and Switzerland (Case, 2017). The global scale of the corruption scandal meant that BN could no longer legitimately distract from the issue, something they possibly learned from the international coverage of the MH370 plane

disappearance when they focussed on the Red Bean Army, accusing them of the criticisms. Secondly, readership of newspapers in Malaysia has been on the decline and as such, the media could no longer play the significant role it did previously in affecting public opinion. Partially following global trends, and partially due to their partisan reporting[26], UMNO-owned newspapers such as *Utusan Malaysia* and *New Straits Time* experienced devastating loses in readership[27]. The third point relates to the 1MDB scandal which caused Najib's campaign funds to dry up (Saravanamuttu & Mohamad, 2019). If indeed the NGOs and third-party groups that were critical of the Red Bean Army were colluding with Barisan Nasional, the lack of funds would have affected their relationship.

A case could also be made for the way in which the political and public understanding of cybertroopers has evolved over the years. While the discourse in articles published between 2010 and early 2015 above have focused very much on discrediting the political parties behind the cybertroopers, the term appears to have been used more generally in the later years. In March 2015, for example, a police officer from the Counter Terrorism Division was quoted in both *The Star* and *New Straits Time* referring to the "thousands of cybertroopers" from the media division of the Islamic State of Iraq and Syria, the terrorist group most commonly referred to as ISIS (6 March 2015; 20 March 2015). While this framing of ISIS might come across as being no different from demonising one's political opponents, this example differs in two ways: first, it is not a direct political statement (in fact, the officer was

[26] There have been informal attempts over the years at getting people to stop purchasing newspapers in Malaysia in protest of their owners, including this petition: https://harismibrahim.wordpress.com/boycott-the-newspapers-online-petition/

[27] Audit Bureau of Circulation Malaysia numbers showed that *Utusan Malaysia*'s readership went from 181,365 in Jan 2012 to 107,609 in June 2018, while *New Straits Times*'s figures dropped from 100,383 in Jan 2012 to 32,064 in June 2018. http://abcm.org.my/wp-content/uploads/2013/08/abc-circulation-figures-jan-to-june-2018-print-newspaper.pdf

reportedly reaching out to Islamic scholars in Malaysia to help counter the ISIS ideology that was seeping into the country) and second, ISIS is not a political party in Malaysia.

In another example, a candidate from the Islamist party PAS, who was facing attacks online claiming that he was a Bangladeshi and not a Malaysian, described his experience with cybertroopers:

> Some of them (cybertroopers) are still targeting me with the same issue. When they post anything on Facebook, they tag me and keep on sending the same message. (Nurul Islam Mohamed Yusoff, as quoted in The Star 25 April 2018)

Granted, many articles which refer to cybertrooping still tend to frame them negatively as purveyors of slander and lies by the opposition, and Barisan Nasional continue to claim that their cybertroopers exist to defend themselves and counter rumours. This was certainly the case in the weeks ahead of the 14th General Election. However, responses like the quote above differ from the earlier news reports, in that those complaining about cybertrooper attacks seem to have accepted it as part of Malaysian political culture. Those quoted do not even name the political party they believe are attacking them anymore; many just dismiss the cybertrooping actions and focus on the issues. Mah Siew Kong, President of Gerakan, which was part of BN ahead of the 14th General Election, was quoted in one article referring to personal attacks he was receiving online: "It's just cybertroopers." (The Star 10 January 2018)

Another shift can be seen in the way the term has been adopted to refer to anyone who may be posting on social media negative comments, criticisms or differing

views. This is most clear when looking at published public contributions to newspapers; in a letter to the editor calling for the death penalty as a solution to corruption, one reader plainly wrote: "One of the favourite allegations among the cyber troopers is corruption" (The Star 31 January 2018). Another, a text message sent in to the newspaper and published, reads: "The CEP [Council of Eminent Persons] is doing a good job so far. Ignore the cyber troopers who purposely undermine all the council's efforts to streamline government agencies and objectives" (The Star 26 July 2018). It would appear that any negative 'noise' on social media is the work of cybertroopers.

5.5 Conclusion

The news reports analysed in this chapter offered insights into the mainstream debates surrounding cybertroopers, some of which have not been previously discussed in scholarly literature. This includes discussions on the roots of the terminology, the accusations surrounding the crafting of the Red Bean Army narrative, and the demonisation of cybertroopers as a media frame. The way cybertroopers are perceived and have been reported over a 15-year period also allows for the subject of this thesis to be studied from three perspectives. First, cybertroopers can be understood in terms of specific teams—whether the self-named Perak Cyber Troopers or just general teams that BN has admitted to operating. This 'Big C' approach will allow for the inclusion of other similar groups that have emerged in the dataset, such as with the 2013 launch of the Sensible and Ethical Malaysian United Troopers, created to monitor social media for racial and religiously sensitive content (Sinar Harian, 22 July 2013). The second perspective

understands cybertroopers from a "small c" approach, referring to teams of cybertroopers that various actors have accused their opponents of having. This could include the "imagined" Red Bean Army, factional groups within the same party, or even the reference to ISIS. The final perspective requires a change of mode, thinking about the practices and activities of cybertroopers as acts of 'cybertrooping'. This is most consistent with the way in which cybertroopers have been reported in the later news articles, specifically focussing on the generic way people have chosen to refer to them—practices of attacks, intentionally undermining authority, disagreements and contentious post, or in the words of Gerakan president Mah, "just cybertroopers".

These latter two perspectives can be useful against which to test the other datasets presented in this thesis. The discussions on the use of propaganda, public relations and spin, for example, do not only imply Barisan Nasional's reliance on these tools as part of its communication strategy (part of the larger media system), but also flags up their use as part of the political parties' cybertrooping strategies (engaged by cybertroopers). The other more specific tactics identified, such as the use of sockpuppetry, the stoking of race and religious tensions, and the mobilisation of cybertroopers to attack opponents on various platforms, can also be used in the triangulation process alongside the other sets of data. Collectively, the discussions in this chapter are analytically useful to craft out an understanding of who these cybertroopers are and what kind of cybertrooping activities they engage in as this thesis moves forward into the next three chapters, which aim to analyse different sets of empirical data to address the research questions.

CHAPTER 6

Who the cybertroopers are: building a case

The aim of this chapter is to investigate instances of cybertrooping from the two primary datasets in this study. From this, some cybertroopers can be identified, allowing for assertions to be made about what they do, and who they represent or work for. It builds on the discussion in Chapter 5 by triangulating the findings from that chapter with the Beruang Biru emails and tweets related to the Bersih rallies. This process corroborates claims by Barisan Nasional leaders that they do indeed mobilise teams of cybertroopers. It finds no evidence within the datasets to suggest that the opposition engage in cybertrooping that mirror the activities of Barisan Nasional cybertroopers, if at all.

This chapter starts by testing—and confirming—the hypothesis that Beruang Biru is part of Barisan Nasional's communication operation. It then presents a discussion on why tasks instructed through the emails can be considered examples of cybertrooping, allowing for the case to be made that Beruang Biru's primary audience is cybertroopers. To strengthen that argument, this chapter identifies instances of cybertrooping within the two Twitter datasets that are similar to the tasks requested in the emails. This identification also allows for the construction of sample sets of cybertroopers, from which patterns of their activities can be further studied to understand better who they are and what they do. The chapter will then discuss the discovery of social bots and the role they play in relation to cybertrooping. The collective identification of cybertroopers' Twitter activities will help explain why other accounts that have emerged from similar patterns in the

analysis were not included in the sample sets. A short conclusion will then be presented to describe how the findings in this chapter will further inform the discussions in Chapters 7 and 8.

6.1 Beruang Biru's links to Barisan Nasional

The analysis of the Beruang Biru emails begins with the hypothesis that the mailing list is one of the ways Barisan Nasional—and by extension, the previous Najib Razak government—communicates with some members of its online team, including cybertroopers. This premise was formed based on the second email in the dataset Beruang Biru sent on 14 March 2012, which explained that the intention for the creation of the mailing list was to help the Barisan Nasional government win the 13th General Election. The email, written in English and presented in its entirety, reads:

> Warmest regards,
>
> As a Malaysian who wants the country to continue marching forward, we are looking to assist the government to win the coming 13th General Election. In this matter, we would like to request your kind cooperation to spread our articles and materials that will be emailed from time to time. Your assistance and consideration is highly appreciated.

There was no mention in the email of who the people behind Beruang Biru are, and none of the other emails within the dataset explicitly claim to represent the party. However, there were numerous indicators that support the hypothesis.

For one, Beruang Biru has access to information that would conventionally only be privy to those close to the coalition or the government. As an example, the email sent on 3 April 2013 asked recipients to tune in to the television to watch a speech that the Prime Minister was due to give later that morning. The subject line "*Pengumuman penting*" [Important announcement] indicates that the sender knew the significance of the speech; indeed, Prime Minister Najib announced the extremely important and long-anticipated dissolution of Parliament to trigger the 13th General Election.

There was also the email sent on 27 March 2013 listing 16 hashtags that Beruang Biru wanted its recipients to use for the purpose of record keeping. Some of these hashtags have been used by the official Barisan Nasional account that is verified by Twitter as authentic[1]. One example of such a tweet was posted on 1 March 2013, which used the #ManifestoBukanJanji [A Manifesto is Not a Promise] well in advance of the 27 March email listing the hashtag, as Figure 6.1 illustrates.

Figure 6.1: *A tweet from Barisan Nasional's official Twitter account using one of the 16 suggested hashtags listed in a Beruang Biru email. The blue tick next to the username indicates that it is a Twitter verified account.*

The list of known Beruang Biru recipients—identified from metadata from the earlier received emails in the dataset—offers another insight. Several of the Beruang Biru emails linked to blogs run by some of these recipients, either as a reference

[1] Twitter explains their verified accounts feature here: https://help.twitter.com/en/managing-your-account/about-twitter-verified-accounts

point for information, or a site to take guidance from. Among them are bloggers named in an organogram that was sent to me by a political commentator[2] (see Figure 6.2).

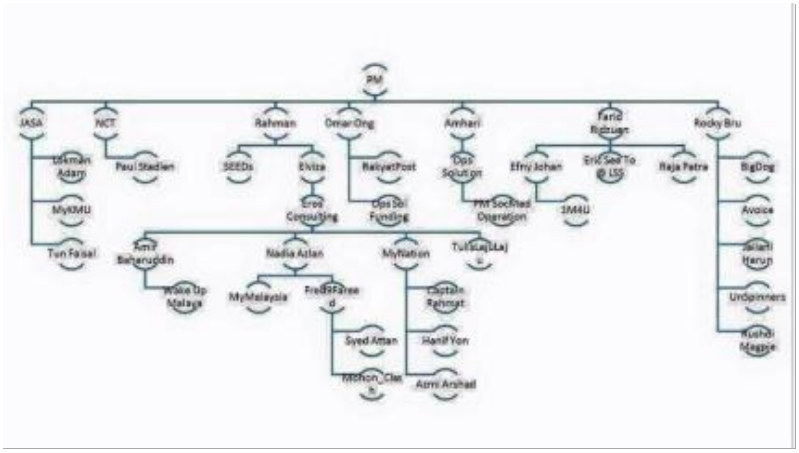


Figure 6.2: *The organogram of Prime Minister Najib Razak's alleged communications operations sent to me on condition of anonymity. It was sent to me via WhatsApp, hence the low-resolution quality of the image. See Appendix II for a version I recreated, with clear mention of names.*

While it was not possible to verify the authenticity of the chart, many of the names and organisations listed have been linked to Prime Minister Najib. Notably, one such organisation is JASA, the Special Affairs Department that published the booklet attacking the Bersih movement and celebrating the Red Shirts, mentioned in Chapter 4. Tun Faisal, who headed the previously discussed UMNO's New Media Unit,

[2] A journalist who I had also spoken to pointed out a discussion on a popular online forum in Malaysia that had published the same chart. In the post (https://forum.lowyat.net/topic/4334063/all), it was alleged that the organogram exposes the identity of Lim Sian See, the online commentator often critical of the DAP. The forum post includes screenshots from Facebook—which I was not able to verify the authenticity of—purportedly showing comments by Lim alleging that this chart is fake because he is named in it, and he claims to not have been paid by any parties. However, Lim's name is not listed except for the initials "LSS" under the name Eric See-To, who was then BN strategic communications deputy director. These comments have been used by forum members to argue that Lim Sian See is a pseudonym for See-To, which may suggest that the organogram is accurate. Interestingly, Lim Sian See's last public Facebook message as of July 2019 (https://www.facebook.com/lim.siansee/posts/2159827657569350) was posted a day after the 14th General Election when Barisan Nasional lost power, stating that he was taking a break after five years of "continuous postings".

and Paul Stadlen, Najib's media adviser and spin doctor, are also named in the organogram[3].

Emails in the dataset also indicate that among Beruang Biru recipients are communication specialists who handle the official social media accounts of both government and party leaders including Ministers, members of Parliaments and government officials. Some of the emails labelled Online Deployment Strategy explicitly remind these specialists that certain content should not be posted on "official accounts". One of the emails, sent on 19 April 2013, was particularly pointed: official accounts should "steer clear" (emphasis in original) from a particular topic. In others, instructions included specific requests to post particular topics on the accounts of Ministers and Deputy Ministers. These directions directly link the party and the state (and blurs the two) to Beruang Biru.

The specific instruction to avoid using certain content also implies that those managing the official accounts are not the primary target audience of these emails. It is likely then that the mailing list was intended to mobilise, by intimation, 'non-official' accounts. The email sent on the morning of 5 May 2013—the polling day of the 13th General Election in Malaysia—indicates that these people are considered members of Barisan Nasional's communication army.

> *Hi Team, Data semasa menunjukkan petanda SANGAT POSITIF kepada BN. Tahniah JENTERA BN - Kelantan, Kedah dan Selangor. Kerja kuat mendahulukan rakyat selama ini menampakkan hasil!*

[3] Raja Petra Kamarudin, who accused UMNO cybertroopers of leaving "sensitive comments" on his website, is also listed. That he possibly turned pro-UMNO as part of Najib's communication team might explain why there were reports that the opposition politician Anwar Ibrahim did not want to speak on the same panel as him at an event (to be discussed in Chapter 8).

> [Hi Team, Current data suggests an EXTREMELY POSITIVE signs towards BN. Congratulations BN ARMY - Kelantan, Kedah and Selangor. All the hard work of putting the public first is reaping rewards!]

The referencing of recipients as team members, and then as part of the "BN Army"—in this specific case those from Kelantan, Kedah and Selangor[4]—is similar to the language used by Barisan Nasional politicians discussing their online teams or cybertroopers. The term "war" was frequently used by Tun Faisal in an interview on radio station BFM talking about cybertrooping practices by the party, which he suggests dates back to 1999 (Tan, 2013). Kasmani, Sabran and Ramle (2014, p. 155) argued that Prime Minister Najib, in a speech in 2011, was referring to cybertroopers when he called on volunteers to be Barisan Nasional's "armies of the virtual world". In lamenting the fact that UMNO cybertroopers were fighting among themselves, then-Deputy Prime Minister Ahmad Zahid Hamidi said in 2015 that instead, they "should be attacking the opposition's cyber armies and become a shield for UMNO"[5] ("UMNO leader in bid to oust govt," 2015).

6.2 The force multiplication of Beruang Biru's talking points

Collectively, the indicators discussed above make the case for linking Beruang Biru to Barisan Nasional. While the final indicator only implies that the 'non-official'

[4] These three are states in Malaysia. It is not clear from the email if it refers to early indications of success in those states, or the "BN army" in those states.

[5] Existing scholarly literature on cybertrooping in Malaysia also uses military and war terminology regularly. Zakaria (2014) talks about how teams are being "outflanked" (p.55) in a "propaganda war" (p.59). Meanwhile, others refer to cybertroopers conducting "cyber-attacks and cyber-warfare" (Leong, 2015) and "cyberwar" (Tapsell, 2013a). The term "troopers" in itself is militaristic, although it is certainly not an analogy only used in Malaysia in discussions about 'information warfare'. Nonetheless, that these connections are being made is no surprise considering propaganda's link to war and the use of psychological operations strategies in the information war in various contexts, as discussed in Chapter 2.

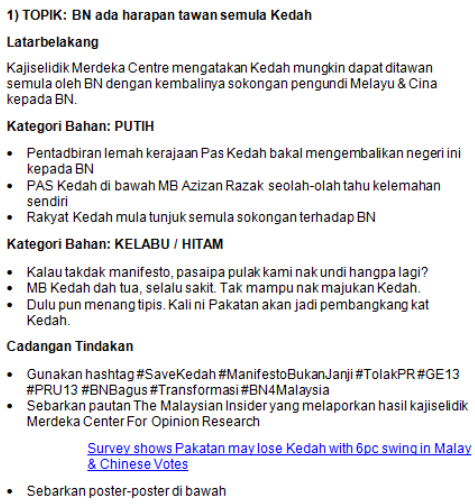
accounts that make up part of the "BN army" are cybertroopers, it is possible to argue that point through an examination of the content of the emails. While this inference is not explicitly mentioned, the analysis suggests that the activities tasked by Beruang Biru can be considered to be cybertrooping.

The instruction to spread "articles and material" in the 14 March 2012 email discussed earlier in this chapter in itself is reminiscent of known activities associated with the online manipulation of communication practices and information flow involving force multiplication of messages. From the dataset, there were 784 emails that had such articles and other materials for dissemination like videos and images, but did not include any direct communication or instructions from Beruang Biru. The content of the articles is varied and sourced from different outlets—most were from blogs and news media—but they were all favourable to Barisan Nasional, either directly, or through the demonisation of the coalition's opponents. The systematic seeding of such political material is classic propaganda at work, a technique often used in psychological operations (psyops) and in political communication.

Above and beyond the dissemination of those materials were the instructions for the propagation and amplification of pre-scripted message in the Online Deployment Strategy emails. On 22 February 2013, ahead of the 13th General Election, an email from Beruang Biru announced it would commence sending "Daily Online Deployment Strategy" directions to strengthen their "struggle" (*perjuangan*) against the opposition through "specific instructions" (*arahan khusus*). The email asked for the "cooperation" (*kerjasama*) of recipients to use "all" (*semua*) materials. Unlike the other instructional emails, a majority of the Online Deployment Strategy (ODS)

emails relate specifically to the general election, that is, going back to the initial purpose for setting up the mailing list as mentioned in the 14 March 2012 email.

The ODS emails mostly consist of several talking points for cybertroopers to focus on, with each "Topic" (*Topik*) generally categorised as "Background Information" (*Latarbelakang*), "Material" (*Bahan*), and "Suggested Actions" (*Cadangan Tindakan*). Figure 6.3 illustrates an example of how the template looks. Occasionally, there is a fourth section included, that is "Related Links" (*Pautan*) for dissemination.



1) TOPIK: BN ada harapan tawan semula Kedah

Latarbelakang

Kajiselidik Merdeka Centre mengatakan Kedah mungkin dapat ditawan semula oleh BN dengan kembalinya sokongan pengundi Melayu & Cina kepada BN.

Kategori Bahan: PUTIH

- Pentadbiran lemah kerajaan Pas Kedah bakal mengembalikan negeri ini kepada BN
- PAS Kedah di bawah MB Azizan Razak seolah-olah tahu kelemahan sendiri
- Rakyat Kedah mula tunjuk semula sokongan terhadap BN

Kategori Bahan: KELABU / HITAM

- Kalau takdak manifesto, pasaipa pulak kami nak undi hangpa lagi?
- MB Kedah dah tua, selalu sakit. Tak mampu nak majukan Kedah.
- Dulu pun menang tipis. Kali ni Pakatan akan jadi pembangkang kat Kedah.

Cadangan Tindakan

- Gunakan hashtag #SaveKedah #ManifestoBukanJanji #TolakPR #GE13 #PRU13 #BNBagus #Transformasi #BN4Malaysia
- Sebarkan pautan The Malaysian Insider yang melaporkan hasil kajiselidik Merdeka Center For Opinion Research

  Survey shows Pakatan may lose Kedah with 6pc swing in Malay & Chinese Votes

- Sebarkan poster-poster di bawah

Figure 6.3: *A screenshot featuring part of the Daily Online Deployment Strategy sent by Beruang Biru on 4 April 2013. The image shows the first of seven topics listed in that particular email.*

The "Material" section in most of the emails lists the scripted messages prepared by Beruang Biru. These talking points—a tool often used by spin-doctors—resemble the description of how cybertroopers operate offered by UMNO Youth's then-Executive Secretary Shahrul Zaman in a 2008 news report. Shahrul was quoted as saying that cybertroopers "are equipped with informational bullets with which to use

as ammunition against anti-establishment forces"[6] ("Net Value: Cyber Wars," 2008). This form of orchestrated mobilisation can be considered astroturfing.

The Online Deployment Strategy email sent on 10 April 2013 can be used as an example. The first topic for that day related to the *Ops Daulat* [Operation Sovereignty], the government's response to an insurgency in Lahad Datu, Sabah. Specifically, the instruction was to spread the word about how the situation in Sabah had "returned to normal" following the success of the operation to defeat the insurgents, ensuring that residents in the affected areas were safe once again. The "Material" category (*Kategori Bahan*) in the email, written in Malay, read:

> *Kategori Bahan: PUTIH*
>
> - *Sekolah-sekolah dibuka semula, kerajaan bantu bina semula rumah-rumah yang musnah di Lahad Datu.*
> - *Penubuhan ESSZONE memang untuk jamin keselamatan Sabah & Malaysia pada masa hadapan.*
> - *Rakyat di daerah-daerah terlibat Ops Daulat mula kembali semula ke rumah masing-masing.*
>
> [Material Category: WHITE
>
> - Schools have been reopened, the government is helping to rebuild houses destroyed in Lahad Datu.
> - Setting up the ESSZONE is to ensure safety for Sabah and Malaysia in the future.
> - Residents of the areas affected by Ops Daulat have started to return to their respective homes.]

[6] Note the strong military language used by Shahrul Zaman as well.

All three of the suggested texts above were within 140 characters, the limit for tweets, which suggests that they were crafted for use on Twitter. A search conducted on that platform using the three examples above as individual queries returned positive results for each.

Figure 6.4: *Example of tweets from a Beruang Biru scripted message appearing following a search on Twitter. The profile pictures and names have been blacked out.*

As an example, Figure 6.4 shows the search results for the first bullet point, which produced three tweets (as of 28 August 2018)[7]. The hashtags used in those tweets were listed in the email as "Suggested Action"—the list offered options such as #PeaceSabah #Pahlawanku #ESSZONE #LahadDatu #OpsDaulat—further confirming that those accounts identified from the Twitter search are likely among the 'non-official' accounts taking instructions from Beruang Biru. Results from the other two queries also showed a similar use of the hashtags. The seemingly random selection of hashtags from the list provided, and their inconsistent placement within the tweets, indicates that the accounts returned in the search were mobilised similarly

[7] None of the usernames from accounts that sent the tweets in this example matched the names and identities (where possibly known) of those who were CCed into the Beruang Biru emails. However, as mentioned in Chapter 3, investigations have shown that other sets of people have also received Beruang Biru emails. There is also the possibility that email addresses were placed in the BCC field, in the way that Beruang Biru eventually did with even my email address.

to the way Beruang Biru operates, as opposed to just Twitter users copying and pasting tweets they come across and agree with.

Alongside these talking points, many of the other activities tasked by Beruang Biru fit within the categories of dissemination and defence, demonisation and disruption, and distraction in the framework presented in Chapter 2, and can be tested against the information manipulation tools including propaganda, public relations, spin and psysops. These will be discussed more extensively in Chapters 7 and 8; however, the connection allows for the argument that 'non-official' accounts that are the primary recipients of the emails from Beruang Biru are Barisan Nasional cybertroopers.

6.3 Instances of cybertrooping on Twitter during the Bersih rallies

To further develop the discussions from the two sections above, this chapter now turns to the datasets of tweets collected during the Bersih 3.0: *Duduk Bantah* and Bersih 4 rallies respectively. Both Twitter datasets showed several patterns that emerged from the analysis of duplicate tweets (herein referred to as #bersih for the 2012 Bersih 3.0 rally and #bersih4 for the 2015 Bersih 4 rally) akin to astroturfing. In some cases, these findings were unique to a specific dataset, while in others, the instances of cybertrooping were similar in both datasets. The patterns identified and presented in this section all involve duplicate tweets, likely based on scripts similar to those discussed earlier from the Beruang Biru Online Deployment Strategy emails. Where the sets of tweets are identical—as opposed to those using varied hashtags or locating them differently within a tweet—I refer to these as *loops*.

6.3.1 *Describing loops created by pools of accounts*

This section turns to the official Barisan Nasional account on Twitter to explain the pattern of loops of messages being sent out by pools of accounts. Using Table 6.1 as an illustration, five of 14 loops identified in the #bersih4 dataset are presented, arranged according to the time the tweets were posted. The table shows loops of identical tweets sent by a pool of three accounts: the official @barisannasional account as well as two others (@FriendsOfBN1 and @BN_4Malaysia). It is not possible to definitively ascertain if the latter two accounts are run directly by Barisan Nasional as well, but there are indicators for that plausibility. For one, the content in the two accounts are pro-Barisan Nasional, with leaders like then-Deputy Prime Minister Zahid Hamidi following them both on Twitter (as of August 2018).

It is also clear from the 14 loops that these are not just two other random pro-BN accounts taking the lead from an official account. Indeed, there were occasions when some of the tweets were posted first by these accounts before the official @barisannasional account did the same, based on the timestamps (the first loop in Table 6.1). For example, the message[8] in the topmost loop in Table 6.1 was first tweeted out by @FriendsofBN1. It was only 23 minutes later that the official @BarisanNasional posted the exact same tweet. The 14 loops consisted of 46 tweets in total, which is notable because those three accounts were found to have collectively sent only 64 tweets in the full #bersih4 dataset. Four of those 64 were retweets from @FriendsOfBN1 and @BN_4Malaysia, but the source tweets were posted from within the pool of three accounts.

[8] Translation: #Bersih4: @KDNPUTRAJAYA [Home Ministry] requests that the public not attend or participate in the illegal assembly held on August 29 and 30.

Table 6.1

A sample of five of the 14 loops sent by three accounts linked to Barisan Nasional. In this example, I consider each set of three messages (as highlighted) sent by the three accounts as a loop.

Username	Date and Time	Tweet
friendsofBN1	2015-08-26 **T15:00:34**	#Bersih4: @KDNPUTRAJAYA meminta orang ramai supaya tidak hadir & menyertai perhimpunan haram pada 29 dan 30 Ogos ini
barisanasional	2015-08-26 **T15:23:50**	#Bersih4: @KDNPUTRAJAYA meminta orang ramai supaya tidak hadir & menyertai perhimpunan haram pada 29 dan 30 Ogos ini
BN_4Malaysia	2015-08-26 **T23:01:20**	#Bersih4: @KDNPUTRAJAYA meminta orang ramai supaya tidak hadir & menyertai perhimpunan haram pada 29 dan 30 Ogos ini
barisanasional	2015-08-27 **T14:47:29**	#Bersih4: @SKMM_MCMC memutuskan untuk menyekat laman-laman sesawang yang mempromosi, menyebarkan maklumat mengenai Bersih 4.0
BN_4Malaysia	2015-08-27 **T16:00:23**	#Bersih4: @SKMM_MCMC memutuskan untuk menyekat laman-laman sesawang yang mempromosi, menyebarkan maklumat mengenai Bersih 4.0
FriendsofBN1	2015-08-28 **T00:01:35**	#Bersih4: @SKMM_MCMC memutuskan untuk menyekat laman-laman sesawang yang mempromosi, menyebarkan maklumat mengenai Bersih 4.0
barisanasional	2015-08-25 **T11:52:38**	#Bersih4: Jika ada mahasiswa yang didapati terlibat, boleh dikenakan tindakan mengikut Akta Universiti Dan Kolej Universiti, (AUKU 1971)
BN_4Malaysia	2015-08-25 **T14:00:20**	#Bersih4: Jika ada mahasiswa yang didapati terlibat, boleh dikenakan tindakan mengikut Akta Universiti Dan Kolej Universiti, (AUKU 1971)
FriendsofBN1	2015-08-26 **T09:01:54**	#Bersih4: Jika ada mahasiswa yang didapati terlibat, boleh dikenakan tindakan mengikut Akta Universiti Dan Kolej Universiti, (AUKU 1971)
barisanasional	2015-09-04 **T10:56:20**	#Bersih4: Pekerja DBKL terpaksa bekerja 36 jam utk membersihkan longgokan sampah yg ditinggalkan peserta di ibu negara, hujung minggu lepas
BN_4Malaysia	2015-09-04 **T11:00:12**	#Bersih4: Pekerja DBKL terpaksa bekerja 36 jam utk membersihkan longgokan sampah yg ditinggalkan peserta di ibu negara, hujung minggu lepas
FriendsofBN1	2015-09-04 **T19:00:24**	#Bersih4: Pekerja DBKL terpaksa bekerja 36 jam utk membersihkan longgokan sampah yg ditinggalkan peserta di ibu negara, hujung minggu lepas
barisanasional	2015-08-27 **T16:44:17**	#Bersih4: Polis akan menggerakkan kira-kira 4,000 anggotanya bagi memastikan ketenteraman awam serta keselamatan rakyat
FriendsofBN1	2015-08-27 **T17:00:24**	#Bersih4: Polis akan menggerakkan kira-kira 4,000 anggotanya bagi memastikan ketenteraman awam serta keselamatan rakyat
BN_4Malaysia	2015-08-28 **T00:01:34**	#Bersih4: Polis akan menggerakkan kira-kira 4,000 anggotanya bagi memastikan ketenteraman awam serta keselamatan rakyat

6.3.2 *Grouping of cybertroopers by hashtags*

While the three accounts mentioned above are not considered to be cybertrooper accounts because they make their identity clear (such as in the username) and as such, do not operate covertly, that pattern of engagement identified in the previous section is mirrored among other pro-Barisan Nasional or pro-government accounts found in both datasets. For example, the #bersih4 dataset had at least 85 message loops sent from numerous pools of accounts, making up a total of 898 tweets. In some cases, these pools were formed around the use of hashtags in their messages. Many of these hashtags reflected the names of the different states in Malaysia (e.g. #nsdk for Negri Sembilan Darul Khusus; #PerlisMaju for Perlis—'*maju'* means progress; #prkdr for Perak Darul Ridzuan). As was the case with the pool of three accounts in Table 6.1, it is not possible to know definitively if accounts in a particular pool work independently of one another. Nonetheless, that they all can be divided into loops in itself shows that they all take similar approaches, whether or not they are taking instructions from the same authority figure.

In general, the text in the tweets used by the respective pools does not overlap across hashtags. This certainly could be coincidental but it is also possible that the different hashtags refer to different groups of cybertroopers, especially if they are mobilised state by state. Findings from the analysis of the news reports in Chapter 5 already indicate that different states—some of whom are governed by different political parties within the Barisan Nasional coalition operating from there—may have their own cybertrooper groups. Then there is also the possible calling out of three states specifically as part of the "BN army" earlier in this chapter. This is also reminiscent of discussion about cybertroopers run by different factions within the same party in

Barisan Nasional. At the very least, Beruang Biru's list of hashtags that is used for maintaining a record of cybertrooping activities shows that hashtags have a practical purpose when used by cybertroopers.

In some cases, the meanings for hashtags used by the various pools were indistinguishable as compared to the ones related to states in Malaysia, such as #KNEWS, #S14 and #C06. Searches on these hashtags conducted on Twitter found that the latter two[9] were still being used for pro-Barisan Nasional and anti-Pakatan Harapan messages in 2018. As there was nothing in these newer tweets to distinguish the meaning of the hashtag either, it is possible that they are code for record keeping or to distinguish groups of cybertroopers from each other, as has been previously argued. The tweets respectively using those three hashtags have one thing in common, however, and that is the use of another hashtag: #AgendaYahudi (Jewish agenda)[10]. This use of a common hashtag across the accounts means that while in some cases the scripts for each pool to tweet out may vary, they may still be following similar instructions.

6.3.3 *Loops which do not involve pools of accounts*

Loops were also found in the #bersih dataset but in smaller numbers. This is to be expected considering that the number of tweets in this dataset is significantly smaller than the #bersih4 dataset. The most obvious set that is similar to the loops described above involved a pool of five accounts, all of which sent three tweets each (15 tweets in total).

[9] In the case of #KNEWS, the Twitter search resulted in many tweets discussing contexts other than Malaysian politics in other countries around the world including South Korea and news sites in India.
[10] The trope of the "Jewish Agenda" in Malaysian politics will be discussed further in Chapter 8.

However, there were also other loops in the #bersih dataset that did not appear to have been sent by a particular pool of accounts. One example of these tweets involved the use of the #dearambiga hashtag, a reference to lawyer Ambiga Sreenevasan, who was at that point the chairperson of Bersih 2.0.

Table 6.2

A sample of the 28 tweets sent out using both the #dearambiga and #bersih hashtags.

Date and Time	Text in tweet
2012-04-28 **T10:31:16+01:00**	#dearambiga SPR has come up with brilliant booklet that can countered all allegations with facts, not like u n #bersih
2012-04-28 **T08:24:20+01:00**	#dearambiga SPR has come up with brilliant booklet that can countered all allegations with facts, not like u n #bersih
2012-04-28 **T08:13:47+01:00**	#dearambiga stadiums were ok for #bersih 2.0 but not good enough for bersih3? what r u trying to do?
2012-04-28 **T07:54:53+01:00**	#dearambiga stadiums were ok for #bersih 2.0 but not good enough for bersih3? what r u trying to do?
2012-04-28 **T08:08:33+01:00**	#dearambiga u must really love d limelight u r getting from d #bersih shenanigans. Dah dapat datuk some french award obviously u want mor
2012-04-28 **T07:41:04+01:00**	#dearambiga u must really love d limelight u r getting from d #bersih shenanigans. Dah dapat datuk some french award obviously u want mor
2012-04-28 **T09:10:32+01:00**	#dearambiga will truly be law breakers if she proceed with #bersih at dataran..pelik! she's ex bar council chairperson somemore!
2012-04-28 **T08:45:59+01:00**	#dearambiga will truly be law breakers if she proceed with #bersih at dataran..pelik! she's ex bar council chairperson somemore!
2012-04-28 **T07:45:27+01:00**	#dearambiga will truly be law breakers if she proceed with #bersih at dataran..pelik! she's ex bar council chairperson somemore!
2012-04-28 **T07:45:08+01:00**	#dearambiga will truly be law breakers if she proceed with #bersih at dataran..pelik! she's ex bar council chairperson somemore!
2012-04-28 **T09:14:15+01:00**	#dearambiga, look at ur generation, they r doing well for the next generation..maybe only u failed! #bersih is a failure!
2012-04-28 **T08:44:02+01:00**	#dearambiga, look at ur generation, they r doing well for the next generation..maybe only u failed! #bersih is a failure!

Table 6.2 shows just a few of the 40 different tweets messages sent out using the #dearambiga hashtag. Although it was possible to identify the 18 accounts that collectively sent all of the tweets, there were no patterns of specific pools of cybertroopers sending each individual message identified. While there were some indications of certain pools of users sending the same tweet, this was not consistent across the 40 tweets. This pattern is similar to another set of over 30 other loops posted from 24 accounts, also found in the #bersih dataset. What is notable, however, is there was a significant overlap in the accounts identified between these two sets; all but two of the 18 accounts using the #dearambiga hashtag were identified in the list of 24.

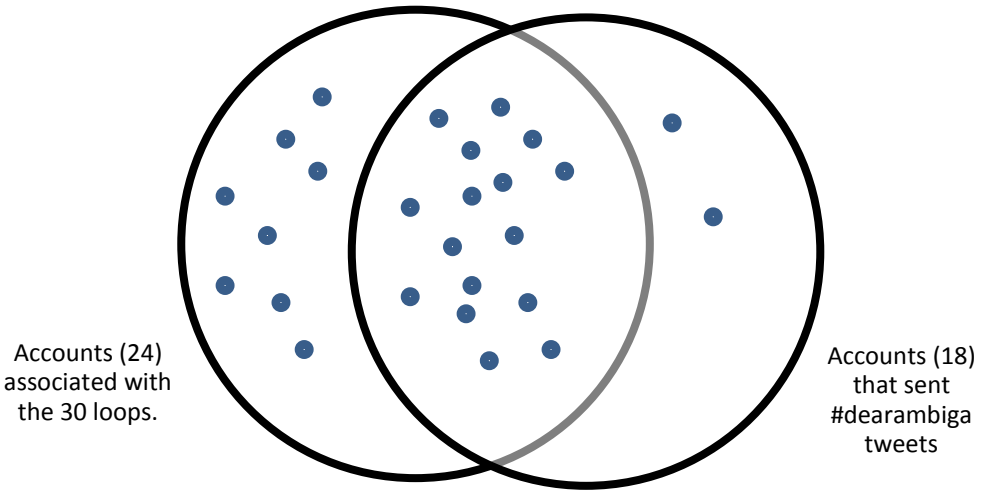


Figure 6.5: *A Venn diagram indicating the 16 similar accounts found from two different patterns of suspected cybertrooping activity. See Table 6.3 for the similar pattern of duplicate tweets sent by the 18 accounts mentioned above.*

The extent of the overlapping accounts suggests that both set of tweets are part of cybertrooping activity, and that at least 16 of these accounts can be considered to be cybertroopers.

6.3.4 *Duplicate messages through a specific messaging point*

Many of the accounts quantified above were also found to have engaged in another instance of cybertrooping. A total of 21 users—only seven accounts from which were not part of the above discussion—had posted a series of 137 duplicate tweets, all of which began with "joining #bersih means u …". There were 48 messages points in total with different reasons why "joining #bersih" was a bad idea. Each was found to consist of between two and four duplicates. Here are some examples of the tweets posted in English:

> joining #bersih means u accept #dearambiga as ur god! an anwar as ur apostle! .. dont join it!
>
> joining #bersih means u r a sinful person because god forbid people to break the law.. dont join it!
>
> joining #bersih means u r destroying the livelihood of hundreds commercial owners near dataran.. dont join it!

While all the other examples discussed in this chapter suggest that the duplicate tweets stem from scripted messages, it is this set of tweets that shows the clearest sign of that form of mobilisation happening. That all of these messages were scripted is evident by the fact that all the tweets used 'internet speak' (for example, "u", "r"), made the same punctuation errors ("dont join it" without the apostrophe) and consistently posted tweets in lower caps, even when it came to names of people (only abbreviations such CNN for the news network, PM for Prime Minister, and EC for Electoral Commission, were capitalised). Even in the two loops (consisting four tweets from four different accounts) where the they wrote "dont joint it" (instead of, "join", and with the same missing apostrophe in "dont") at the end of the tweets, it is highly unlikely that all four different accounts spelling it that way made the same error independently of each other. At the very least, it may be argued that these four

accounts are operated by the same person, alluding to the use of fake accounts—sockpuppetry—or automated bots.

6.3.5 *Clusters of users*

The 24 accounts mentioned earlier (which includes the #dearambiga tweets and the 30 other loops) are also linked to the "joining #bersih" tweets in that they were mostly sent from the same accounts. In total, 36 accounts were identified to have sent at least one duplicate tweet with the accounts within these sets. To illustrate this, Table 6.3—featuring just a random 10 of the 36 users as a sample—indicates when two users have sent the exact same tweets within the dataset.

Table 6.3

The coloured boxes indicate when two users have sent the same tweets from the #bersih dataset. Three main clusters—coloured red, purple and green—of users sending the same messages can be seen.

	Account 1	Account 2	Account 3	Account 4	Account 5	Account 6	Account 7	Account 8	Account 9	Account 10
Account 1										
Account 2										
Account 3										
Account 4										
Account 5										
Account 6										
Account 7										
Account 8										
Account 9										
Account 10										

Table 6.3 shows three clusters of accounts that have sent duplicate tweets: the first between Accounts 1 through 3, the second between Accounts 4, 5 and 10, and the third, with Accounts 7 through 9. These clusters do not represent loops, but instead reflect a series from a variety of duplicate tweets. Looking at the accounts from cluster one, one can see that Account 1 had sent the exact same tweet as only Account 7 from cluster three. Account 2 (first cluster) and Account 10 (second cluster) also had duplicate tweets. Due to the fact that others within the same cluster did not share duplicate tweets with those other clusters, loops are not formed by the pools of accounts.

6.3.6 *Identical messages from the same account*

Another pattern that emerged from the datasets were the loops of messages sent from the same account. This is worth unpacking further because Twitter in general does not allow the same account to post the same tweet twice. There are loopholes to overcome this restriction, and the datasets shows two ways in which this can occur. In the first way, account repeats the post at different times with other tweets sent out in between them. For example, one account was found to have sent seven duplicate tweets over a nine-hour period, with other tweets posted in between each of those. The second loophole involves changing the text of the tweets enough to get around Twitter's restriction. As Table 6.4 illustrates, using asterisks at the end of each tweet is sufficient, ensuring that the key message remains unaffected. Making such minor modifications to the tweet allows a user to send multiple tweets with the same message quickly.

Table 6.4

Example of tweets from a single account using asterisks to make each tweet appear unique. The timestamps indicate that each tweet was sent within seconds of each other.

Date and Time	Text in tweet
2015-08-30 **T13:59:30**	#Malaysia Selamat #Bersih4 #PerlisBoleh say no to bersih..stupid stupid fool*
2015-08-30 **T13:59:35**	#Malaysia Selamat #Bersih4 #PerlisBoleh say no to bersih..stupid stupid fool**
2015-08-30 **T13:59:48**	#Malaysia Selamat #Bersih4 #PerlisBoleh say no to bersih..stupid stupid fool***
2015-08-30 **T13:59:41**	#Malaysia Selamat #Bersih4 #PerlisBoleh say no to bersih..stupid stupid fool****

Besides using the asterisks, the dataset also showed some accounts using numbers at the end of each tweet, seemingly for the same purpose. There are also some tweets which tagged other accounts which alert different users to the same message. This approach serves two potential purposes; besides also allowing a user to post multiples of the same tweets in quick succession, tagging accounts of people likely sympathetic to one's 'cause' brings attention to one's tweet and increases the chance of it being retweeted. Table 6.5, for example, shows that Prime Minister Najib, other ministers and UMNO leaders like Tun Faisal were among those who were tagged in tweets sent by the same user.

The example in Table 6.5 also shows the same user using the same technique twice in the same day. The six tweets in the first half of the table were sent within seconds of each other, before the same pattern reoccurred just short of two hours later.

Table 6.5

Tweets sent by a user which shows how the account tags different usernames in the tweet to overcome Twitter's restriction on duplicate tweets. Again, the timestamps show that the tweets in each set were sent within seconds of each other.

Date and Time	Text in tweet
2015-09-01 **T07:11:10**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @Huan2U
2015-09-01 **T07:11:16**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @spk5447
2015-09-01 **T07:11:58**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @NajibRazak
2015-09-01 **T07:12:04**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @TengkuAdnanReal
2015-09-01 **T07:12:09**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @tunfaisal
2015-09-01 **T07:12:22**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @mpkotabelud
2015-09-01 **T07:12:34**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @azizanjang
2015-09-01 **T07:12:56**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @SoloRideJer
2015-09-01 **T08:51:17**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @Huan2U
2015-09-01 **T08:51:41**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @spk5447
2015-09-01 **T08:51:48**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @mpkotabelud
2015-09-01 **T08:52:11**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @SoloRideJer
2015-09-01 **T08:52:18**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @azizanjang
2015-09-01 **T08:52:24**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @TengkuAdnanReal
2015-09-01 **T08:52:29**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @NajibRazak
2015-09-01 **T08:52:46**	Some irresponsible people are behind this @Idris_Haron #Bersih4 http://t.co/embq2mLo6Q @tunfaisal

6.3.7 *Identical messages from similarly named accounts*

One other variation to the instances identified in the previous section is when identical messages are sent from different accounts bearing similar sounding names. One example of this was found in the #bersih4 dataset, which was initially identified as a loop. However, further investigation showed that the tweets were sent from several accounts that could likely have been sent by the same individual. Table 6.6 illustrates how 10 accounts created using different permutations of the name Shukri Ali—in most cases, using numbers to create the variation—had sent the exact same tweet.

Table 6.6

Example of tweets likely sent by the same individual who had created several accounts using numbers to create a variation in the username.

Username	Text in tweet
shukri_ali	#Bersih4 Puak-puak ini perlu ditentang habis-habisan sebelum negara menjadi lebih parah #AgendaYahudi #C06
ShkreeMuhali1	#Bersih4 Puak-puak ini perlu ditentang habis-habisan sebelum negara menjadi lebih parah #AgendaYahudi #C06
shukri8ali	#Bersih4 Puak-puak ini perlu ditentang habis-habisan sebelum negara menjadi lebih parah #AgendaYahudi #C06
shukri10ali	#Bersih4 Puak-puak ini perlu ditentang habis-habisan sebelum negara menjadi lebih parah #AgendaYahudi #C06
shukri44ali	#Bersih4 Puak-puak ini perlu ditentang habis-habisan sebelum negara menjadi lebih parah #AgendaYahudi #C06
shukri11ali	#Bersih4 Puak-puak ini perlu ditentang habis-habisan sebelum negara menjadi lebih parah #AgendaYahudi #C06
shukri12ali	#Bersih4 Puak-puak ini perlu ditentang habis-habisan sebelum negara menjadi lebih parah #AgendaYahudi #C06
shukri13ali	#Bersih4 Puak-puak ini perlu ditentang habis-habisan sebelum negara menjadi lebih parah #AgendaYahudi #C06
shukri14ali	#Bersih4 Puak-puak ini perlu ditentang habis-habisan sebelum negara menjadi lebih parah #AgendaYahudi #C06
shukri15ali	#Bersih4 Puak-puak ini perlu ditentang habis-habisan sebelum negara menjadi lebih parah #AgendaYahudi #C06

The hashtags #AgendaYahudi and #C06 used in the tweets displayed in Table 6.6 were also used by many other cybertrooper accounts, linking these Shukri Ali accounts to cybertrooping activities.

6.4 Human, cyborg and bot cybertrooper accounts

In the process of analysing the data presented in the previous section, there were signs within the #bersih4 dataset to suggest that some form of automation was being used for cybertrooping. Automated accounts on Twitter are often referred to as bots, but as discussed in Chapter 2, not all are fully automated and as such, may be cyborg accounts (Gorwa & Guilbeault, 2018). Although bots are now able to replicate a lot of the actions of human cybertroopers, this thesis does not attempt to distinguish them from one another for the purpose of analysing cybertrooping activities. I consider all three types of accounts—human, cyborg and bots—engaging in such activities to be cybertrooper accounts. Nonetheless, a discussion on bots is necessary because their behaviour can provide more insights into cybertrooping.

An analysis of the #bersih dataset showed little evidence that bots were being used in 2012. Using volume to gauge, only 993 of the primary tweets from the over 60,000 tweets (1.7%) collected were found to be duplicates by potential cybertroopers. In contrast, the percentage of duplicate tweets to unique tweets in 2015 had increased significantly as seen in the #bersih4 dataset, with over 20,000 (+/-10%) tweets identified as likely cybertrooping. This significant difference can be attributed to the increased use of automated bots, which had several characteristics that made them identifiable.

First, many of these accounts had suspicious-sounding usernames. To illustrate this, the tweet in Figure 6.6—which appears 13 times in the dataset—is used as an example.

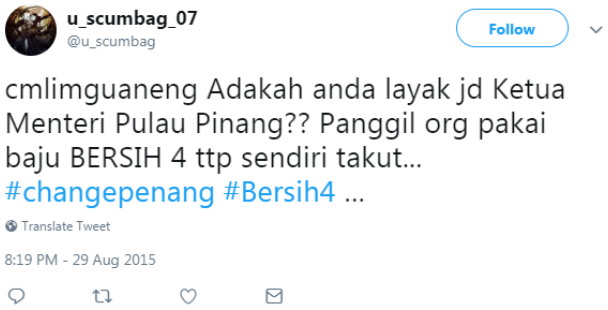


Figure 6.6: *Tweet from Bersih 4 dataset by user @u_scumbag. The name associated to the username is u_scumbag_07.*

Many of the accounts associated to this tweet in the dataset included "07" in the username such as @whyme2_07, @thinkb4talk__07, @thinkb4talk07 and @Piscean_J_07. A Twitter search on 31/5/2018 on the tweet showed other accounts not captured in the dataset (although, some of the accounts have appeared in the dataset tweeting other material), all of which have "07" in either the username or the name associated with the account. It is likely that these accounts are not human accounts because they all made a similar presumed error in the text of the tweet: the mention @cmlimguaneng (Twitter account of former Penang Chief Minister Lim Guan Eng) was missing the @ symbol, which means he did not get tagged into any of the tweets although the message is addressed to him directly. Translated, the message reads: "Are you qualified to be Chief Minister of Penang? You call for people to wear the BERSIH 4 T-shirt but you yourself are afraid…"

Considering the number of accounts that had sent this tweet, it is unlikely that not a single person had noticed this error if they were human operated[11].

Figure 6.7: Results of a Twitter search shows that all of the accounts associated with this tweet had used the number "07" in their names.

Another way bots can be identified is in the way that they were set up to retweet each other. While retweeting is common practice, and does not require bots, the dataset shows some suspicious retweeting patterns. For example, hundreds of tweets in the Bersih 4 dataset show that these accounts were not just retweeting each other but were seemingly caught in a constant cycle of retweets. I use the following tweet from @whyme2_07 to illustrate this.

[11] The tagging of an account using the '@ mention' is a basic and key feature of Twitter that would be known to any user of the platform. This is in contrast to the punctuation and grammatical errors in the previously discussed 'joining #bersih' tweets, where a grasp of the English language is necessary to identify the mistake.

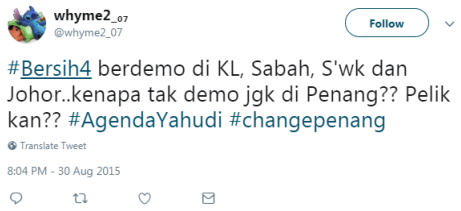


Figure 6.8: Screenshot of tweet from user @whyme2_07, which on its own, looks seemingly innocuous.

The account not only retweeted itself, but also retweeted three others who had sent the exact same tweet, as the following examples show:

> RT jacklim76_07: #Bersih4 berdemo di KL, Sabah, S'wk dan Johor..kenapa tak demo jgk di Penang?? Pelik kan?? #AgendaYahudi #changepenang
>
> RT actwisez: #Bersih4 berdemo di KL, Sabah, S'wk dan Johor..kenapa tak demo jgk di Penang?? Pelik kan?? #AgendaYahudi #changepenang #change…
>
> RT pinkroses69: #Bersih4 berdemo di KL, Sabah, S'wk dan Johor..kenapa tak demo jgk di Penang?? Pelik kan?? #AgendaYahudi #changepenang #cha…

Such behaviour is noticeable because retweeting oneself is not common Twitter practice. What is more, a human cybertrooper covertly operating their accounts manually will unlikely retweet numerous accounts with the same message, in order to not bring attention to themselves. It is likely that what has occurred here is that these bots are also automated to retweet accounts from a list of other bots, aside from just being configured to post 'unique' tweets. In doing so, these bots are inadvertently retweeting similar content leading to a chain of retweets to be formed, as another tweet by whyme2_07 below illustrates.

> #changepenang #changepenang RT SWR40: RT pinkroses69: RT pinkroses69: RT jacklim76_07: #changepenang #Bersih4 berdemo di KL, Sabah, S'wk da…

The above example also shows how the chain is not always linear as it is a retweet of @pinkroses69 retweeting itself. Patterns of a recursive and repetitive nature can be seen, such as when an account has retweeted itself and a previous chain of retweets, as can be seen from the example below.

> #changepenang RT whyme2_07: RT whyme2_07: #changepenang RT SWR40: RT pinkroses69: RT LimCaiHin: #changepenang #Bersih4 berdemo di KL, Sabah…

The example above shows another characteristic of the cybertrooping bots; they have been configured to add particular hashtags to retweets. It shows the hashtag #changepenang, which is one of those listed in Beruang Biru's email requesting they be used for record purposes, being added to retweets. It is likely that the hashtags appear several times because the bots are retweeting each other after they have added the hashtag on. However, there are also cases where hashtags keep getting added (perhaps a glitch) which causes the original messages to be truncated due to Twitter's character-count restrictions, as the following examples show based on this original tweet sent out by @whyme2_07:

> #bersih4 #changepenang Super Son hits hat-trick as S Korea rout Laos 8-0 http://t.co/iINV2IBLwN[12]

Below are other tweets the same account had sent out in multiples, first by retweeting itself and then incrementally by adding the #changepenang hashtag.

[12] This tweet does not appear to have anything to do with Malaysian politics but is used here just for illustration purposes. It is unclear why the account would have sent this tweet.

#changepenang RT whyme2_07: #bersih4 #changepenang Super Son hits hat-trick as S Korea rout Laos 8-0 http://t.co/iINV2IBLwN

#changepenang #changepenang RT whyme2_07: #bersih4 #changepenang Super Son hits hat-trick as S Korea rout Laos 8-0 http://t.co/iINV2IBLwN…

#changepenang #changepenang #changepenang #changepenang RT whyme2_07: #bersih4 #changepenang Super Son hits hat-trick as S Korea… … #change…

#changepenang #changepenang #changepenang #changepenang #changepenang RT whyme2_07: #bersih4 #changepenang Super Son hits hat-trick as S Ko…

#changepenang #changepenang #changepenang #changepenang #changepenang #changepenang RT whyme2_07: #bersih4 #changepenang Super Son hits hat…

The identification of these accounts in 2015 is notable because mainstream discussion on bots in the news only significantly emerged in Malaysia during the 14th General Election in 2018[13]. As recent as 2017, the report on Internet Freedom by Freedom House (Kelly et al., 2017) suggested that Malaysia only engaged in "Paid Pro-Government Commentators" in a table summarising the various manipulation strategies employed by political actors across the world. In a table found in the report, 20 countries were listed as having engaged in the use of political bots, but Malaysia was not included in it. This is further evidence of the richness of the datasets analysed for this thesis.

While bots are identified here in this section to make a distinction between the various types of accounts that engage in cybertrooping, it is worth noting—at least from a strategic perspective—that it does not matter if the activity is conducted by a

[13] On April 22 of that year, Reuters reported the Digital Forensic Research (DFR) Lab of the Washington-based Atlantic Council think tank in the United States' discovery of over 17,000 bots believed to have tweeted content related to the Malaysian election over a one-week period (Ananthalakshmi, 2018). The Lab found that most of the accounts focused on the propagation of two hashtags, #Kalahkanpakatan and #sayNOtoPH, and spread the word by tagging numerous accounts (some believed to be genuine and others, like the ones the tweets originated from, those of bots) in the tweets.

human, an automated programme, or a combination of both. This is because they end up effectively serving the same purpose: either the human or bot is given a set of instructions which they then proceed to carry out. For this reason, I consider all of the instances in this chapter as cybertrooping in general.

6.5 Identifying the non-cybertrooper accounts

The mixed-method approach described in the previous two sections was crucial to the complex process of identifying cybertrooper and bot accounts because the procedure of making inferences about the data alone is not always precise. After all, there is always the possibility that Twitter users could have followed, or come across, a cybertrooper account, and in believing those to be authentic (as opposed to being orchestrated) shared their tweets. As such, these users may unintentionally appear in the series of identical tweets found within the datasets. Additional analysis of hashtags, timelines and profiles through the use of observational and scrollback methods allows for genuine Twitter users—who may inadvertently be mixed up with cybertroopers from a study of their tweets alone—to be isolated from that sample. For example, there were some accounts—possibly genuine—found within both the #bersih and #bersih4 datasets that showed similar duplicate tweet patterns as those identified in Section 6.3, although there were no overlaps found with tweets from the suspected cybertroopers.

Having established certain characteristics of cybertroopers, it was possible to isolate some accounts from the sets of duplicate tweets. One example relates to two Twitter accounts with similar sounding names, not unlike the 10 accounts linked to Shukri Ali in Section 6.3.7. However, a study of their timelines and Twitter profiles shows

that both accounts do not hide the fact that they belong to the same person. On the respective profile sections of the accounts, both link to the same blog, which belongs to the user behind both accounts. This is a classic example of an 'alt account'[14], where alternative usernames are linked to the username of their main accounts for legitimate reasons such as boundary regulation purposes (van der Nagel, 2018). In addition, the tweets found within the dataset sent from the two accounts were not found to be identical to those from any other account. This is another way to test whether some accounts may be associated with orchestrated mobilisation. Accounts in the datasets that match the use of alt accounts—such as those in this example—are not considered cybertroopers.

Similar sounding usernames aside, there were also a number of accounts in the datasets that had sent tweets with the exact same text originally posted by organisations, including media outlets who were tweeting live updates from the rallies. In the case of the #bersih dataset, there were 63 such tweets involving news organisations like *Malaysiakini* and *Yahoo! News*, and the media arm of the then-opposition party, *Keadilan Daily*. The accounts which posted the duplicate tweets with these news updates are also not considered cybertroopers for two reasons.

First, where the identical tweet is of one sent from a news outlet (50 of the 63 tweets), the timestamps clearly show that the news outlet had tweeted it out first. It is likely that these identical tweets sent by other users were a result of them following those news accounts or having encountered the said tweets through a hashtag search

[14] Alt accounts are commonly found on social media platforms, often created for various purposes including privacy, identity management, throwaway accounts for specific topics, and the creation accounts for different personas, such as drag artists (van der Nagel, 2018). In her study on pseudonymous accounts, van der Nagel states that "some people have an alt in order to distinguish themselves from their professional account, some are connecting with those who share a specific interest, and others deliberately create an alt account to harass and troll others on Twitter" (para. 22).

before sharing them on their own accounts without using Twitter's retweet function. Secondly, a further investigation into these accounts—as with the case involving the two alt accounts discussed above—did not produce any connections to the identified cybertroopers. In fact, the top two accounts found within the 50-tweet sample posted only a total of seven and three identical tweets with the news outlets respectively. In addition, the duplicates consisted mostly of live updates and retweets, and did not take a particular stand, whether for or against, on Bersih. In contrast, there were 72 different messages (all of which followed the "joining #bersih" theme) which were sent out as duplicates in different numbers by the cybertrooper accounts discussed earlier.

For this thesis, it was important to distinguish actual cybertrooper accounts from genuine accounts because the few tweets mentioned above involving genuine alt accounts and news organisations were also different in that they were not specifically pro-Barisan Nasional or pro-government. This finding does not suggest that the then-opposition, or a civil society group like Bersih 2.0, do not engage in manipulative strategies online. After all, the leaders from the Democratic Action Party (DAP) themselves admitted to having their own online team of volunteers. However, what this analysis of the two datasets indicates is that, if indeed the opposition or groups like Bersih do engage in such practices, they do not use a similar approach as the Barisan Nasional cybertroopers. This finding is significant considering accusations by DAP leaders that allegations of their funding of the Red Bean Army is framed within the understanding of how Barisan Nasional cybertroopers operate. There is no evidence within the Twitter datasets of this similarity.

That is not to say that there were no pro-opposition or pro-Bersih tweets found within the identical tweets identified from the datasets. However, the number of such tweets in both datasets was small compared to those which were pro-Barisan Nasional. In the #bersih dataset, these only amounted to between less than forty from datasets as large as 60,000 tweets. In contrast, the accounts which make up the "joining #bersih" sample alone consist of 438 tweets. Again, in all of these instances, no other suspicious patterns emerged to suggest that such tweets were part of an organised effort to push a particular message. There are other reasons that could explain the existence of these other 'non-cybertrooper' identical tweets, aside from the use of alt accounts and sharing of news as discussed. One possibility is that genuine users who were keeping up to date with the rally just copied tweets they felt strongly about and posted them from their accounts, or that random automated accounts (in this instance, non-political bots) were picking up on tweets sent using a popular hashtag at that point in time[15]. It is also worth noting that a similar collection of duplicate tweets that were pro-Barisan Nasional, pro-government, or anti-Bersih, can be found in the datasets but are not considered to be cybertrooper accounts upon further analysis for the same reasons. The number of these accounts is equally negligible as the pro-opposition or pro-Bersih ones.

There was one instance, however, where a notable pattern involving seemingly pro-Bersih tweets emerged. This pattern was found in both datasets, and involved numerous tweets where the text primarily contained the hashtags with little or no context. Hundreds of the tweets—193 in first dataset and 355 in the second—were found to have used only the hashtag with no other text, and in some instances, were

[15] The adoption of a popular hashtag to boost one's completely unrelated tweet is sometimes referred to as 'hashtag hijacking'. However, another interpretation of this term is discussed further in Chapter 7.

repeated numerous times within the same tweet. Some of these tweets can be seen in Table 6.7.

Table 6.7

Some examples of tweets which used only the #bersih hashtag with little or no context. The timestamp reflects Coordinated Universal Time (UTC).

Date and Time	Text in tweet
2012-04-28**T04:37:10+01:00**	#Bersih
2012-04-28**T04:09:27+01:00**	#Bersih
2012-04-28**T10:35+01:00**	#Bersih
2012-04-28**T04:30:28+01:00**	#Bersih
2012-04-28**T08:47:33+01:00**	#bersih
2012-04-28**T07:07:13+01:00**	#bersih !
2012-04-28**T06:25:12+01:00**	#Bersih !
2012-04-28**T03:50:19+01:00**	#bersih!!
2012-04-28**T03:31:40+01:00**	#bersih!!
2012-04-**28T03:44:10+01:00**	#BERSIH #BERSIH #BERSIH
2012-04-28**T12:07:48+01:00**	#Bersih #Bersih #Bersih
2012-04-28**T13:05:35+01:00**	#bersih #bersih #bersih
2012-04-28**T03:49:39+01:00**	#Bersih #Bersih #Bersih
2012-04-28**T06:08:57+01:00**	#bersih #bersih #bersih
2012-04-28**T07:01:46+01:00**	#bersih #bersih #bersih
2012-04-28**T04:56:46+01:00**	#Bersih #Bersih #Bersih
2012-04-28**T03:20:54+01:00**	#bersih #bersih #bersih #bersih #bersih #bersih #bersih #bersih #bersih #bersih
2012-04-28**T07:20:27+01:00**	#Bersih #Bersih #Bersih #Bersih #Bersih #Bersih #Bersih #Bersih #Bersih #Bersih
2012-04-28**T04:25:55+01:00**	#Bersih #Bersih #Bersih #Bersih #Bersih #Bersih #Bersih #Bersih #Bersih #Bersih #Bersih #Bersih #Bersih #Bersih #Bersih

In the limited occurrences where there was other text accompanying the hashtag, most generally represented support: "*Saya sokong #Bersih*" [I support #Bersih],

"*Hidup #Bersih"* [Long live #Bersih], "#Bersih4 Happy to walk" and "*Jom #Bersih4*" [Let's join #Bersih4]. The ways these hashtags are used speaks to the many "communicative functions" scholars have associated with the hashtag, which within this context constitutes the "demonstration of emotion, solidarity, or reaction" (Highfield, 2018, para. 2 and 6). Granted, these tweets amplify support for a movement—in this case, the Bersih rally—the same way it can be argued that Beruang Biru seeks to support Barisan Nasional.

For example, this high number of tweets using just the #bersih or #bersih4 could well be an organised effort to make the hashtag appear in the Twitter Trending Topic list for visibility purposes. However, no evidence within the dataset suggests that the accounts posting these tweets were centrally mobilised the way cybertroopers are. From the collection of 193 tweets using the #bersih hashtag, only five accounts out of 182 sent more than one tweet that could be found within the dataset. These were also the only duplicates within the whole #bersih dataset sent from these five accounts.

There were also other ways in which these tweets stood in contrast to those identified as cybertrooping activity. As Table 6.7 illustrates, the minor differences in the text of the tweets—different capitalisation of particular words (even within the hashtag, variations include #bersih, #Bersih, #BERSIH), the number of exclamation marks used (#bersih! #bersih!!) or the language used ("*Saya sokong #Bersih*" in Malay and its English version "I support #Bersih" were both found in the dataset)—stood in stark contrast to, for example, the scripted Lahad Datu tweets discussed in Section 6.2 where identical tweets were presented verbatim from several accounts.

In addition, it was not possible to link these accounts to other identified cybertroopers because of the way they all seemingly take a different stand on the Bersih rallies. Based on the lack of any activities found within the datasets that mirrored those executed by the pro-Barisan Nasional cybertroopers identified, these accounts cannot be considered to be engaging in cybertrooping. As such, these pro-Bersih tweets discussed above are considered part of promotional culture using hashtags on social media, often seen in marketing and advertising campaigns. Scholars have long studied the effectiveness of repetition in communication practices and reception (Campbell & Lane Keller, 2003). Even when discussing the use of multipliers in the military, Dean (2010) argues that the strategy is based on lessons learnt from advertising and pop music.

This understanding is another way to consider the pro-Bersih tweets discussed above to be conceptually different from cybertrooping. Promotional culture on social media does not always require covertly asking users (as is the case with cybertroopers) to adopt a generic hashtag to amplify it with the aim of making it trend. There is also no evidence to suggest that the organisers of the Bersih rallies have even called for users to amplify that hashtag; the adoption and amplification of the #bersih and #bersih4 hashtags is not unusual for a movement or event of this scale. Taking into consideration the hundreds of thousands of people who took to the streets at both Bersih rallies, a few hundred tweets of support is not a very significant number.

6.6 Conclusion

This chapter has presented an extended discussion on the instances of cybertrooping conducted by Barisan Nasional cybertroopers, based on the analysis of the Beruang

Biru emails and the Twitter datasets. It showed that one of the features of cybertrooping is the propagation and amplification of articles and materials—or astroturfing—including pre-scripted messages. This was evident from not just the discovery of tweets matching the suggested texts from the Beruang Biru emails, which occurs when the recipients disseminate the same information, but also in the patterns stemming from identical messages found in the Twitter datasets. Indeed, propaganda—in whatever shape or form—is often most effective with volume and was found to have been used by cybertroopers in two ways.

First, the discovery of loops of identical messages posted can be understood within the context of what Dean (2010) calls the force multiplication of messages. Secondly, the many instances of sockpuppetry, creation of several similar-sounding accounts and bots found are instead examples of multiplication of message forces. The many recipients of the Beruang Biru emails following its instructions—those identified within the dataset or otherwise—can also be considered multipliers. Significantly, no accounts featuring pro-opposition or pro-Bersih messages were found to have used similar approaches by the cybertroopers. Where similar patterns emerged, these accounts were linked to news organisations, legitimate alt accounts, or matched instances of promotional culture on social media. These reasons discounted said accounts from being considered cybertroopers.

This chapter has focused on force multipliers because it is the most readily identifiable instance of cybertrooping in a large dataset. This allowed me to establish the extent of cybertrooping activity being conducted and that Beruang Biru's instructions are being followed. The discussions presented clear evidence extracted from the datasets to further develop the understandings of how Barisan Nasional

and its former governments' cybertroopers are mobilised. The key points elaborated in this chapter will be useful as a basis for the analyses to be presented in the next chapter.

CHAPTER 7

Decoding cybertrooping activities: operations and mobilisation

This thesis has already established that Barisan Nasional cybertroopers engage in activities involving the force multiplication of messages. Moving that discussion forward, this chapter aims to unpack the other tasks and activities instructed within the emails which were not as easily identifiable as the instances of cybertrooping discussed in Chapter 6. Some of these activities such as trolling, brigading and spamming may overlap with the previously discussed efforts at force multiplication—in that amplification and volume are also key features—but they proved more difficult to identify on their own, requiring further examination of the datasets.

This chapter will begin with a discussion on how cybertroopers are coordinated and deployed to better understand the functions of an operation like the one behind Beruang Biru. This section will further support the assertion that cybertroopers are part of Barisan Nasional's larger communication strategy through a discussion of the extent of the strategising and planning that goes into the mobilisation as well as the hierarchical structure and covert nature of the operations. Next, a typology of the various strategies, techniques and tactics beyond just the force multiplication of messages will be presented. The discussions in this section will illustrate the extensive scope of work that is expected of cybertroopers. This typology is not meant to be exhaustive, but it sufficiently provides insights into how the various features and affordances of social media and the internet can be used for illiberal practices such as the manipulation of communication practices and information flow. The chapter

then concludes with a summary of how the findings presented to that point can be understood within the framework that shapes this study.

7.1 Beruang Biru mobilising cybertroopers

This thesis has so far made the case that Beruang Biru is part of a strategic unit aimed at assisting Barisan Nasional to secure its grip on power at the 13th General Election. The very nature of the Online Deployment Strategy (ODS) template in itself indicates how Beruang Biru and its cybertroopers are part of an extensive communication plan. However, the analysis of the email dataset presented in Chapter 6, for example, posited that the operations involve more than just dissemination of information; it also includes record keeping through the use of hashtags on Twitter, and the monitoring of political support based on "current data" on polling day. The release of regular topics to be addressed almost daily as part of a "deployment strategy"—some of which include the launch of campaign material such as websites and the party's electoral manifesto—and the specificity of what materials can and cannot be used by "official accounts" also indicates the strategic role that Beruang Biru plays.

That there were two forms of ODS emails found in the dataset—the 'regular' daily updates previously discussed and 'Ad Hoc' deployments—further emphasises the extensiveness of the operations. In total, there were 19 emails in the dataset labelled 'Ad Hoc' as per the subject line (most of which followed the ODS template) and were sent out in the weeks ahead of the general election. The use of the term 'Ad Hoc' suggest that the topics the emails include were not premeditated and were released as a response to events or conversations that were occurring during the

election campaign period. This was evident from the regular ODS email sent out on 4 March 2013 which advised recipients to "standby for further ad hoc deployment" related to the Lahad Datu insurgency in Sabah. Despite the standby notice, the next 'Ad Hoc' email was sent out over 24 hours later, following Prime Minister Najib's announcement that the Armed Forces had stormed the insurgents earlier that day. The email was likely labelled as such because Beruang Biru was awaiting updates from an active ongoing event. In any case, both sets of instructional emails attempt to mobilise cybertroopers to engage in astroturfing, which by definition involves orchestration and coordination in advance.

Another indicator of the planning that has gone into the mobilisation of cybertroopers can be found in the email received from Beruang Biru on 16 March 2012, aimed at plotting an online attack against then-opposition leader Anwar Ibrahim. A line from the email reads, "This is something we should definitely be flagging online, offline and in traditional media – loudly and immediately." This email further supports my argument in Chapter 5 that cybertroopers are part of a multi-pronged attack on the opposition, using both online and offline media, and on-the-ground methods such as through third party groups (although, it is worth noting that third party groups can also be mobilised online). This approach is another indicator of cybertroopers' role in Barisan Nasional's communication operations.

It is also possible to look to the discussion above to make the case that cybertroopers—at least those mobilised by Beruang Biru or in a similar manner—operate within a hierarchical structure. This matches the structures of contemporary political communication, through its reliance on public relations specialists and spin doctors to manage and execute a political entity's communication strategy. Aside

from all the undertakings that a campaign the scale of a general election requires, the top-down nature of cybertroopers is also evident in the way they are instructed by Beruang Biru. The seemingly casual tone and use of language found in the earlier dated emails—asking for the recipients' "cooperation", "kind consideration" or "assistance and consideration"—belies the reality of these requests. Emails like the one received on 23 February 2013 that labelled topics in the ODS as "This week's compulsory strategy" and "Today's compulsory strategy"[1] are indicative that the volume of "assistance" being requested by Beruang Biru are tacit instructions. The term "compulsory" does raise the question of how cybertroopers are being rewarded for their service, or what sanctions may be in place for non-compliance. There are no indications within the datasets to evidence that any form of reward was on offer although previous discussions have already indicated, based on news reports quoting former UMNO Youth leader Khairy Jamaluddin for example, that some cybertroopers are on the payroll of parties. The Pakatan Harapan Minister Saifuddin Abdullah also confirmed that some cybertroopers are paid, adding that sometimes cybertroopers are paid in kind (S. Abdullah, personal communication, July 14, 2018). He also claimed that individual leaders in UMNO, his former party, had their own teams of cybertroopers.

It is also possible that the mandatory requirements are for specific recipients of the emails, such as those operating the accounts of Barisan Nasional and state officials who are likely under the employ of the party or government. There is also a case that can be made for unpaid volunteers who have agreed to follow directives—or simply supporters who are following many pro-Barisan Nasional accounts—to support and assist the coalition to return to power, which in itself can be seen as a reward.

[1] In both instances, the quotes are translated from the Malay word "*wajib*".

Whatever the case may be, these sorts of directives are seemingly no different from how certain talking points are prepared in advance for press officers by spin doctors ahead of their meeting the press. This correspond with the way UMNO's Shahrul Zaman and Khairy Jamaluddin described information being fed down from the party to their online teams. Shahrul even likened cybertrooper operations to the structures of multi-level networks.

This hierarchical structure is also important in investigating cybertrooping because it extends the understanding of cybertroopers beyond just those who may be employed or have signed up to directly take instructions from Barisan Nasional. This point specifically addresses instances where some accounts—possibly genuine users—were found in Twitter searches to have sent identical messages as cybertroopers but were not in the datasets. In the context of astroturfing, this distinction is not significant because if indeed those accounts are genuine, then they only show the effectiveness of the cybertrooping strategy. In their study, Rakiewicz et al. (2011) note that regular users have been found to be involved in astroturfing after having been deceived by the original set of astroturfers[2]. In this sense, genuine users inadvertently become part of the hierarchical structure—right at the bottom—much like the end users purchasing goods from downlines in a multi-level marketing scheme.

[2] Understood within the context of this study, it is not just genuine users—likely already pro-government supporters considering the talking points being propagated by Barisan Nasional—on social media platforms who are deceived, however. The tone used by Beruang Biru when requesting for "assistance" and "kind consideration" could also be an approach to recruit unsuspecting recipients of the emails who they believe to be sympathetic to the Barisan Nasional cause. This could explain why some people—like myself—were added to the mailing list in the first place without having signed up for it. In a reply to the 14 May 2012 email that explained the purpose of the emails, one recipient thanked Beruang Biru and said that they would use the material. These decentralised cybertroopers, not working directly for the coalition, could be among those former UMNO Youth leader Khairy Jamaluddin calls "hardcore cybertroopers", who he describes as "fanatic Barisan Nasional" supporters not "under the payroll of political parties", as presented in Chapter 5.

In spite of all these premeditated plans, predetermined messages and mandatory directives, there are indications within the dataset that cybertroopers are given some flexibility in the way they execute some of the tasks. This is to be expected considering the amount of information that is provided by Beruang Biru, whether in the various articles and media content sent each day for dissemination or the numerous topics each Online Deployment Strategy email includes. Even the email with the "compulsory" instruction included a list of topics (four for the week and five for the day). In some instances, cybertroopers are also given leeway in how they craft the messages based on the talking points. Bloggers in particular were asked to discuss the topics on their blogs in the "own style" ("*gaya sendiri*") using information provided. Although there was no explicit mention of this approach for Twitter messages in the emails, some tweets from the "joining #bersih" sample show how "own style" might have also been adopted for tweets. As previously mentioned, many of the tweets in the sample set were found to be identical. However, there were a number of tweets beginning with "joining #bersih …" that only appeared once in the dataset, highlighting the possibility that they may have been personally crafted by a cybertrooper[3]. While this is merely conjecture, there is evidence within the Twitter datasets that cybertroopers do make modifications to the scripted messages provided by Beruang Biru.

Using the example from Section 6.2 in the previous chapter related to the government response to Ops Daulat in Lahad Datu, Sabah (10 April 2013), one

[3] To ensure that this was not the result of duplicate tweets not being captured due to API limitations, a Twitter search was conducted on those non-identical tweets, which showed that no other users had posted the exact same text. It is possible however that the search returned a negative result because Twitter accounts or individual tweets might have been deleted.

particular account had posted a tweet with slight edits by incorporating hashtags—from the options provided by Beruang Biru—into the text of the tweet.

Figure 7.1: *Example of two tweets with text similar to those suggested in an Online Deployment Strategy, except that the sender had replaced certain words with hashtags.*

The two tweets in Figure 7.1 are not explicitly duplicates of the suggested messages but the primary text was essentially verbatim from the email.

The differences in the propagated messages due to the use of a cybertrooper's "own style" does not detract from their objectives. While the identical tweets presented in Chapter 6 demonstrates an obvious way that scripted texts are multiplied, the core topic (and angle) within each of these messages remains the same. If anything, the use of "own style" allows for an element of plausible deniability on the part of the blogger (or Twitter user), which means that they can get away with making it look like a genuine grassroot message, or astroturfing. It also enables them to push the same agenda without bringing attention to the work they conduct on behalf of Barisan Nasional, an extremely valuable element considering the negative perception of cybertroopers in political discourse. Aside from the use of sockpuppets, this stealthy approach is another way that cybertrooping involves covert action.

7.2 Typology of activities and tactics

Having presented a discussion on how cybertroopers are coordinated and how they receive their instructions and material for dissemination, this chapter now proceeds to discuss what other propagandistic techniques and tactics were apparent within the emails. This section builds on the instances of astroturfing already identified in Chapter 6 to illustrate the other tasks that are expected of cybertroopers. The discussion so far has only involved the dissemination of information, propagation of hashtags, and spreading of external links. These additional approaches that involve amplification and volume include the use of memetic signifiers and sockpuppet accounts, spamming and hashtag hijacking. The emails also show how cybertroopers are involved in organised attacks on their opponents, using tactics such as brigading, trolling and priming. It supports the arguments made in Chapter 5 that Barisan Nasional cybertroopers engage in more than just correcting "lies and slander" distributed by their opponents. It is also pertinent to note that typology reflects only what could be illustrated or inferred from within the datasets that make up this study, and as such does not set out to be exhaustive. However, they do develop further the seemingly straightforward approach of force multiplication of information based on predetermined messages and talking points, contributing to a more extensive understanding of cybertrooping.

7.2.1 *Coordinated trolling*

Aside from disseminating information—whether scripted or in "own style"—one of the tasks instructed by Beruang Biru is to attack opposition personalities on social media. While the talking points in some Online Deployment Strategy emails include

messages that can be considered 'attacking' in nature, these tasks in question involve a direct assault on the accounts of said political opponents. As one example, an email sent on 12 April 2013 called for the account @Khalid_Ibrahim (belonging to former Selangor Chief Minister Khalid Ibrahim) to be "challenged" (*cabar*), thereby pushing him into naming the source of his claims that university research showed Pakatan Rakyat could win 125 seats at the 13th General Election. While not directly calling for it, Beruang Biru was encouraging its cybertroopers in name-calling, stating that if he failed to provide said evidence, it would mean that he is a "big liar" (*pembohong besar*). In other instances, Twitter usernames of those deemed to be pro-opposition (including political leaders, activists, and cartoonists) were identified for coordinated attacks without providing scripted messages (6 March 2013). The instruction below illustrates this:

> *Terus menghentam pemimpin-pemimpin & personaliti Pakatan yang masih menyalahkan UMNO/BN dan mempertikaikan tindakan kerajaan @mbnizar @tianchua @LatheefaKoya @abby_abadi112 & @ZunarKartunis*
>
> [Continue bashing leaders and personalities linked to Pakatan that vilify UMNO/BN and are critical of government actions @mbnizar @tianchua @LatheefaKoya @abby_abadi112 & @ZunarKartunis]

These sorts of attacks are akin to online bullying or harassment. This is sometimes referred to as trolling, which is historically conducted for no other purpose than, in internet speak, 'for the lulz' (just for laughs). In this instance, however, the act is premeditated and orchestrated through the mobilisation of a group of people, and the subject is targeted for a very specific intent and political purpose. It is because of this distinction that I describe these acts as 'coordinated trolling'. It is worth noting

that the term 'trolling' in itself has been used by Beruang Biru to describe similar activities. In an email sent on 10 May 2013, cybertroopers were asked to "troll" Anwar Ibrahim's Twitter account by criticising his characterisation of the increase in cooking gas prices as Barisan Nasional's victory gift to the public. The implicit instruction is for cybertroopers to tag his account (@AnwarIbrahim) in their tweets calling him out. The choice of the term troll by Beruang Biru is worth highlighting because it speaks to the conventional understanding of trolling described above—an online act of disruption—as opposed to the many motivations and strategies that may be employed by political 'trolls' (e.g. Russian troll factory), in their attempt to undermine democratic practices[4].

'Coordinated trolling' as cybertrooping features two characteristics from the framework: demonisation and disruption. The first characteristic is clear from the act of targeting Barisan Nasional's opponent with a negative message. Disruption, meanwhile, refers to the tangible consequence of such flooding of tweets on a particular politician's account, interfering with their use of Twitter. This point on disruption also distinguishes such attacks from instances where an opposition politician is publicly demonised by tarnishing their image on social media. For example, Beruang Biru had instructed cybertroopers to use a hashtag created for Vice President of the then-opposition National Justice Parti (Keadilan) Tian Chua—#tolaktianchua [reject Tian Chua]—that was to be used alongside the #pengkhianatnegara [national traitor] hashtag. This directive was in response to Tian Chua's court appearance for allegedly seditious comments he made about the insurgency at Lahad Datu in Sabah. The attack on Tian Chua can be considered in

[4] This distinction has been discussed in Chapter 2.

the same vein as the tweets found using the #dearambiga hashtag mentioned in Chapter 6, aimed at attacking Ambiga Sreenevasan, who was then the chairperson of Bersih 2.0. In both these cases, the Twitter accounts of Tian Chua and Ambiga are not directly affected by the creation of these hashtags.

7.2.2 *Brigading*

The instructions to attack political leaders through coordinated trolling could also to a certain degree be seen as a form of 'brigading', where cybertroopers are being directed to a website or platform to perform a particular task. This thesis, however, turns to the more common use of the term, referring to groups of users on discussion site Reddit[5] that engage in "mass coordinated voting" to upvote or downvote a particular post (Carman, Koerber, Li, Choo, & Ashman, 2018). In this context, I argue that brigading refers primarily to the quantifiable elements (votes)—such as the 'Like' or 'Dislike' buttons—to impact on how a particular content is viewed (and perhaps, along the way, game the algorithms on social media platforms).

Numerous Online Deployment Strategy emails have requested that cybertroopers 'Like' a particular Facebook page such as *Friends of BN*, and the Prime Minister's *Najib Razak Club* and *Ah Jib Gor* pages (16 April 2013). On YouTube, videos such as the one produced by government agencies in conjunction with the 206th National Police Day—a video related to *Ops Daulat* in response to the insurgency at Lahad

[5] In describing Reddit as a site, Massanari (2015, p. 339) argues that "Reddit already functions as a de facto vote-brigading platform, as it encourages large numbers of people to visit (and comment on) material other sites host". This more general interpretation of the term is also used by other scholars such as Glenski and Weninger (2017, p. 15) in discussing the "retweet armies" on Twitter "that attempt to manipulate the velocity of some discussion in order to artificially force a topic to become a 'trending' topic".

Datu—were also identified by Beruang Biru for a 'Like' (28 March 2013). These examples show elements of positive brigading (in the same vein as positive propaganda); however, similar instructions could be used to attack the opposition as well. For example, cybertroopers were asked to 'Like' a video comprising footage of DAP leader Lim Kit Siang being chased out of a food outlet while canvassing ahead of the general election (29 April 2013). Upvoting a video which negatively portrays the opposition can be seen as an attack on his public image, in the same way hashtags such as #tolaktianchua achieve this objective. In all the instances of brigading mentioned above, the instructions to 'Like' a page or content were also accompanied by the request to share and distribute those links to propagate them. Conversely, where Beruang Biru listed links to YouTube videos attacking Barisan Nasional or the government, cybertroopers were instead asked to defend the image of the party by using the 'Dislike' button (or thumbs down), and to leave "negative comments" in the comments section to "reveal the lies" behind the video (10 May 2013)[6].

Where the line between brigading and astroturfing might blur is in instances where Beruang Biru asks its cybertroopers to "like and share" postings. For example, posts flagged for sharing included those related to *Gerakan Menolak Penipuan Pembangkang* (GEMPAK), which is UMNO Youth's campaign to "expose opposition lies" (16 March 2013), on the *Friends of BN* Facebook page, and those on then-Home Minister Hishammuddin Hussein's Facebook page related to the Lahad Datu incursion (13 March 2013). With these cases, it was not just about the number of 'Likes' a post received but also about the multiplying of the posts using the 'Share' feature on those platforms.

[6] Cybertroopers were also sometimes asked to leave positive comments where the videos or post are favourable to the government or Barisan Nasional (instead of just 'Like-ing' them).

7.2.3 *Spamming*

A key feature of astroturfing, coordinated trolling and brigading collectively is the volume of the messages and multipliers. Some of the activities that fit within those strategies can be considered 'spamming'[7], commonly used as part of marketing and political communication strategies. Studies have found that militaries, state actors and political parties around the world engage in political spam (Woolley, 2016), and this is no different for cybertroopers in Malaysia. To understand spam, I turn to Cormack and Lynam's (2005, para. 4) definition: "unsolicited, unwanted email that was sent indiscriminately, directly or indirectly, by a sender having no current relationship with the recipient." In the context of Twitter, these are tweets where users are tagged into a post unsolicited, particularly by someone who is unknown to said user. The tweets from the two Bersih rallies did not show significant use of spamming—the tweets tagged other users that I used as an example of how to get around Twitter's duplicate tweets loophole were minimal—although there were many identical messages in the datasets.

This is not to say that cybertroopers do not engage in the dissemination of spam content. In the conducted Twitter searches to support the analysis of cybertrooping from Bersih tweets, I identified several accounts not found in the dataset that engage in spamming. As an example, Figure 7.2 shows three of eight similar tweets sent by one account which contains the same content but tagging different users (the first, @CLanPaul, followed by @adpadiputra and then @aizatjaafar).

[7] Aside from 'brigading' because astroturfing and spamming both deal with the creation and/or dissemination of content.

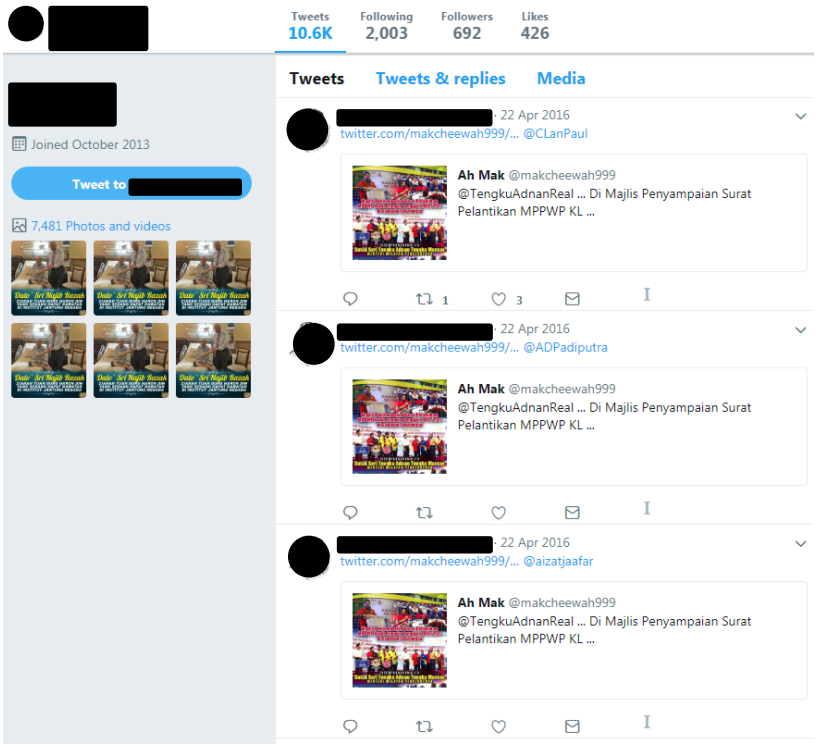


Figure 7.2: *An example of a suspected cybertrooper account that engages in spamming.*

As can be seen on the left side of the screenshot, Twitter shows six of the most recent "Photos and videos" sent by the user, each representing a tweet. Those six were part of 10 of the same image that were sent from the account, each post containing the same text and hashtag, but each tagging a different user to get into their timelines. Figure 7.3 shows some examples of this from the same account.

Figure 7.3: *Three of 10 images featuring former Prime Minister Najib Razak visiting one of his political foes at hospital, all of which contain the same text and hashtag but tagging different users. Translated, the tweet reads: "Political differences aside, friendship among Muslims trumps all. #RespectMyPM".*

While accounts like these may look primarily like spam accounts—that is, one that was created for the sole purpose of sending those kinds of messages—this is not always the case. For example, the account in Figure 7.4 also engaged in spamming (note the left side of the screenshot below where Twitter shows five tweets of the same image having been sent, each tagging different users). On the right side, however, the timeline shows that the account used Twitter's other functions as well, including retweeting news accounts.

Figure 7.4: *Example of a suspected cybertrooper account that does not exclusively exist for the purpose of spamming.*

The example in Figure 7.4 considers the distinction between astroturfing and spamming based on Ratkiewicz et al.'s (2011, p. 249) distinction: "… spammers are often interested in causing users to click a link; in contrast, astroturfers want a particular tweet or idea to have a false sense of group consensus." Spammers like the one in Figure 7.2 and 7.3 do not necessarily attempt to hide the fact that they are engaging in that activity—the pattern of the content they share easily identifies

that—unlike astroturfers who may attempt to disguise their activities so as to come across as genuine users. However, when contextualised in terms of cybertrooping, these two groups of people (spammers and astroturfers) do not necessarily need to be considered separately; instead, the distinction is in the tactics they employ (spamming versus astroturfing). As illustrated in the second example above, a cybertrooper account can engage in both.

Spamming can also be expanded to include the mass sending of messages, which do not necessarily intrude into someone's (virtual) space such as their email inbox or Twitter streams (from being tagged into a tweet). This understanding turns to the 1990s definition of spam, when the term was first used to describe electronic messages by users of online discussion groups referring to "annoying and distracting cross-postings", specifically postings that drowned out conversations on those groups (Massof, 2004, p. 631). In this context, the identical messages discussed in Chapter 6 (astroturfing) could also be considered spam, particularly when used to refer to the flooding of hashtags (to be discussed later in this chapter). This understanding is not novel; a study by Verkamp and Gupta (2013) argues that spam is used online in countries like China, Syria, Russia and Mexico to suppress political speech.

7.2.4 *Memetic Signifiers*

Aside from the tasks described above, Beruang Biru also instructed its cybertroopers to engage with various social tools it had created. It requested that cybertroopers embed the widget for Better Nation—the campaign website for Barisan Nasional—on their blogs ahead of the 13th General Election (30 March 2013). However, there

was no widget to be found on there based on a snapshot on the date of the email using the Internet Archive's Wayback Machine (the site is no longer accessible). What the site did have, however, was a mechanism for the creation of a personalised "badge" that allows a user to include their name onto the image, which could then be downloaded and shared. This badge was possibly what was being referred to in the Beruang Biru email. Figure 7.5 shows a version of the badge being shared on Lowyat.net, a popular online forum in Malaysia. As the screenshot shows, the badges are personalised ways users can show their support for Barisan Nasional. The website suggested that the badge could be shared on social network platforms such as Twitter, Facebook, Tumblr and Instagram.

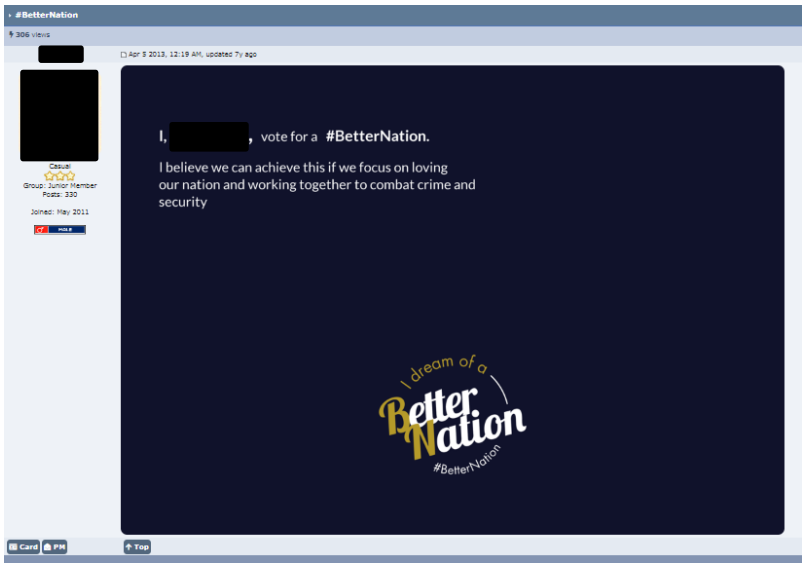


Figure 7.5: *The personalised badge from the Better Nation website—which is no longer accessible—as shared on an online forum in Malaysia. The identity of the person posting it has been blacked out.*

Similarly, Beruang Biru had also asked its recipients to display a Twibbon titled "Let's thank our brave troops" in conjunction with Prime Minister Najib's visit to Lahad Datu to observe the *Ops Daulat* response to the insurgency. The Twibbon—an image which can be used to overlay a user's profile picture on platforms like

Facebook and Twitter, and usually associated with a particular message or campaign—can be seen in the Figure 7.6. It reads: "*Jasamu dikenang*" [We appreciate your service].

Figure 7.6: *Screenshot from the "Jasamu Dikenang" Twibbon page, showing how it can be added to a social media profile picture. The page showed that the Twibbon was used by 760 users.*

The use of the badge and Twibbon can be considered "memetic signifiers", described by Gerbaudo (2015, p. 918) as "symbolic references that because of their … capacity to spread with extreme rapidity, are highly conducive to processes of collective identification". In describing this, Gerbaudo was referring to protest avatars which he likened to political T-shirts, stickers and buttons, among other items. Barisan Nasional's intention to use these signifiers may not be in the context of a protest, but their characteristics are shared. Perhaps more close to Beruang Biru's use was the call by US-based Human Rights Campaign for the replacement of social media profile photos with its Marriage Equality logo in 2013, which Vie (2014) argues is a form of memetic transmission (the power of the replication of memes).

To discuss the potential reach of such a tactic in Malaysia, an example can be made of the 2016 #RespectMyPM campaign. It gave supporters of Prime Minister Najib a selection of images created for the campaign featuring flags from all the states in Malaysia, which they can post on their timelines alongside the following text: "I am from <insert Malaysian state> and I … #RespectMyPM". The campaign is reported

to have been started by the anonymous *Pertahan Negara Kita* [Defend Our Country] Facebook account, although this cannot be verified as the page no longer exists (Chew, 2016). However, Azalina Othman, a Minister in Najib's cabinet at the time, had posted the image on Twitter.

Figure 7.7: *Screenshot of a Tweet sent by former Minister Azalina Othman, with the #RespectMyPM hashtag and attached graphic.*

That Azalina participated in this movement could of course be a coincidence. However, she was formerly the chief of Puteri UMNO, the young women's wing of the party who has admitted having previously set up a team of cybertroopers, and as such, this could be a campaign she is associated with. Indeed, the hashtag was also used by a suspected cybertrooper account in a different context (see Section 7.2.4), adding to the suspicion that #RespectMyPM could indeed be a Barisan Nasional-organised campaign. Tan Keng Liang, a politician from the BN component party MCA, had also sent a similar tweet (Samadi, 2016).

There have also been accusations that accounts flooding Najib's Facebook page with the hashtag were sockpuppet accounts, another indicator that this could be a cybertrooping campaign ("Fake #RespectMyPM account busted for stealing another Malaysian's profile picture," 2017). If this campaign was indeed cybertrooping in action, it speaks to the use of memetic signifiers as part of a distraction strategy, or at the very least, to divert attention. These images appeared soon after the press conference organised by high-profile politicians, which saw the then-former Prime Minister Mahathir Mohammad appear alongside opposition and civil society leaders who had come together for the first time to collectively sign a citizen's declaration calling for Najib's resignation. The significance of the press conference no doubt led to a huge amount of attention (both in the press and on social media using the #SelamatkanMalaysia and #SaveMalaysia hashtags). However, the #RespectMyPM campaign grew large enough to generate attention from local and international media ("#RespectMyPM: Online war breaks out in Malaysia," 2016; "#RespectMyPM campaign gains traction," 2016; "Hashtag backfires in Malaysia PM's campaign," 2016), showing the effectiveness of this tactic, whether or not the #RespectMyPM campaign was cybertrooping in action. Even the media has reported that the campaign can be seen as a response to the #SaveMalaysia event (Chew, 2016).

7.2.5 *Hashtag hijacking*

Considering how common it is for hashtags to be used on Twitter for users to connect to each other, and to coordinate discussion (Bruns & Burgess, 2015), it should come as no surprise that they are targeted as part of efforts to manipulate communication flow and information. This targeting of hashtags goes beyond its use

for indexing purposes such as the way a list was provided by Beruang Biru for record keeping. Hashtags such as #bersih and #bersih4 have also been appropriated by cybertroopers to push Barisan Nasional's agenda as can be seen through the examples of loops of messages by pools of accounts discussed in Chapter 6. The same can be said of the "joining #bersih" tweets. The fact that these examples are indicative of astroturfing only shows that the strategies cybertroopers adopt in their tasks are not always mutually exclusive. Some instances, however, do show how this approach is more pronounced; for example, the duplicate tweets sent out by the same users (overcoming the various loopholes related to Twitter restrictions on repeated tweets) can serve this purpose. This is also the case with users who create multiple accounts—specifically those with similar sounding usernames—to send the same tweets. The volume of the tweets posted to appropriate the hashtag—both in terms of accounts and number of posts—is where said weaponising occurs.

Some scholars would describe the above as acts of 'hashtag hijacking' (Sanderson, Barnes, Williamson, & Kian, 2016). Jackson and Foucault Welles (2015) use that term to describe the hijacking of the #myNYPD hashtag—created as part of a public relations campaign inviting Twitter users to post photos of them with members of the New York Police Department—as a form of protest. Users appropriated the hashtag and tweeted about police brutality and racial profiling instead. In this sense, hashtag hijacking can be seen as a version of 'culture jamming', the movement which aims "to undermine the marketing rhetoric of multinational corporations, specifically through such practices as media hoaxing, corporate sabotage, billboard 'liberation,' and trademark infringement" (Harold, 2004, p. 190).

It is worth noting that the instances of hashtag hijacking found should be seen as distinct from instances of 'hashtag poisoning', which researchers studying online manipulation of information have found (Bradshaw & Howard, 2017; Kelly et al., 2017). Where hashtag poisoning is concerned, this refers to the method of drowning out tweets with irrelevant material to suppress the networked effects of a hashtag (Bradshaw & Howard, 2017; Kelly et al., 2017). It does not rely on the message of the tweets to make sense, because the message does not matter. In this sense, hashtag poisoning is similar to the early understanding of spam as junk mail (as opposed to the tactical use of spam to distribute a particular political message in large numbers). Hashtag hijacking is different in that the context of its use remains the same—the tweets found in the datasets using this strategy were still addressing the Bersih rally, as an example—except that it had been appropriated to suit a different agenda.

Hashtag hijacking can serve several purposes. Like with hashtag poisoning, it could flood a hashtag, rendering it useless for mobilisation or genuine discourse when used alongside amplification strategies. In order to achieve this, the team behind cybertroopers needs to ensure that there is volume in their tweets, through the use of multiple accounts including sockpuppets. Bots are specifically ideal to be used in these situations, due to the fact that automation means that hundreds or thousands of accounts can hijack a hashtag simultaneously and at a fast pace. Another purpose this tactic serves is to change the dominant narrative associated with a particular hashtag. In the case of the Bersih, for example, a flood of "joining #bersih" may encourage more criticism against the event to counter the many tweets in support of the rallies. This practice has been also referred to as reverse censorship (King et al., 2017). The third purpose is related to the occasions when hijacking tweets come

across as junk because there is no clear message in the tweets. Below are two tweets that can be used as examples:

> #changepenang #CHANGEPENANG #CHANGEPENANG #changepenang #CHANGEPENANG #changepenang #CHANGEPENANG #Bersih4 #AgendaYahudi #DAPpenipu budaya …
>
> #changepenang #changepenang #changepenang RT whyme2_07: #bersih4 #changepenang Penang providing face masks to primary schools … #changepena…

Despite the fact that both tweets do not have a clear message, this is not considered hashtag poisoning because they are still clearly related to the Bersih event, or at the very least, Malaysian politics (mentions of DAP and Penang, the state it governs). What is notable about them, however, is the use of the #ChangePenang hashtag. That this hashtag is included also speaks to another way the #bersih hashtag is appropriated, in this case, to bring—and even divert—attention to different hashtags the cybertroopers created where they may already hold the dominant narrative.

7.2.6 *Priming*

Hashtags can also be useful to cybertroopers as a tool for priming. In political communication, priming "occurs when news content suggests to news audiences that they ought to use specific issues as benchmarks for evaluating the performance of leaders and governments" (Scheufele & Tewksbury, 2007, p. 11). While content disseminated on social media platforms does not necessarily constitute 'news', priming can be useful to understand how cybertroopers are able to take advantage of the "specific issues" to influence the way the public thinks (or perceives). In the case of the Bersih movement, hashtags can be used for priming in order to affect the public's perception of Bersih 2.0, its agenda and the rallies it organises.

One of the clearest examples of this comes from the Bersih 4 dataset, a large number of which were tweets that included the hashtags related to the 'Jewish agenda' (*Agenda Yahudi*). The most common one used was #AgendaYahudi (with some tweets spelling it differently as #AjendaYahudi), although several were spelt #AgenYahudi. It is not clear if this latter spelling was a typo on 'Agenda' or if the cybertroopers intended on using the term to mean "Agent of Jews". What is clear is that the hashtag was widely found among identical tweets in the #Bersih4 dataset a total of 1,365 times. Chapter 8 will present a more extensive discussion on accusations of interference by Jewish people in Malaysian politics, but this example shows how hashtags can be used to trigger a particular impression of the Bersih rallies. Tellingly, in most cases, the hashtag was used even though the messages in the tweets had nothing to do with Jews or Israel, as the following examples illustrate.

> *#KNews #AgendaYahudi #Bersih4 sedaq la Melayu...Cina nak tuntut hak sama rata....bnyk cantik...*
> [Open your eyes, Malays… The Chinese want to demand equal rights… No chance …]
>
> *Melayu bersatu,Penang dh jd bukti bahawa bila mereka berkuasa,sekat sume sumber ekonomi*
> [Come together, Malays. Penang is evidence that when they[8] are in power, they will control all of the economy.]
>
> *Tolak #bersih4 menghuru-harakan ketenteraman awam bulan Kemerdekaan #AgendaYahudi #Kelat*
> [Reject #bersih4 for disrupting public peace during the month of our Independence celebrations]

The examples suggest that the Jewish agenda-related hashtags were only used as a mechanism for priming, which "shape the considerations that people take into account when making judgements about political candidates or issues" (Scheufele & Tewksbury, 2007, p. 11). Putting the description above of the effects of priming into context, the use of #AgendaYahudi at the Bersih 4 rally was likely used to direct a

[8] "They" in this instance refers to the Chinese. This is a reference to the predominantly Chinese party DAP governing Penang and often described as the 'Chinese party'.

particular "judgement" on Bersih 2.0 and Maria Chin (the "political candidates") or their suggestion that the electoral commission is corrupt (the "issues").

7.2.7 *Sockpuppetry*

The creation of multiple accounts to send the same messages belies the claims by Barisan Nasional party leaders that the cybertroopers consist of just volunteers defending the party from its opponents. It is one thing for an individual to create multiple alt accounts for cybertrooping purposes (some identifiable through similar sounding usernames), but it is another to create numerous accounts that do not clearly indicate that they are connected to each other. The Twitter datasets showed that the instances of alt accounts were dwarfed by that of other accounts seemingly independent of one another yet were connected through the ways in which they used their respective Twitter accounts. This is clearly seen with the "joining #bersih" tweets where 36 accounts were identified as potential cybertroopers[9].

To identify which of these accounts could potentially be cybertroopers, further analysis was conducted on their respective timelines using observational internet research and scrollback methods. At the time of analysis (up to August 2018), 26 of the 36 accounts were still accessible online. Searches were not conducted on Twitter by usernames because of how easy it is to change them, as was proven to be true with seven of the 36 accounts. Instead, they were identified using the Twitter ID from tweets sent by these accounts found within the dataset. The other 10 accounts

[9] Only 21 accounts were found to have sent "joining #bersih" tweets. However, an additional 15 that were found to have sent identical tweets to the 21 were added to create a sample of 36 accounts for the purpose of this discussion. These 36 accounts were also discussed in Section 6.3.5.

could no longer be accessed online; they were either suspended by Twitter or have been deleted by the users themselves.

A notable trend that emerged among these 26 accounts was that many of them were created in the same month, based on information on their Twitter profiles; 20 were created in April 2012, while five were created in February 2012. The remaining one was created in 2010, the only anomaly. That so many accounts were opened in the same month—Twitter does not publicly show the dates these accounts were created on—comes across as more than a coincidence, suggesting that this was an organised effort to create new accounts (whether 'real' or sockpuppet). If these accounts were not opened by the same person (or group of people), then it is likely that they were all instructed to do so at around the same time.

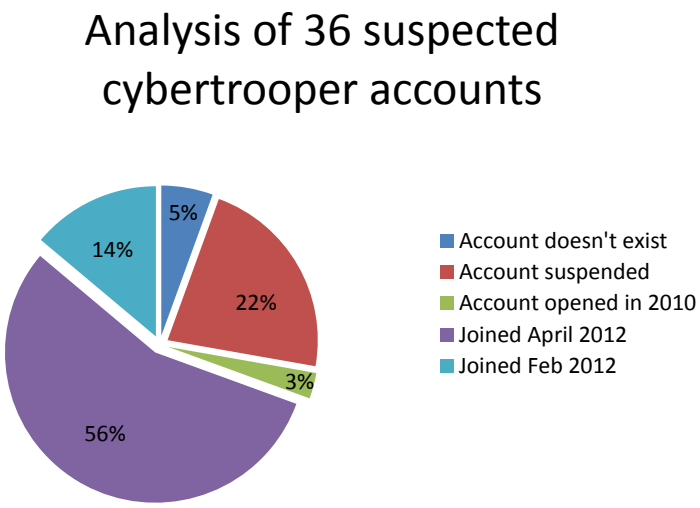


Figure 7.8: *The pie chart shows the percentage of accounts created in the same months; 70% of the 36 suspected accounts were opened in two months in 2012. This chart was created based on analysis as of August 2018.*

In addition, a total of 23 of the 26 accounts have retweeted content from a news account called @kwiknewsMY, self-described in its profile as "Displaying the top news on #Malaysia as it happens". That this is the news account those 23 already

suspicious accounts chose to retweet is in itself worth noting, not least because it is not well known in Malaysia with only 2,004 followers[10] (compared to other news sites in Malaysia like *Malaysiakini* or *The Star*, with follower counts that go well beyond the one million mark). Also adding to the suspicion is the fact that the @kwiknewsMy account was also created in February 2012, similar to four of the accounts in the dataset.

As examples of the accounts discussed above, I use the suspicious Twitter accounts belonging to those who go by the name Ameera Arini[11] (@meera_rin) and Tony (@TtonySt). These two accounts were found to have changed their usernames from @mira_rin and @Long_Ttony previously, taking advantage of how easy it is to change usernames on Twitter. It is not clear why they changed their usernames considering both still included elements from the previous version. One possibility is that this makes them less easily searchable on the internet. In fact, I was only able to confirm that both accounts changed their usernames—as opposed to opening another account with a different permutation of their respective names—by matching the Tweet IDs extracted from the datasets to the accounts using the newer username.

Table 7.1

Two tweets from suspected cybertroopers identified from the dataset, with the Tweet IDs for each one.

Username	Tweet	Tweet ID
Long_Ttony	I just dont get it that #dearambiga still doesnt wanna relinquish his #bersih leadership...cmon la...Mat sabu is waiting!! hehehe	196142096548249600
mira_rin	#dearambiga is an irresposible person...how can she let #bersih to continue n let KL be chaotic this saturday!!!	196141073607835648

[10] As of August 2018.
[11] This name first appeared in this thesis in Chapter 3. Meera Rin's email address appeared twice within the Beruang Biru dataset; one in their own name, and another as 'Ah Boon'.

The text in the screenshots in Figure 7.10 from both accounts is identical to the text from the dataset shown in Table 7.1. More significantly, the Tweet ID in the URL in the screenshots also matches directly with the Tweet ID from the dataset, confirming that they are the same account.

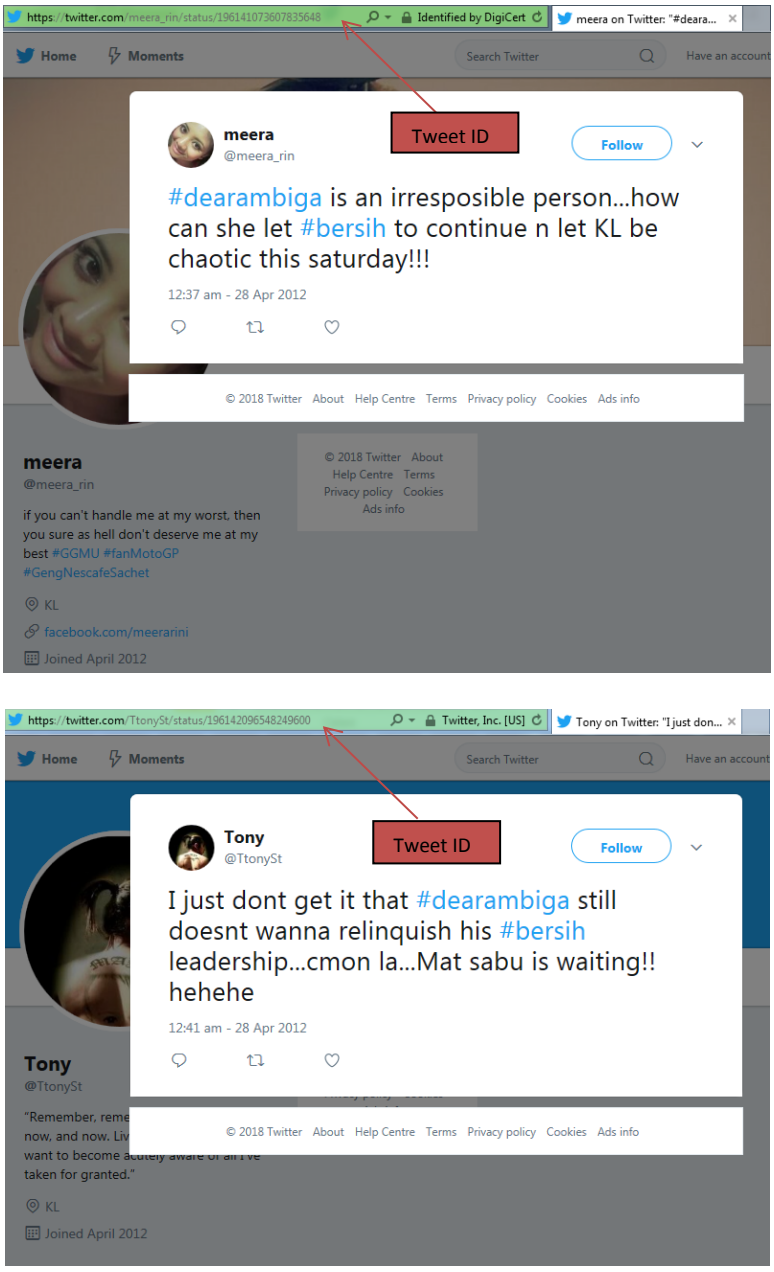


Figure 7.9: *Screenshot of the same tweet posted by @mira_rin and @Llong_Tony in the dataset, now associated with similar but different usernames. Note the Twitter IDs in the URL which match the ones in the dataset.*

While there was no evidence that @mira_rin and @Long_Ttony had sent identical tweets to each other within the dataset, they both used the same hashtag, such as #dearambiga. Many of the other "joining #bersih" accounts also used that hashtag, another pattern identified from that sample of cybertroopers as mentioned above. Besides the commonalities and patterns which have already been described, there is nothing on the two profiles that may link them directly to Barisan Nasional or the government. Yet, it is arguable that the activities they engage in, particularly those that match cybertrooping practices, is part of organised action.

This strategy of creating sockpuppet accounts—as opposed to running genuine alt accounts—is well documented in public discussions on cybertrooping. In 2016, a Facebook account sending messages supporting Prime Minister Najib was accused of using a profile picture of someone who had passed away (Buang, 2016)[12]. Similar instances to this were also found in the analysis of the Twitter dataset, specifically related to the sockpuppet account @uncleahboon. The account used the image of Chinese dissident Liu Xiaobo, who died in 2017. Tweets from this account had also appeared in the #Bersih4 data, under the username @ahboon4, meaning that the account also changed its username the same way @meera_rin and @TtonySt did. The tweets found in the dataset sent from @AhBoon4 include retweets of two tweets found within the sample of "joining #bersih" cybertroopers. In 2013, the user @TtonySt had also retweeted one of @UncleAhBoon's tweets[13]. The name is also similar to Ah Boon—possibly Ameera Arini's sockpuppet identity—one of the names linked to the meera_rin@yahoo.com email in the Beruang Biru dataset as described in Chapter 3.

[12] A Twitter user also claimed that his photo had been used for the same purpose, according to news portal Cilisos (Uihua, 2016). The tweet is accessible at: https://twitter.com/Attnuor/status/752056476189941761
[13] The tweet in question can be viewed at: https://twitter.com/TtonySt/status/302281098216480768

The time period in which these sockpuppet accounts were opened (@UncleAhBoon's account was also created in February 2012, like some of the other cybertroopers in the sample of 31 accounts) matches the testimony of self-confessed former cybertrooper Syarul Ema Rena Abu Samah, who claimed in an interview published by *Wired* magazine, that her network of 80 cybertroopers themselves were managing thousands of sockpuppet accounts by 2013, the year of the general election (Guest, 2018). Sockpuppet accounts on social media do not just provide a mask for users to hide their identities; their existence also speaks to the current discourse on the use of bots in the manipulation of online sentiment worldwide.

That several email accounts using the name Beruang Biru were created pseudonymously to hide the identity of those behind the emails and instructions in itself speaks to the covert nature of cybertrooping, and its reliance on sockpuppet accounts. But even within the Online Deployment Strategy directions, there are indications that Beruang Biru's instructions were targeted at an extensive team of cybertroopers who may serve different purposes. While most of the emails came across as speaking to each respective recipient as individuals, there were also indications that some of these instructions were aimed at people who manage Twitter accounts beyond their own personal ones, such as the official social media accounts of Ministers and government officials.

7.3 Conclusion

This chapter has offered insights into how much planning and strategising goes into the mobilisation of cybertroopers, which can be used as indicators of the extensiveness of cybertrooping operations. It further argued that cybertroopers are a

part of Barisan Nasional's larger communication machinery, and that the instructions from Beruang Biru are tacit instructions aimed at helping the coalition secure victory at the 13th General Election. These operations are often conducted covertly, allowing for an element of plausible deniability. This covert nature of cybertrooping—or deception, returning to the framework presented in Chapter 2—is most useful in countries like Malaysia, which use the veil of democracy for political legitimacy. It would be detrimental to its public image if the government was found to be manipulating its citizens for personal gain, especially when it is likely that public funds are involved through the blurring of the state and party[14]. The discussions in Chapter 5 already illustrate how opposition parties have attempted to capitalised on this; indeed, then-opposition party DAP was the first to accuse BN cybertroopers of bad practices. This could explain why Barisan Nasional leaders tend to frame their use of cybertroopers within the context of good practices such as correcting lies and defending themselves against slander. In this regard, how cybertroopers are mobilised is no different from psychological operations, which explains why the Edward Snowden leaks of the covert military involvement in online manipulation of information in the United States and United Kingdom was such a scandal in the historically liberal countries. This sort of deception is widely considered as undemocratic and illiberal when used against one's own citizens.

The second part of this chapter presented an extended typology of strategies and tactics cybertroopers use in conducting their tasks based on the directions from Beruang Biru. This typology is evidence that cybertrooping goes beyond merely the dissemination of information (or astroturfing)—whether positive propaganda or

[14] There is also evidence of the Prime Minister's Department organising workshops for cybertroopers, based on documentations given to me in confidentiality by one of its participants.

attacks on the opposition—and includes a variety of activities based on amplification and volume to impact public perception of Barisan Nasional or its opponents. This chapter has shown that these approaches used by cybertroopers are not always mutually exclusive, and are often used together in ways that best serves to achieve their goals.

This chapter also extends the discussion of how cybertrooping activities can be considered within the framework of online manipulation of political communication presented in Chapter 2. The discussion on spamming and the use of memetic signifiers further contributes to the understanding of dissemination and defence, which was covered in Chapter 6. Activities such as trolling and brigading show that there is more to demonisation and disruption than just negative propaganda being distributed by cybertroopers. Hijacking hashtags too can be considered a form of disruption, but it also serves as a technique for distraction. Hashtags used as a priming tool can transcend the categories and be used for demonisation or distraction. That is to say that the execution of these strategies can be considered to be fluid, depending on the objectives and goals of the particular task at hand.

The discussion in this chapter also illustrates how internet affordances and cultures can be taken advantage of, such as with the exploitation of hashtags, the manoeuvring of online ranking systems through brigading and the ephemeral nature of online identities.

CHAPTER 8

Shades, themes and performance styles: Messaging Strategies

This chapter focuses on the cybertrooping messages in the datasets that make up this study, and will be presented in two parts. First, it unpacks Beruang Biru's categorisation of its 'Materials' into different shades (white, grey and black) in emails using the Online Deployment Strategy template. Secondly, it discusses the specific messages in those emails as well as those found in the instances of cybertrooping from the Bersih datasets to understand better the messaging approach used by cybertroopers.

In the first part, I test the data against two hypotheses: first, against the similar shades scholars have used to categorise propaganda, and second, using the descriptor 'controversy' found in the Beruang Biru emails. Following that, I will argue that the tone messages take on in the different shades reflect the 'message style' of a cybertrooper, whether to portray their public personas or to speak in the language of their audiences, and as a labelling mechanism to identify which materials are allowed to be used by whom.

The chapter then turns to the analysis of the messages found in the datasets. The objective of this discussion is not to examine the kinds of discourse that emerge from the dissemination and propagation of this cybertrooping content. Instead, it aims to present an understanding of how different message themes and approaches are used for the purpose of dissemination, defense, demonisation, disruption and distraction. The chapter will conclude by arguing that the approach to messaging adopted by cybertroopers, together with the other tactics discussed in Chapters 6

and 7, serve to manipulate the public into favouring Barisan Nasional and the government over the opposition and their supporters.

8.1 Beruang Biru's categorisation of shades

A prominent feature of the Online Deployment Strategy (ODS) template—described in Chapter 6—is the categorisation of "Material" according to shades of white (*putih*), grey (*kelabu*) and black (*hitam*). The emails in the dataset do not explicitly explain what these shades represent, although two instances which refer to them offered a starting point for further investigation. The first instance that alluded to what the categories mean was found in the email informing recipients to start expecting "daily" Online Deployment Strategy emails (22 February 2013). It then went on to discuss the categories:

> *Buat sementara waktu bahan-bahan berbentuk kategori putih (tidak kontroversi) akan banyak disebarkan. Selepas ini bahan di bawah kategori kelabu dan hitam juga akan dihantar bergantung kepada situasi.*
>
> [For the time being, only materials categorised as white (not controversial) will be distributed. Subsequently, materials categorised as grey or black will also be sent over depending on the situation.]

In the email, Beruang Biru does not make it clear in the email what it means by "not controversial". The process of interpreting that description is made more complex by the several instances where materials were categorised in pairs, such as white/grey and grey/black.

The other hint as to what the shades might mean was in the instructions for those managing "official accounts" not to disseminate certain messages in the emails. Specifically, the instructions were for these accounts to not post any material categorised as grey or black. The following notice (written in the email in red colour) was found in the Online Deployment Strategy email on 29 March 2013.

> *PERINGATAN PENTING*
>
> *Mohon kerjasama tuan/puan yang mengendali akaun rasmi Twitter, Facebook, website atau laman blog rasmi milik Barisan Nasional/parti komponen/menteri dan timbalan menteri/ahli parlimen/jabatan kerajaan/ketua jabatan agar TIDAK MENGGUNAKAN bahan di bawah kategori KELABU / HITAM.*
>
> *Akaun-akaun rasmi hanya boleh menggunapakai bahan di bawah kategori PUTIH sahaja.*
>
> [IMPORTANT REMINDER
>
> To those of you handling the official Twitter, Facebook, website or blog accounts belonging to Barisan Nasional/component parties/ministers and deputy ministers/members of parliament/government departments/head of departments, your cooperation TO NOT USE the materials categorised as GREY/BLACK is requested.
>
> Official accounts may only use materials categories as WHITE.]

To investigate this categorisation of shades further, the 73 Online Deployment Strategy emails[1] in the Beruang Biru dataset were analysed. Each of these emails feature between one and 10 'Topics' (as labelled by Beruang Biru), some numbered more explicitly than others[2]. These 'Topics'—289 in total in the sample set—tended to form the basis of the talking points prepared by Beruang Biru for cybertroopers. The scripted messages previously discussed in Chapters 6 and 7 are presented under each 'Topic' as categories of materials. The content in each category were essentially scripted messages presented in bullet points, usually written in the length of a tweet. Most of the materials were categorised as white, with grey/black being the second most commonly used, as Figure 8.1 illustrates. The other three categories were found infrequently.

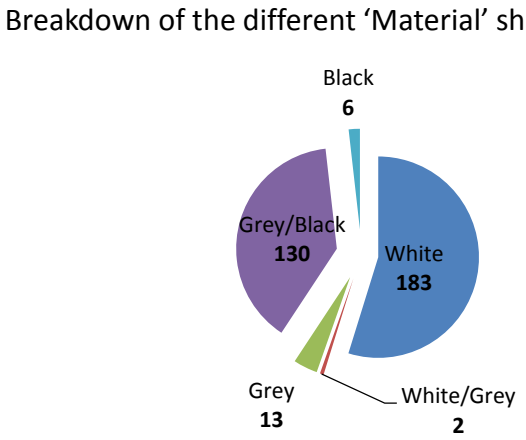


Figure 8.1: *Breakdown of how many different shades were allocated within the 287 'Topics' in the 73 emails sample*[3].

[1] There were 76 such emails in total in the dataset. However, three of them were duplicates, leaving 73 emails for analysis.

[2] In the case of the Chinese topics, they were presented in the emails as a separate set of instructions from the Malay or English ODS. However, for the purpose of this dissertation, I included them in the count of topics per email.

[3] A note on the number of 'Topics': Figure 8.2 illustrates an example where the 'Topic' was for the dissemination of external links; each link was allocated a different shade. Where there were multiple links with the same shade, I only coded that shade once because they were all listed in the same 'Topic'. This decision was made for consistency with the regular talking point 'Topics', which did not have a particular category of shade (or a combination e.g. white/grey or grey/black) appearing more than once each.

In the cases where an email did not include any material categories, Beruang Biru allocated the 'Topics' themselves with a shade. Not all 'Topics' featured talking points, however; some were just a list of links to other websites or online videos, or images, for distribution (*Pautan untuk sebaran*), as Image 8.1 illustrates.

4) Cadangan sebaran pautan, poster & video

- **Pautan:**

i) Don't even think of causing trouble on polling day, warns EC chairman (PUTIH)

ii) Mahkamah: Keputusan UPSI gantung Adam Adli sah (PUTIH)

iii) Budak kecil disepak, penyokong PAS ganas macam Israel (KELABU)

- **Video:**

i) Azhar Sulaiman sindir Pakatan & Anwar (KELABU / HITAM)

ii) BNYV 2012: No matter who you are - take Charge, make a Difference! (PUTIH)

iii) Najib Razak : Lawatan Ke PDM Seksyen 18 Barat 1 Shah Alam Parlimen Kota Raja (PUTIH)

iv) Husam Musa mungkin jual Putrajaya (PUTIH)

Figure 8.2: *A screenshot of an ODS topic (translation: #4 –Suggestions of links, posters and videos for dissemination). The image shows that each link is unrelated to the other, and how each is allocated a shade. There are also instances where a few links are listed under a particular category (shade) instead of individually.*

Due to the complex way Beruang Biru had used the shades for categorisation, and without a reference as to what "not controversial" means, I test them against two hypotheses. I begin with the propaganda hypothesis, considering how closely cybertrooping is linked to that information manipulation technique, and because the shades mirror those used by some scholars to categorise forms of propaganda as well.

8.1.1 *Beruang Biru's shades and the propaganda hypothesis*

One way to interpret the categorisation of materials by Beruang Biru is through existing understandings of propaganda, which some scholars have broken down into the same three shades as discussed in Chapter 2. It is possible to test this hypothesis in two ways. First, the shades of propaganda can be understood as referring to the transparency behind its dissemination: white for when its origins are known, grey when this is not clear, and black for when it is made to look like it came from the party it seeks to discredit. Beruang Biru taking this approach is a plausible interpretation of its use of shades considering that official accounts—publicly identifiable as associated with the government of Barisan Nasional—were only allowed to use materials categorised as white.

However, if this was the primary purpose of the categories, then it is arguable that Beruang Biru only needs two: one to reflect which materials can be used by official accounts and which can't. Factored alongside my assertions in earlier chapters about how the people managing official accounts are not the primary target of the Beruang Biru emails, it is reasonable to argue that these categories were not created specifically to deal with such material selection issues. This is not to say that the categories cannot be used for this purpose, as I will elaborate on in Section 8.1.3, but the point of this argument is that the categories were not distinctively created to indicate which material can be used by official accounts. This is further supported by the analysis of the 22 February 2013 email informing recipients that only materials categorised as white would be distributed for the time being. What is implied in the email is that the categories are created for all recipients, both the people behind official and non-official accounts. The association of shades to the transparency of

the material source is also doubtful because cybertroopers already operate covertly, and as such, the materials they disseminate cannot be considered as conventional white propaganda.

The second way to test the hypothesis is to view the shades within the context of truthfulness, where white concerns generally truthful and factual messages, black refers to disinformation, and grey is where the two blur. This can be done by examining the materials marked as black. In most cases, there did not appear to be any obvious lies or deceit within the content of the material. Take the email from 27 February 2013 as an example. Within the links categorised with a shade, the one item that had been singled out as black was a short YouTube video showing people wearing cut-out masks of leaders from the parties that make up the then opposition pact Pakatan Rakyat in a *Harlem Shake* internet meme[4]. The meme had become an internet sensation around the world at the start of that month, and involves people dancing to a short video of the song *Harlem Shake*, with people from around the world—including politicians, celebrities, and corporations—having contributed to make the meme go viral (Soha & McDowell, 2016).

Where the version distributed by Beruang Biru is concerned, there did not appear to be any explicit disinformation in the video. It did, however, feature references to some issues that Pakatan Rakyat appeared to be at odds about including the 'Hudud issue' related to the Syariah (Islamic) laws[5]" in Malaysia; contention as to whom is the pact's choice for Prime Minister; and the infighting within DAP. The video ended

[4] The video is available at https://www.youtube.com/watch?v=ht5pte4yitg

[5] References to the 'Hudud' issue in Malaysia refer to PAS's push for the implementation at Federal level of a particular type of enforcement in the Syariah (Islamic) laws. The law was already passed in the PAS-controlled state of Kelantan in 1990s, but was not ratified by the Federal government. It "included a section on *hudud* offences such as wine drinking, apostasy, unlawful sexual intercourse (*zina*), robbery and accusing someone of *zina",* with some critics claiming that the laws are draconian and inhumane (Osman, 2017, p. 10).

with the actor impersonating then-opposition leader Anwar Ibrahim dancing naked wearing only a towel, seemingly referencing the alleged sex video he had been associated with. It is plausible that the *Harlem Shake* video was created to leverage on a popular meme—and by extension, drawing more attention to it—as a way to troll members of the opposition seemingly 'for the lulz'. It could also have served as a priming tool to remind the public of Pakatan Rakyat's 'flaws'. While there was a significant element of propaganda to the content—the issues highlighted in the video have been played up by Barisan Nasional to show discord within the opposition parties—there were no explicit lies involved.

Similarly, "posters" that were flagged for distribution categorised as 'black' by Beruang Biru also did not include any direct indications of deceit, although elements of spin and emotional appeals were found. Figure 8.3, for example shows Wong Tack, a DAP candidate at the 13th General Elections, appearing to be angry Lynas Ltd., the Australian rare-earth mining company operating in Malaysia.

Figure 8.3: *An online poster for distribution categorised by Beruang Biru as 'black' in an ODS for 25 April 2013.*

The claims made in the poster features an accurate quote attributed to the DAP candidate; he has reportedly apologised for making that statement ("Wong says sorry over 'burn Lynas' threat," 2013). Setting a photo of Wong against a picture of a building on fire and describing his words as a threat is an example of negative spin aimed at invoking an emotive response against him. This use of the emotional appeal in spin can also be seen in Figure 8.4, which refers to a point in Pakatan Rakyat's manifesto for the 12th General Election in 2008 with regards to giving an allowance to single mothers. The pact repeated this promise in its manifesto for the 13th General Election. In the poster, a picture of a woman crying accompanies a real news article reporting that 3,011 single mothers had sued the PKR state government in Selangor, implying that the public has been lied to.

Figure 8.4: *An online poster for distribution categorised by Beruang Biru as 'black' in an ODS for 6 April 2013.*

The three examples above do not include outright lies, but instead use spin—with the two posters—and the seemingly crass and unsophisticated use of a meme for priming—with the *Harlem Shake* video. All that said, where truthfulness is concerned, these materials would not fall under what is conventionally understood as black propaganda. In addition, the fact that many of the 'Topics' in the emails include more than one category shade of materials also suggests that the shades used by

Beruang Biru do not refer to facts or disinformation[6]. As such, I turned to another possible hypothesis to interpret the categories: to test the descriptor "controversial" used by Beruang Biru by taking it at face value.

8.1.2 *'Controversial' decisions for categorisation*

To test this other hypothesis, I began by examining specifically materials categorised as white. Within this category were some positive propaganda 'Topics' such as the release of Barisan Nasional's manifesto (18/4/2013); boasting the size of the crowd at Prime Minister Najib's rally (22/4/2103); or his announcement to increase the salary of civil service personnel (12/3/2013). As they stand, these examples can rightly be considered "not controversial". However, the investigation also showed that some other 'Topics' involving more negative propaganda such as the demonisation on the opposition (as opposed to the positive propaganda examples above) were also categorised as white.

One such example was the 'Topic' found in the Online Deployment Strategy sent on 29 April 2013 aimed at pushing the claim that the Democratic Action Party (DAP) and Malaysian Islamist Party (PAS)—both of whom were part of Pakatan Rakyat, the pact of opposition parties—were at war with each other due to disagreements about the Hudud issue[7]. This was in spite of the policy pushing for the implementation of the laws having been put on the backburner by the pact ahead of the 13th General

[6] This is not to say that cybertroopers do not engage with disinformation. However, the verification of accuracy of the thousands of different materials provided by Beruang Biru is not only beyond the scope of this study, but also seemingly impossible due to the complex nature of 'truth'. The analysis presented regarding black category materials in this section, however, suggests that the shades are not directly associated to truthfulness.

[7] DAP's secular policies meant that they disagreed with PAS's previous attempts at pushing for this specific implementation of the Syariah laws.

Election (Tayeb, 2013). Barisan Nasional had been capitalising on this rift—whether perceived or otherwise—during the election campaigning period including placing political advertisements in newspapers that a vote for DAP is a vote for PAS and its policies on Hudud[8]. The reference to Hudud in the *Harlem Shake* video was likely highlighting this fracture within the opposition pact as well.

In the email, the 'Topic' headline read: "*DAP & PAS terus-terusan bertelegah*" [DAP and PAS can't stop fighting]. No "Material" category was included in this email which meant that scripted messages were not offered; instead, the 'Topic' in itself was labelled as white and bloggers were told write their posts in their "own style". The instructions also requested the distribution of links and images, one of which can be seen in Figure 8.5.

Figure 8.5: *An online poster for distribution categorised by Beruang Biru as white in an ODS for 29 April 2013.*

The issue of Pakatan Rakyat parties getting along was also raised in another Online Deployment Strategy email (25 April 2013). Figure 8.6 features the leaders of Pakatan Rakyat's three main parties—PKR, DAP and PAS—engaging in a boxing match with

[8] This further supports arguments I've previously made about how cybertroopers are part of a larger communication strategy by Barisan Nasional that transcends the digital space.

the caption, "Can they get along?", to make the point that the opposition are not united and therefore, not fit to govern.

Figure 8.6: *An online poster related to infighting in Pakatan Rakyat for distribution categorised by Beruang Biru as 'black' in an ODS for 25 April 2013.*

As with the earlier image featuring Wong Tack's 'threat', Figure 8.6 was also categorised as 'black' although it did not feature any factual inaccuracies. In addition, the key message in this poster is similar to other instances where Beruang Biru has spun the supposed rift in Pakatan Rakyat which were categorised as white, despite it being a contentious claim. The opposition pact had, after all, released a manifesto ahead of the elections which did not include policies related to Hudud ("Manifesto Rakyat: Pakatan, the People's Hope," 2013).

That both positive propaganda and attacks can be categorised as white suggests that the shades are not associated with how contentious Beruang Biru considers some of its claims to be. As such, these examples dismiss the likelihood that shades are related to extent of contention or valence where issues being highlighted are concerned. Most significantly, even topics which can be considered sensitive and controversial in Malaysia have been categorised as white. This can be seen from the

example of the Online Deployment Strategy for 2 May 2013, where the first topic involved the issue of Saiful Bukhari Azlan and his accusing Anwar Ibrahim of sodomy, which had eventually landed the latter in jail on those charges. A previous ODS which touches on the same issue (5 April 2013), but with a different talking point, was labelled Grey/Black, further suggesting that how "controversial" an issue is does not intrinsically mean it is categorised based on a particular shade. This led me to revisiting the material to examine if the shades have anything to do with the way the messages are presented by cybertroopers to fit the public personas they adopt.

8.1.3 Beruang Biru's shades as message style

Returning to Figures 8.5 and 8.6, which essentially addresses the same talking point, it is possible to argue that where the content between the two differs is in the way that they are presented. With the former, the quotes attributed to the respective party leaders featured in Figure 8.5 are reportedly accurate, although the larger claim of the implementation of Hudud can be considered spin. This claim was also one that featured in other media, indicating that it is not a one that Barisan Nasional was shying away from. This could potentially explain why this particular piece of material was categorised as white. Although Figure 8.6 speaks to the same talking point, the presentation of the poster—superimposing the bloodied faces of the leaders onto the bodies of random boxers to illustrate infighting—could be seen as inappropriate campaign material—a product of 'dirty politics'—and as such, should not be distributed by official accounts.

The contrasts between the posters above are able to be interpreted in two ways, which can help build the understanding of what Beruang Biru means by its categorisation. In the first way, I posit that the shades used by Beruang Biru are related to how the messages are presented publicly. To describe this, I crafted the term 'message style', borrowing from the field of linguistics where the term 'linguistic style' is "implied and described by such labels as 'baroque', 'impressionistic', polyphonic', 'serene', 'colloquial', 'formal', etc." (Sandell, 1977, p. 6)[9].

A 'Topic' from the Online Deployment Strategy for 26 February 2013 can be used as another example to further illustrate this point. The first one is titled "*Mematahkan Manifesto 'Pakatan Harapan Rakyat'*" [Demolishing the 'People's Alliance of Hope' Manifesto]. Where politics is concerned, such a topic can come across as mundane; after all, it is normal in any elections to dismiss the manifesto of one's opponents. For this topic, Beruang Biru categorised eight talking points as white, and 10 as grey/black. Among those categorised as white are:

> *Pakatan terus menjadi bahan kritikan apabila manifesto mereka dibidas sebagai tidak praktikal dan bakal memufliskan negara.*
>
> [Pakatan continues to be subjected to criticism after their manifesto is slammed for being impractical, and likely to bankrupt the country.]
>
> *Bagaimana Pakatan akan membiayai janji-janji manifesto mereka? Jawab dulu please.*
>
> [How is Pakatan going to afford to fulfil their manifesto promises? Please answer.]

[9] It is worth noting that there exists other terminology in the field of linguistics that could equally be used such as 'register' or 'genre'. However, to make such a nuanced distinction will require studying the material from a linguistics perspective, which is beyond the scope of this dissertation. I opted for 'style' because the description offered in the text above comes from a book looking at the relationship between linguistic style and persuasion (Sandell, 1977), the latter of which is within the realm of this study.

The style of these messages comes across as rational and appropriate, appearing to be reasonable conversations about politics in a mature democracy highlighting the impracticalities of the opposition's manifesto by questioning its fiscal feasibility. Presentation wise, they are written seemingly formally, with the correct punctuation. The messages categorised as grey/black from the same email 'Topic', however, use a more informal and aggressive style despite addressing the same mundane topic:

> *Sekali lagi Pakatan keluarkan janji-janji palsu – versi baru yo!*
>
> [Pakatan makes false promises again –new version yo!]

> *Semua benda nak kasi free? Kau dok dalam syurga mana neh?*
>
> [Want to give everything out for free? Which kinda heaven do you live in, eh?]

The use of 'yo!' in the first message, and "*nak*" [want], "*dok*" [short for *duduk*, or live in] and "neh" indicate a colloquial approach to the messaging. The messages are stripped of proper arguments; they replace the realities of funding the manifesto to a simplistic "free", and as "false promises". Comparing both examples, all four messages attack the opposition on the same issue, casting the same doubt but taking on a different styles. With the grey/black examples, they do not rationally discuss fiscal responsibility. Instead, they turn to the use of rhetoric to elicit an emotional response from the public and the use of name-calling by insinuating that supporters of the manifesto are stupid, that that kind of "heaven" does not exist.

To contrast the above example with a more sensational and thus possibly "controversial" topic, the Online Deployment Strategy email for 14 March 2013 can be used. The topic in question relates to a police report made by the political

secretary of a PKR MP claiming to have received threats from those close to party president Wan Azizah Wan Ismail, who is also the wife of Anwar Ibrahim. The political secretary had allegedly written a letter to PAS president—a partner alongside PKR in Pakatan Rakyat—stating that Wan Azizah is jealous of his close relationship to Anwar. That Beruang Biru offered scripted messages for two categories—white and grey/black—for an issue that can be considered a scandal further supports the earlier argument that shades cannot be intrinsically linked to how controversial a talking point is.

A comparison of the materials in the two categories, however, shows again how both take on different styles despite addressing the same topic, and intending to portray Anwar and Wan Azizah negatively.

Table 8.1

Comparison of the material categorised as white and grey/black in the ODS for 14 March 2013.

White	Grey/Black
Mohd Fareez membuat laporan polis kerana bimbang keselamatan beliau diancam ahli-ahli PKR. [Mohd Fareez has made a police report because he fears for his safety following threats from PKR members.]	*Apa pulak lagi ni? PKR tak habis-habis dengan anak-anak ikan.* [What now? PKR's issues with toyboys are never ending.]
Beliau yakin beliau sedang diburu oleh orang suruhan Dr Wan Azizah akibat surat yang beliau tulis kepada Hadi Awang. [He is convinced that he is being hunted by Dr Wan Azizah's people as a result of the letter he wrote to Hadi Awang.]	*Kesian pulak tengok budak ni. Siapa suruh kerja dengan Anwar?* [The kid looks so pitiful. But who asked him to work with Anwar in the first place?]

As in the earlier example of Pakatan Rakyat's manifesto, the messages categorised as white are written in a formal, almost news-presentation style. They could easily be interpreted as the presentation of facts. Those in the grey/black category, however,

are much more colloquial and harsher. Calling a young man allegedly close to Anwar a "toyboy" is a direct character assassination of a politician who had already served his time in prison on 'trumped up' sodomy charges. The second example puts the blame on the political secretary himself as a veiled attack on Anwar in direct contrast to the way the white category messages were spun. These two examples show how the same talking point can be presented differently. Offering such options to cybertroopers allow them to select either the ones that most represents their own voice to fit their public persona—whether authentic or made up, especially where sockpuppetry is involved—or the ones that will speaks best to their audiences or elicit an emotional response in favour of Barisan Nasional.

The argument related to performance styles above also raises the issue of which material is more suited for whom to use. This can be tied back to earlier discussions about how shades are not specifically created for the purpose of labelling talking points that can be used by official accounts. For instance, Beruang Biru has already been explicit about how official accounts should only use white material, suggesting that these accounts should not be associated with the negative styles and spin associated with the grey or black categories. To use these latter two categories would expose Barisan Nasional for the kind of gutter politics it expects of its cybertroopers—a nod to the use of third-party groups and proxies to say things they cannot, as discussed in Chapter 7—which is not what legitimate democracy looks like.

To illustrate this, the example from a 'Topic' in the 16 March 2013 email can be used. It relates to the death from a heart attack of Perumal Balasubramaniam (also known as PI Bala), a private investigator who had in 2008 controversially retracted a

statutory declaration he made 24 hours prior linking Prime Minister Najib Razak to the murder of a Mongolian model ("PI retracts declaration," 2008). Following his death, rumours that Najib and his wife were involved in his death started circulating. Even PI Bala's wife, A. Santamil Selvi, made those accusations, although she attempted to retract them three years later[10] (Kanyakumari, 2016).

The 'Topic' categorised its materials in two categories: grey and black. Consistent with the examples presented above, all four scripted text in the black category took used an informal and colloquial style. The spin was extremely negative as well, and targeted not just supporters of the opposition ("Pakatanis will spin ANYTHING including death[11]", emphasis in original) but also the deceased. One tweet, translated from Malay, read: "This is what you get for messing around with swearing" ("*Jangan main2 dengan sumpah. Kan dah kena*"). This likely refers to PI Bala's swearing on a holy book that his original statutory declaration—linking Najib to the model's murder—was true. Message styles not appropriate for legitimate political discourse aside, the vulgarity of suggesting that divine retribution caused the private investigators death makes it clear why these messages were categorised as black.

However, why Beruang Biru categorised the message "Condolences to the family of PI Bala" ("*Takziah kepada keluarga PI Bala*") as grey—the only scripted text provided for that category—is less obvious. It would be a difficult task to read that message in a negative light; the message style is formal, and there is no sign of spin. In regular circumstances, a condolence message like this would be categorised as white. This

[10] I use the term 'attempted' here due to the complexity of the case. The press conference where A. Santamil Selvi apologised publicly to the Prime Minister and his wife, and retracted her accusations, was in itself controversial. At the session, she seemingly retracted her apology, and then walked out midway through being questioned by journalists. A video of the press conference can be found on YouTube (https://www.youtube.com/watch?v=FgyTOiuR7E8).

[11] It was not possible to ascertain if there were indeed accusations on social media of foul play, or if this was just the cybertroopers spinning a message.

suggests that the death is something that Barisan Nasional does not want associated with them directly, and as such, was placed in a category that official accounts do not use—an indirect feature of the categories. This is plausible because the extent of the allegations, and the unanswered questions related to both deaths over several years meant that this was an issue that the opposition had tried to capitalised on, and not one that Najib wanted to address.

There were also other instances where Beruang Biru used the grey category for talking points that Barisan Nasional would not want directly linked to them. For example, an April 30 2013 email featured a link to a post by blogger Syed Akbar Ali who claimed that the Bersih rally in 2011 was organised with the support of the United States' Central Intelligence Agency (CIA)[12]. Beruang Biru mentions that these "negative foreign elements" ("*anasir-anasir jahat dari luar*") will cause similar "chaos" ("*huru-hara*") as Bersih if Pakatan Rakyat loses the 13th General Election. A few days prior to this email, Beruang Biru had sent another ODS using the grey category for claims that the opposition parties were attempting to beat Barisan Nasional at the elections with violence, citing the explosion near the BN operation room in Nibong Tebal in Penang as an example.

In both these instances, no evidence was given for the claims and as such, these are not accusations that Barisan Nasional would want to be directly associated with. Without evidence, these claims could be considered misinformation. That they were still labelled grey and not black supports the assertion earlier in this chapter that the shade categories used by Beruang Biru do not match those used to describe

[12] The blogger has since deleted all his blog archive, but a copy of the post in question was captured by the Internet Archive and available at https://web.archive.org/web/20130602083607/http://syedsoutsidethebox.blogspot.com/2013/04/polis-sila-ambil-perhatian-cia-bersih.html.

propaganda. Categorising the examples above as grey—taking advantage of the metaphorical murkiness of the shade—would mean that only cybertroopers would distribute such content. It is within this context that the descriptor "controversial" may be understood. It does not refer to how controversial a talking point is but instead alludes to the controversy that Barisan Nasional may generate from the dissemination of those messages, and so it is in the coalition's interest to stay away from such topics.

Granted, all of the contradictions presented so far in this chapter could well be the consequence of the people behind Beruang Biru themselves not having a clear system of categorisation, or that the labelling of shades was based on arbitrary decisions. However, considering how systematic Beruang Biru has been with all other aspects of their organisation, as Chapter 7 has argued, suggests that this is unlikely. While it is hard to identify intent dealing with data like these, what the analysis presented in this section suggests is that at the very least, the categories of different material allows cybertroopers to 'perform' their craft to unsuspecting publics in the ways that best suit their approach, personality and the transparency behind their partisanship.

8.2 Message directions and themes

Although sections presented in this chapter so far have been primarily aimed at testing various hypotheses to give meaning to the different categories of material found in the email, the discussions also included numerous examples of the types of messages that have been prepared by Beruang Biru for its cybertroopers to use. This section aims to move the discussion forward by presenting considerations on the

various message directions and themes found in the emails and Twitter datasets to further understand the approach to messaging that cybertrooper adopts. To do this I will return to the framework presented in Chapter 2, to analyse the messaging strategies used by cybertroopers to fulfill their roles through dissemination, defence, demonisation, disruption, and distraction[13].

8.2.1 *Dissemination*

Considering that the main objective of cybertrooping is to keep Barisan Nasional in power, all information distributed by cybertroopers should not be viewed in the same neutral way as the term 'disseminate'. Simply put, even the most seemingly benign message from them should be considered propaganda. This was clearly seen in all the materials—text, images and video—found in the Beruang Biru emails, which were pro-Barisan Nasional, whether by putting a positive spin in favour of the coalition, or by criticising their opponents.

This section describes instances of propaganda distributed specifically to reflect positively on Barisan Nasional and the government. As would be expected during a campaign period, there were many instances of messages being pushed by Beruang Biru related to Barisan Nasional's manifesto and the strength of the coalition's candidates. Besides these, there were two other kinds of messages that could be labelled as positive propaganda. First, there were messages of praise towards Barisan Nasional, particularly with regards to non-valance issues, where voters choose based

[13] Deception is not explicitly examined as a category in this section for two reasons. First, the extent to which spin is used can be considered as a form of deception and as such, this criterion is pervasive throughout all five other categories. Secondly, the extent to which the messages and information disseminated are 'factual' or 'true' is complex and requires extensive examining and fact-checking, and does not fit within the scope of this study.

on "on the perceived competence of the parties and their leaders" (Johnston & Pattie, 2011, p. 284). One clear example was found in the 5 April 2013 email, which asked cybertroopers to bring attention to the 100 biggest achievements by Najib during his tenure as Prime Minister. These include the setting up of affordable clinics across the country, introduction of numerous wealth distribution initiatives, and the so-called liberalisation of some repressive laws.

Secondly, there were also 'factual reporting' messages playing up Barisan Nasional's success. Among these were messages highlighting opinion polls favourable to the coalition (4 April 2013; 2 May 2013) and research reports such as the one by Deutsche Bank Market Research, which—according to Beruang Biru—listed Kuala Lumpur as one of the most affordable cities to live in and visit. How the latter can be linked to politics is through one of the scripted messages, which translated from Malay, reads: "Malaysia's peaceful socio-political environment and progress under Barisan Nasional continues to draw the attention of foreign tourists". However, there is a heavy element of spin involved in this statement, considering that the results in the report were based on a "simple survey of prices and price indices of a wide array of goods and services from around the world", and not directly crediting government policies (Sanyal, 2013, p. 1). Kuala Lumpur was actually listed as "just as affordable" as the cheapest cities for a weekend getaway, Mumbai and Delhi (p. 1).

There were also instances of positive propaganda distributed by Beruang Biru, which initially seemed unrelated to politics. On 9 March 2013, one of the 'Topics' for the day was to support the country's badminton champion (since retired) Lee Chong Wei's advancing into the semi-finals of the All-England Open Badminton Championships. This request was especially unusual because Lee had competed in

the finals of the championships for four consecutive years before then, winning twice, and as such, making it into the semi-finals wasn't such a notable achievement. While such content may appear harmless, this form of positive propaganda can be considered more insidious because it doesn't directly link itself to politics. It is likely that Beruang Biru is tagging onto Lee's success as the nation's success, which also reflects well on Barisan Nasional. The blurring of state and party in Malaysia lends itself to this, and in the larger context of cybertrooping as a practice, this is an especially useful approach when cybertroopers are state-sponsored.

8.2.2 *Defence*

Messages that are used for defence are seeded out in the same way the positive propaganda is disseminated. However, there are two key differences between the two. First, the kind of talking points featured in the messages are different; in the context of defence, they are usually written in response to a sentiment or claim that is already circulating publicly. Second, unlike positive propaganda material, which tends to be categorised as white (suggesting that they can only be performed in one way), options provided, and used, for defence can take on different message styles.

Cybertroopers were also found to be defending both party and the state, again alluding to the blurring of the two. With the Online Deployment Strategy that was received following Barisan Nasional's victory at the 13th General Election, the first talking point was in response to opposition leader Anwar Ibrahim's organization of a rally to protest the alleged irregularities of the elections. Cybertroopers were instructed to ask on social media why the Chief Ministers of the states of Penang and Kelantan—won by Pakatan Rakyat—accepted their posts if their parties did not

accept the results. While this 'Topic' comes across as Barisan Nasional defending its own victory, it was also implicitly speaking up for the Election Commission (EC)[14].

There was also evidence within the Beruang Biru emails of cybertroopers explicitly defending these Barisan Nasional-linked public institutions. For example, there was a more direct defence of the EC (25 April 2013), and also the Registrar of Societies (RoS), which intervened in DAP's 2012 internal elections in the weeks ahead of the 13th General Elections (19 April 2013). With the latter email, Beruang Biru was direct about the reason for addressing this issue—to respond and defend the RoS:

> In light of the ROS decision on the status of CEC (DAP) election yesterday, please help control the negative buzz on all internet platforms via directions stated in this email.

In the two instances of defending the EC above, the materials were categorised as white. The RoS materials however were as not labelled with a shade, although there was an explicit instruction for official accounts not to discuss the issue. This raises an interesting question about why the defence of one institution is allowed to be associated with Barisan Nasional, while another is not. It is plausible that defending the EC is seen as reinforcing the coalition's electoral success by calling out a flawed argument by the opposition, whereas to comment on the RoS would be seen as state interference, and raises legitimacy issues in a perceived democracy like Malaysia.

Moving forward to the tweets from the Bersih rallies, similar messages defending the EC were also found in the Twitter datasets responding specifically to the

[14] In Malaysia, the Chairman and Deputy Chairman of the Election Commission are usually appointed by the King, on the advice of the government. This means that the roles are essentially political appointments. Specific to the 13th General Election, both the Chairman and his deputy (who were in the role at that time) had previously reportedly admitted to being members of UMNO, although the deputy chairman later claimed that this was untrue (Shazwan Mustafa Kamal, 2012).

movement's call for free and fair elections in Malaysia. Examples of such tweets can be seen below, posted to engage with Bersih's list of eight demands to the EC for electoral reform.

> why have #bersih 3.0 when 7 out of 8 demands fulfilled? maybe only for thrill having street demos?!!
>
> There is really no pleasing ppl nowadays. 7/8 demands met and 18/22 recommendations agreed unanimously. Still want to #Bersih
>
> joining #bersih means u havent read the booklet printed by the EC explaining their excellent electoral reform effort.. dont join it!
>
> I hope #bersih people will read SPR [Electoral Commision] booklet first b4 embarking on this bullshit #bersih thingy

The logic used by Beruang Biru regarding leaders from the opposition parties accepting their victories but not Barisan Nasional's was also seen in both the #bersih and #bersih4 datasets. Take for example, the following tweets:

> our election is so #bersih that even some idiots from pakatan can win their election seat..hehe
>
> *Kalau PRU lps x adil x bersih mcm BN tak bleh kekalkan majoriti 2/3 di Parlimen selama 2 penggal?? #Bersih4 #changepenang*
> [If the Electoral Commission is not fair and clean, how come BN was not able to maintain it's 2/3 majority in Parliament for two terms?]

These are clear examples on how cybertroopers used defence as a messaging strategy to respond to claims that are seen to be critical of Barisan Nasional or the government. This can also be seen as a form of attack, albeit a more subtle and less invasive approach as compared to the instances that will be discussed next.

8.2.3 *Demonisation*

The analysis of cybertrooping content that could be considered as attacking in nature found three main targets: individuals (both politicians and civil society leaders), institutions (political parties or civil society groups) and the public (usually those seen as anti-government or pro-opposition). Depending on who the target is, the messaging approach differed.

Where political personalities are concerned, cybertroopers engage in what can be considered systemic attacks, at times resorting to 'character assassination' through name-calling and slander, to the extent of dehumanising the individuals. One clear instance was the messages attacking DAP leader Tian Chua found in a Beruang Biru email, in response to comments he allegedly made about the Lahad Datu insurgency[15]:

> "Tian Chua, are you still a human? Our army has sacrificed themselves and you call them mad dog drama? You are not human!"
>
> "DAP/PKR called our troop, who died, 'coward' who run away when they heard gun shot. These are not human. These are animals." (2/3/2013)

It was not possible to verify the facts of these accusations against Tian Chua, although he was later charged with sedition related to the incident for allegedly suggesting that UMNO was responsible for the insurgency (he has since been acquitted). Factuality aside, cybertroopers could have used a different approach to respond to his alleged comments such as by defending the Armed Forces in the same way they rebutted claims again other government institutions like the Election

[15] These were the English translations within the email itself of the "Chinese Online Deployment Strategy" material.

Commission or the Registrar of Societies. This suggests that these messages were intentionally crafted to demonise Tian Chua specifically. It is also possible to argue that these sorts of attacks are part of the cybertrooping playbook as there were many similar instances found within the Twitter datasets as well.

Ambiga Sreenevasan, who was chairperson of Bersih when the 2012 rally was held, in particular attracted a lot of attention from cybertroopers, to the extent that a hashtag was created specifically to target her. Tweets using the #dearambiga hashtag saw Ambiga's integrity as a prominent lawyer and former president of the Bar Council attacked. Those tweets refer to her as "irresponsible", someone who "love[s] the limelight", is "a lawbreaker", has "failed as a person" and more. This use of hashtags, like the #tolakTianChua one mentioned in Chapter 7, further supports the assertion that particular individuals are identified for systemic attacks. Other personalities who were picked on by cybertroopers on Twitter include Anwar Ibrahim as these tweets from the #bersih sample can illustrate.

> joining #bersih means u accept anwar with all his sexual tryst to be ur dirty leader.. dont join it!
>
> Anwar is a moron, #dearambiga is an oxy-moron but #bersih is the grand daddy of all super morons!
>
> if anwar is eager to be PM, then he doesn't have to call all foreign diplomats..its pre-emptive ..shame on u #bersih
>
> anwar n #dearambiga will need some botox injection since lotsa foreign media will focus on them on #bersih!

As leader of the opposition, it should come as no surprise that Anwar was a significant target by cybertroopers, whether during the Bersih rallies or during the election campaigning period. One Beruang Biru email specifically illustrates how

Anwar was being monitored for attacks, highlighting what it calls "an Anwar misstep" that could be "an opportunity for us" (16 March 2012). The incident, according to the email, was that Anwar was due to appear via Skype in a forum alongside Wikileaks founder Julian Assange. It alleged that political blogger Raja Petra Kamarudin[16] was meant to participate as well but was removed at the last minute following objections by Anwar. In referring to the two final speakers on the panel, part of the email reads, "So now the discussion will involve a suspected rapist with a messiah complex … and Julian Assange". This attack on Anwar Ibrahim is a clever dig at him and Assange, who both faced accusations of rape, with the former having served time in prison for sodomy[17] and the latter having taken refuge at the Ecuadorian embassy in the UK away from authorities until asylum was withdrawn in early 2019. Specifically, Beruang Biru mentioned that they were gathering more information on the forum to see if any form of online audience engagement would be incorporated into the event; if there was, "we should make sure they're bombarded with messages from people asking why Anwar is silencing his critics".

While this email clearly indicates some form of 'targeted trolling' being mobilised, it differed from the other examples presented in Chapter 7 calling for certain political personalities to be tagged and challenged on Twitter. In this instance, the Beruang Biru email included five suggested tweets[18] that could be used by cybertroopers although the email did not use the Online Deployment Strategy template—the email was sent almost a year ahead of the ODS being introduced—or categorise them using any of the shades. One of the suggested tweets even included a hashtag for

[16] Raja Petra Kamarudin was also a name listed in the organogram of PM Najib's alleged communication team presented in Chapter 6.

[17] Anwar has always claimed that these were politically-motivated trumped-up charges, and in 2018, received a Royal Pardon clearing him of his convictions.

[18] This direct mention of scripted texts as tweets was the reference point for my argument that the tweet-length materials in the ODS emails were indeed messages crafted for use on Twitter.

Anwar—#HypocritAnwar—which shows consistency in the way hashtags are used in tweets as a form of attack by cybertroopers.

Like with the messages vilifying political personalities, institutions such as the opposition parties were also subjected to a significant use of negative spin. This chapter has already discussed the efforts by Barisan Nasional generally, and cybertroopers specifically, to perpetuate the narrative that the opposition bloc Pakatan Rakyat was in disarray due to infighting among the political parties for different reasons such as ideological stance on Islamic laws and their choice of Prime Minister. The intrinsic link between politicians and the party they represent meant that cybertroopers could also attack both at the same time, as one example from the 'Ad Hoc' ODS on 23 April 2013 shows. In this instance, Beruang Biru suggested several possible messaging approaches cybertroopers could take. These involved spreading the sentiment that DAP preferred the Islamist party PAS's president Hadi Awang as Prime Minister over Anwar Ibrahim, the natural candidate for the role as opposition leader. This messaging fits not only into the Barisan Nasional spin of a rift between the parties, but also amplifies the narrative found in the ruling coalition's other media material that a vote for DAP is a vote for PAS. This is 'race-baiting' in action considering that DAP is seen as a party for the ethnically Chinese (despite its claims of being a multiracial party), who make up a large portion of the population who are generally critical of PAS for its Islamist policies.

However, Barisan Nasional does not only score political points by attacking political parties. Civil society groups such as Bersih and the Bar Council have also been targeted by cybertroopers, as the following tweets from the #bersih dataset demonstrates:

> bar council only know how to speak thru their asses praising pakatan n #bersih when they themselves r opportunist sharks!
>
> strange to know that bar council approves #bersih at dataran when it hasnt been approved by authorities..stupid lawyers!

Attacks on civil society groups are also, by extension, attacks on the public by virtue of who they claim to represent. Tying attacks on the public to a social movement like Bersih for example, is an efficient way of demonising a collective of faceless people seen to be anti-government. That is not to say that the language used by cybertroopers in addressing these publics does not get personal. In tweets, they were attacked by being called, among other things, "idiots", "fanatics" and "stubborn", all pejorative terms.

But more than namecalling, the cybertroopers' attacks on the public—in the context of Bersih, this would be protestors and those supporting them—tend to use the emotional appeal to score points by targeting values, morals and ideology. One way this is done is by using patriotism, which in Malaysia is predominantly linked to pride, love and compassion of the citizen's homeland as well as their willingness to defend national interest when threatened, attacked, ridiculed or humiliated (Bandu & Ahmad, 2015). In this sense, there are often overlaps with nationalism. As discussed in Chapter 4, one of the most significant ideologies used by past Barisan Nasional governments is the concept of multiculturalism, to the point where it has essentially been considered a source of national pride. However, the issue of race and religion is tense in Malaysia, which means that the concept of multiculturalism is arguably superficial.

This hasn't stopped cybertroopers from using this ideology to evoke an iconoclastic patriotism emotion to dismiss the Bersih movement. Numerous tweets explicitly state that the Bersih rallies are a threat to unity among the different races in Malaysia. Terms like "unity", "harmony" and "peace"—often associated with the problematic concept[19] of 'Asian values'—are commonly used in mainstream discourse surrounding multiculturalism in Malaysia. The example tweet below speaks directly to this issue, using the "tourist" as a vantage point to invoke patriotism through the need to defend our country against being viewed negatively (ridiculed or humiliated) by outsiders.

> #bersih has created total disharmony among peace loving malaysians according to many tourists.. so better cancel it now

While the message style from the example above stands in contrast to the following tweet, they appeal to the same issues of public perception of Malaysia, and conflates the idea of the nation and the state.

> *#bersih4 memburukan negara di mata dunia. #ubahpenang*
> [#bersih4 is tarnishing the country's image in the eyes of the world. #changepenang]

> *#doauntukmalaysia Harap #Bersih4 x menghuru-harakan negara #MalaysiaSelamat ##perlisboleh #perlisboleh*
> [#prayformalaysia Hope #bersih4 doesn't cause chaos in the country #MalaysiaIsSafe ##perlisboleh #perlisboleh]

These messages are consistent with what is known as the 'protest paradigm', which "refer to the pattern of delegitimizing news coverage of protest and dissent" (Lee, 2014, p. 2726). Within the Malaysian context, Yang and Ishak (2012) found that the media's coverage of the Hindraf rally in Kuala Lumpur to be consistent with

[19] Scholars have critiqued this concept as being used by some illiberal regimes for oppression and to maintain hegemony. See Subramaniam (2000) for an extended discussion on the debates surrounding Asian values and its place in liberal democracies.

understandings of the protest paradigm. Indeed, the datasets in this study also indicated that this could be the case; the tweet about tourists above is similar to the frame used in a 2015 article by the government-controlled national news agency Bernama featuring two tourists who attended the Merdeka Day (Independence Day) celebrations at Dataran Merdeka (Merdeka Square), ended with the following quote to further demonises street rallies:

> Despite many unexpected incidents such as the earthquake and airplane tragedies, *and even the rally yesterday*, you can see the joy on the faces of the people who are living in this country," they said. ("Tourists impressed with Merdeka Day celebration," 2015, emphasis mine)

This narrative—that rallies are dangerous—is one that has been perpetuated by Malaysian media for decades. Activist and academician Syed Hussein Alatas (1977) argued that the narrative that protests are not part of Malaysian culture is a misrepresentation because there have been examples of such acts of civil disobedience in the country's history dating back to the colonial period. What's more in recent years street protests in Malaysia—from the Reformasi protests calling for justice for Anwar Ibrahim when he was first arrested in 1998 to the Hindraf protest in 2007 following the demolishment of several Hindu temples in Malaysia to the numerous Bersih protests since 2007—have shown that peaceful protests and rallies can be successfully organised, that is, until the police brutality begins.

8.2.4 Disruption

The tweets above may be addressing the perceived disruption of the Bersih street rallies, but it is possible to make the case that like with character assassination and

party politicking, the main objective of demonisation as a messaging strategy is to score political points. In contrast, the following discussion instead focuses on messages that were crafted with the outright intention of causing palpable disruption, whether at an individual, institutional or societal level. These messages take demonisation one step further, and include an element of incitement, which has an almost tangible quality to it in the same way that acts of 'targeted trolling', 'brigading' and 'spamming' do.

It could, for example, involve physical threats as a form of attack (as opposed to the disruption of one's social media accounts). They could take on an implicit form, and target an individual like Ambiga, as the tweet below illustrated.

> #dearambiga should wear chastity belt when rally #bersih starts.. u dont want anything to happen do u hehe!

The tone of the tweet—seemingly like a joke—suggesting physical harm, including rape, is even more significant when considered alongside the fact that Ambiga has over the years reportedly been the subject of death threats for her activism work ("Ambiga gets death threats," 2011; Kamal, 2016).

However, it is not just political personalities that are subjected to threats. Cybertroopers also use their messages to intimidate and perpetuate fear among those who were planning to take to the streets.

> DBKL n PDRM[20] will have joint operation on #bersih 3.0! *tangkap aje n buang negeri pengkhianat2 negara ni!* [Just jail and exile these national traitors!]
>
> *Perlukah ISA dikembalikan utk ajar penganjur #Bersih4 #AgendaYahudi #S14*
> [Does the ISA need to be reinstated to teach organisers of #Bersih4 a lesson?]

[20] DBKL is the Kuala Lumpur City Hall. PDRM is the Royal Malaysian Police.

> prepare to face ur consequences #bersih demonstrators! court has barred u from entering dataran..u now have no rights to be there!

Years of social control by the Barisan Nasional governments have created a culture of fear in Malaysia, and the perpetuation of such narratives feed into the chilling effects that loom over the heads of most Malaysians. These messages amplify the BN government's declaration of the rallies as illegal and threats of arrest before the events actually take place in order to scare supporters and prevent them from showing up. This strategy also shows that cybertroopers do more than attack their opponents but also disrupt the lives of citizens by ensuring that the chilling effect is alive and well.

Cybertroopers are also able to disrupt the political structures in Malaysia through their messages. This chapter had already earlier discussed the way in which PAS and DAP have been pitted against each other as a way to demonise Pakatan Rakyat by spinning about the instability of the opposition pact. Above and beyond convincing the public to vote for the more 'stable' Barisan Nasional, this narrative can also lead to an actual fracture between the political parties. Even during the Bersih rally, cybertroopers took on the issue of political partisanship by making PAS seem like the outlier among supporters of Bersih. While there were indeed rifts within the opposition front at the time, the cybertroopers were clearly stoking the fire, as the following tweets illustrate.

> PAS needs to leave #bersih coalition n take ur members too.. anwar n #dearambiga is manipulating ur members everywhere!

> aiyoyo ambiga u r finished! PAS doesnt want anything to do with u... just quit being #bersih leader laa

I will relinquish my PAS membership if PAS didnt pull out from #bersih !

joining #bersih means u r associated with #dearambiga who has been rejected by PAS!.. dont join it!

Using Bersih as a tool, the cybertroopers were attempting to pile the pressure on PAS to pull out of Pakatan Rakyat. This worked to a certain degree; in mid-2015, the relationship between the parties has soured to the extent that DAP declared the opposition pact as essentially dead. By the time of the Bersih 4 rally, PAS had pulled out of the alliance. Without this huge Malay-Muslim support, Barisan Nasional was able to shift the narrative to suggest that Bersih was a Chinese-led rally (see Johns & Cheong, 2019). This development allowed cybrtroopers to continue using a similar strategy during the 2015 rally, emphasising the fracture to make the point that the opposition parties are weak without PAS.

The tweets below also show that cybertroopers are not just pitting two opposition parties against each other but are critical of both. It is clear then that the disruption agenda is to cause, and then perpetuate, a fracture in the opposition front, to score points for their political masters, Barisan Nasional.

#Bersih4 yahudi Bersih4 Penyertaan Bersih4 tidak mendapat sokongan drp PAS #PrkDr
[#Bersih4 jew Bersih4 Bersih4 did not get support from PAS #PrkDr]

Pas tak sertai bersih4 kerana mereka x bersih dan bershit #Bersih4.0 http://t.co/dBNMzkevvL @rajaretorik
[Pas did not participate in bersih4 because they are not clean and 'bershit'[21]]

#KNews #AgendaYahudi #Bersih4 akhirnya PAS sedar mainan DAP....yg dua 3 kerat Malayu yg p tu....memang tak tau apa...xkenal sejarah...

[21] "Bershit" was a common attack in the form of play on words against Bersih.

[#KNews #AgendaYahudi #Bersih4 PAS has finally seen through DAP's games…. Those few Malays that are on the street … really ignorant … not aware of their history…]

#Bersih4, digerakkan oleh DAP. PAS dah nampak kebenarannya. Bagaimana yang lain? #MalaysiaSelamat #MelakaMajuF2
[#Bersih4, mobilised by DAP. PAS has seen the truth. What about the rest? #MalaysiaIsSafe #MelakaMajuF2]

It is also worth noting that unlike the 2012 tweets, most of the #bersih4 tweets which play up the partisan politics sentiment used the Malay language. This was likely for the benefit of PAS supporters—the party's stronghold is in the less urban states of Kelantan and Terengganu and as such, English is not commonly used[22]—and also UMNO's nationalist base. Both these sets of people, in urban and non-urban areas, are primarily made up of Malay-Muslims, and are the ones most likely to be threatened by the 'Chinese' factor and DAP's supposed 'anti-Islam' agenda. It speaks very much to the racial (and religion) politics embedded within the discourse of partisanship in Malaysia.

These attempts by cybertroopers to pit PAS against DAP wasn't just about affecting the number of people going onto the streets to attend the rallies. The rift between the two parties and its impact on the rallies provided an opportunity to play up and trigger ideological stances of Malaysians related to race and religion, a tactic also used by the Barisan Nasional-owned media outlets (Moses, 2002). In particular, there is a sense among the Malays that the Chinese—with their dominance in the economy and education achievements—are a threat, leading the former to lose their 'rightful' place as the original people of the land (Noor & Leong, 2013). The sentiment is one widely felt because it is not just the Malays who feel threatened, particularly with regards to Islam as "its most potent identity symbol", but also the Chinese, among

[22] Bahasa Melayu is the medium of instruction in the national schools; English is taught as a subject.

other non-Malays who worry about the loss of their identities (Muzaffar, 2002, p.5 in Noor & Leong, 2013, p. 719).

This form of racial politics has tangible consequences to a society like Malaysia where multiculturalism shapes the social fabric of the country. This is even more pronounced considering that Malaysia's history is marked by a racial riot event in 1969 which caused the death of hundreds of people. Figure 8.7 illustrates just how the blatant efforts to racialise Bersih to score political points can be. Posted by a suspected cybertrooper—note the use of hashtags used by other cybertroopers—the tweet presents unattributed (and likely inaccurate) statistics on the racial breakdown of Bersih rally participants over the years ('M' for Malay, 'C' for Chinese), conveniently leaving out a large number of ethnic Indian Malaysians and those of other ethnicities.

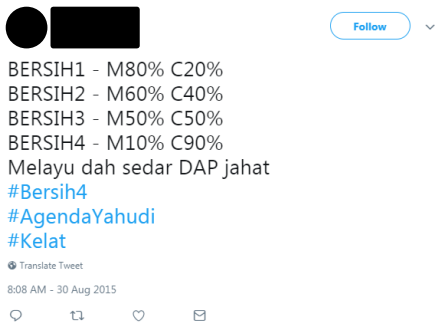


Figure 8.7: *A tweet with the alleged racial breakdown of street protestors at the various Bersih rallies. Note the text in the tweet "Melayu dah sedar DAP jahat" [Malaysia are finally aware that DAP is bad] is a clear attempt to make DAP synonymous with 'Chinese'.* The identity of the user has been blacked out.

Cybertroopers have also taken to perpetuating negative stereotypes through the use of racist lingo, including referring to non-Malays—especially the ethnically Chinese—as "*babi*" (pig), alluding that they are unclean because they eat pork[23].

[23] In Islam, eating pork is forbidden and considered not 'Halal'.

The following tweet shows how the term was used to both disparage Ambiga (who is ethnically Indian) and the Chinese, by using the racist hashtag #*babikuning* (#yellowpigs):

> *amBABIga selaku ketua #bersih seharusnya didakwa atas kesalahan gagal mengawal #babikuning sehingga menyebabkan kematian anggota polis*
>
> [amBABIga as the head of #bersih should be charged for her inability to control the #yellowpigs which has caused the death of a police officer[24]]

Between the talking points calling on the Malays to be cautious of the ethnically Chinese citizens in Malaysia demanding for equal rights, and the outright racist language used on supporters of Bersih, it is not far-fetched to argue that the messages sent out by cybertroopers contribute to the disruption of social life in the country.

8.2.5 Distraction

The discussion on memetic signifiers in Chapter 7 has already made the case for how content generated and disseminated by cybertroopers can be used for distraction. Specifically, the postings related to the #RespectMyPM campaign managed to divert attention away from the Save Malaysia campaign led by Mahathir Mohamad and other then-opposition members. It is not easy to apply intent, especially one as abstract as distraction, to the individual messages sent by cybertroopers. With the Beruang Biru emails, specifically, there were no explicit mentions of using distraction as a tactic to win the 'information war'.

[24] The reported death was an unfounded rumour that circulated during the Bersih 3.0 rally.

Having said that, it is possible to identify themes from the Twitter datasets from messages that cybertroopers posted that were not directly related to issue at hand. Whether or not distraction was the intention, the planting of these unrelated flags—including hashtags—in the messages can lead to that outcome. Unsurprisingly, the themes of these messages tapped into issues of ideology and values in the same way that other messaging strategies have adopted.

One clear theme used was the supposed 'Jewish agenda', which perpetuates religious ideology by linking it to anti-Islam sentiment. I have already described the out-of-context use of #AgendaYahudi in the #bersih4 tweets in Chapter 7, arguing that it served as a priming tool to associate the Bersih movements with the purported 'Jewish agenda'. The Malaysian obsession with the 'Jewish agenda' goes back decades to the early years of the first Mahathir Mohamad Prime Ministership. In the 23 years that he was in power, Mahathir had made several claims that have been considered anti-Semitic (Kessler, 1999).

He had claimed, for example, that the hostility his party faced from the foreign media was because of their Jewish (and Zionist) ownership. Protesting against what he found to be a seemingly overly sympathetic tone towards Jewish people in a movie set in Poland related to the Holocaust, Mahathir's government banned *Schindler's List*.

In 1997, Mahathir blamed the Jewish investor and philanthropist George Soros for his alleged role in the Asian economic crisis, according to reports:

> "We do not want to say that this is a plot by the Jews," [Mahathir] said, "but in reality it is a Jew who triggered the currency plunge, and coincidentally Soros is a Jew. It is also a coincidence that the Malaysians are mostly Muslim. Indeed, the Jews are not happy to see Muslims progress." ("Mahathir's Dark Side," 2003, para. 7)

Part of this anti-Semitism stems from the conflation of Jewish people and Zionists; Malaysia is strong supporter of the Palestinian state and have rejected formal relations with Israel (Yegar, 2006).

Over the years, these anti-Semitic sentiments have been reduced to two words, "Jewish agenda". This made it easy for cybertroopers to distract from whatever accusations against Barisan Nasional they were responding to by claiming that whatever was being referred to was part of a 'Jewish agenda'. One tweet referred to the rally as a proxy for Jewish people, while another claimed that Bersih 4 was part of the 'Jewish agenda' to "defeat Islam and cause chaos" in Malaysia. These were likely in response to allegations that Bersih had received funding from George Soros' Open Society Foundation. The former Bersih chairperson Maria Chin Abdullah, who was taken into custody under the anti-terrorism law Sosma, confirmed that the connection to money coming from an organisation funded by a Jewish man was part of her questioning while she was in detention (M. Chin Abdullah, personal correspondence, July 2, 2018). In this sense, Jewish people were being used as scapegoats by cybertroopers as a way of distracting from the issues of free and fair elections, and police brutality during street demonstrations.

Cybertroopers have also relied on other existing ideologies in the Malaysian psyche to contribute to the race and religion sentiment. Another ideological theme that cybertroopers latched on to was the negative impression of the Lesbian, Gay, Bisexual and Transgender (LGBT+) community. By associating Bersih with this marginalised community, cybertroopers were able to draw the focus away from the protestors' demands, and instead, brush them off as deviants or "sick people". The third tweet in the examples below specifically speaks to the homophobic trope surrounding homosexual activity in prisons, an indication of how the LGBT+ community is viewed in Malaysia.

> i think anwar n #dearambiga will be garlanded as heroes by LGBT communities, kudos to these sick people! stop #bersih now!
>
> joining #bersih means u agree with #dearambiga n anwar on LGBT rights n wanna them to flourish in malaysia.. dont join it!
>
> joining #bersih means u r eager to see ur fellow inmates in the lock up..hopefully it'll be an LGBT members hehe!

While the references to "LGBT" in the tweet above may appear to be plain homophobia, the issue in Malaysia is often linked back to religion. Although sodomy laws in Malaysia are colonial legacies, the arguments that tend to be made for the retention of such laws are due to morality and that it is forbidden in Islam (Cheah & Singaravelu, 2017).

The final theme identified from the Twitter datasets returns to the protest paradigm discussed in the previous section. Specifically, cybertroopers use the emotional appeal—tugging at heartstrings and use of guilt—to distract from the core issues that Bersih is protesting by talking about the implications of street protests. While some

of these messages also serve similar purposes as those sent out to demonise Bersih, they do not specially attack the movement. Instead, the messages ask the public to consider the consequence of such actions on other people such as taxi drivers, traders and tourists, to show the negative impact of street protests. The cybertroopers calls for the public to "pity" taxi drivers who wouldn't be able to "make ends meet", and that "peaceful" rallies would still affect the "livelihood of traders". Some tweets referred to the "safety" issue, suggesting that the general public and tourists might be in danger. That some of their tweets refer to Bersih's rallies as "peaceful" and yet still say that "safety is compromised" shows the same contradictions found in the messaging crafted by Beruang Biru discussed earlier in this chapter, and further proof that the messages are spun to their convenience.

8.3 Conclusion

While Chapter 7 showed that not all tactics adopted by cybertroopers relate to information dissemination (and communication), instructions from Beruang Biru suggest that this is the predominant task assigned to its recipients. The key feature of the Online Deployment Strategy—the use of shades to categorise the materials for propagation—certainly alludes to this. The system used in the ODS template to categorise these materials may not be explicitly clear, but the fact that the categories exist indicate that there is some consideration by Beruang Biru as to the kind of messages they want to put out on social media. I tested the shades—white, grey, and black—against the propaganda hypothesis, and found that they did not match understandings of propaganda shades on two counts. First, the covert nature of

cybertrooping in itself removes the element of authenticity of source, and secondly, it was not possible to make any distinctions based on truthfulness.

Instead, I argue that these categories can serve two purposes. First, it offers options of 'message styles' for cybertroopers to choose from. Based on the way they want to or may already be perceive, the cybertroopers can opt for whichever material is more relevant and appropriate for their platforms and public personas. Secondly, the categorisation system also allows Beruang Biru to indicate through its directions which accounts are allowed to use what material. I posit that talking points that could cause most problems for Barisan Nasional—as opposed to issues or topics that in themselves are controversial—are labelled grey or black (or both) to ensure that, among other consideration regarding style, it's not disseminated on official accounts.

This chapter also discussed the various messaging strategies and themes found in both the Beruang Biru and Twitter datasets to extend on discussions from Chapters 6 and 7 to better understand how cybertroopers operate. I presented the findings based on the framework set out in Chapter 2, identifying messages based on dissemination, defence, demonisation, disruption and distraction. While each of the categories served different purposes, they all served to portray the Barisan Nasional government in the best light, blur party and state lines, and portray its opponents as the enemy, particularly through the conflation of nation and state. There were also instances across several categories where the targets of cybertrooper messaging were the same: politically-linked individuals, political institutions like parties or civil society groups and some segments of the public as well.

This section showed that cybertroopers engage in the dissemination of positive and negative propaganda, both laced with a heavy dose of spin. Key message points that

are similar to frames—including the protest paradigm, and ideology linked to racism and anti-semitism, among others—used in the mainstream media also underpin my assertions that cybertroopers operate as part of the larger Barisan Nasional communication mechanism. The extent to which these frames are primed as found in the Twitter data also supports that argument. The findings in this section additionally showed how some of the messaging tactics are well placed to be used alongside the others discussed in previous chapters including targeted trolling, brigading and the use of memetic signifiers.

The approaches to messaging discussed in this chapter raise the question of just how far a political party is willing to go to secure power. The significant amount of planning that has gone into the creation, and subsequent propagation, of these messages only shows the extent to which Barisan Nasional were willing to engage in illiberal practices to achieve its strategic goals. The significant use of negative spin—particularly in attacks against its opponents—alongside the spreading sentiment aimed at disrupting public life, further brings the problems with the coalition's claim of legitimate democracy into the spotlight.

CONCLUSION

In this thesis, I have investigated how cybertrooping serves as an online extension of the states' control mechanism to secure and retain power through the influencing and manipulation of communication practices and information flow in the political sphere. I have presented the findings from the analysis of data related to cybertrooping in Malaysia during the Barisan Nasional years (pre-May 2018), and discussed the operations behind numerous cybertrooping campaigns, the ways in which cybertroopers are mobilised as well as the various activities that they engage in. The above discussions resulted from the examination of instructional emails pseudonymously received from Beruang Biru, which offered the first direct empirical evidence of its kind to be studied academically. Two datasets of tweets related to the Bersih rallies—arguably the most significant social movement in Malaysia in over a decade—collected and analysed using elements of computational data science methods provided further evidence of cybertrooping in action. These latter two datasets were valuable in the triangulation process to verify and extend on the findings from the analysis of the Beruang Biru emails. In addition, the analysis of over 400 journalistic reports related to cybertrooping from 13 news outlets across Malaysia and Singapore offered an understanding of the media's portrayal of the practice. These news articles also served as documents of records of the statements, claims and assertions made by leaders across the political divide as to their respective party's disclosure—or denial—of their use of cybertroopers. Interviews with politicians who are currently or formerly with parties accused of cybertrooping were also used in the triangulation process. Through the analyses presented in the thesis, I

have been able to address certain gaps in the existing literature from both a methodological perspective as well as empirical perspective. Collectively, the analysis of all the datasets described above makes this thesis the most extensive investigation specifically into the operations of Malaysian cybertroopers to date.

Malaysia is a unique location for study because of the many existing forms of control by the state, which had to eventually navigate a new space where they did not previously control. More interesting is that the Malaysian case offers a perspective from a quasi-authoritarian country where limited democracy is practiced. That Malaysia is a developing nation which needs to maintain its international standing through the veil of legitimacy contributes to the novelty of this study. This stands in contrast to many studies over the past decade which focused on the more authoritarian regimes, and the more recent investigations into the traditionally liberal democracies.

In this Conclusion chapter, I will discuss how the findings presented in this thesis so far—in particular, those found from Chapters 5 to 8—directly address two of the three aims of this study that I set out in Chapter 1, which were to:

- Examine instances of cybertrooping in Malaysia and identify how cybertroopers are mobilised.
- Explore the activities cybertroopers engage in, and locate these within the current understandings of political communication tools and strategies.

I then go on to offer operational, theoretical and practical ways in which cybertroopers can be studied, explaining how this thesis, and the Malaysian case, can contribute to further research to better understand this global phenomenon.

9.1 Operations and mobilisation

In addressing the first aim, the Beruang Biru emails and dataset of news reports were most useful in understanding how cybertroopers are mobilised. That the instructional emails included over 70 emails self-described as Online Deployment Strategy—that primarily contained material for distribution (usually the length of tweets) in the form of scripted messages—point to the hierarchical nature of cybertrooper operations. This finding matches descriptions found in the new reports attributed to politicians familiar with Barisan Nasional's operations regarding its cybertrooper teams being mobilised as part of a top-down structure akin to "multi-level networking", with information bullets provided to them for distribution. The analysis from the two datasets of tweets found that this was indeed the case, considering that numerous accounts were found on Twitter to have posted the same pro-Barisan Nasional or pro-government, and anti-opposition messages. The discovery of these instances of cybertrooping was discussed in Chapter Six.

The Beruang Biru emails also reveal the way that the teams behind the cybertroopers operate. First, they take on the role as a 'curator' of materials—from media outlets, blogs and other online sources—that are then distributed to cybertroopers for further dissemination. The complete dataset of emails shows how hundreds of such articles, images and videos were distributed by Beruang Biru over a two-year period between 2012 and 2014. As the 13th General Election approached, Beruang Biru's mobilisation went beyond the dissemination of materials and links; between March and May 2013, its focus shifted on to the Online Deployment Strategy emails where a variety of talking points were planned and distributed almost on a daily basis for cybertroopers' action. It was during this two-month period that the team behind

Beruang Biru stepped up their efforts of helping Barisan Nasional retain power through the manipulation of communication practices and information flow, including the gaming of algorithms, the hijacking of hashtags, and disruption of social media accounts run by its opponents.

In addition, that Beruang Biru sent seemingly ad hoc emails during the same period also indicates how the team were likely monitoring the political discourse closely, and were ready to mobilise their cybertroopers to respond to issues that could not be planned in advance. This further supports assertions made about the strategic role Beruang Biru takes on, based on emails that indicated that more details were being sought on a particular event or incident, or that recipients of the emails should be on standby for more information. It wasn't just with the Online Deployment Strategy emails that these kinds of mobilisation were found; well ahead of the general election, the occasional instructional email was distributed intermittently among all the other curated material flagging up events of incidents that required the attention of cybertroopers. This intervention could be in the form of attacks, such as when opposition leader Anwar Ibrahim allegedly orchestrated the removal of blogger Raja Petra Kamaruddin from a panel they were due to speak at—described as an "opportunity" for the cybertroopers—or the use of brigading as a tactic such as when Prime Minister Najib Razak's live interview was getting a negative response on YouTube. With the latter case, cybertroopers were activated to neutralise the situation by clicking on the 'Like' button. In addition, the circulation of a series of hashtags to be used for record keeping purposes also show the level of planning that goes into Beruang Biru's operations.

On the basis of my analysis of the emails, it is reasonable to conclude that these operations are part of Barisan Nasional and Prime Minister Najib's larger communication apparatus. This was evidenced not just by the organogram of Najib's alleged communication structure but also by the emails that showed that Beruang Biru was privy to party and government information. This meant that it was able to warn its cybertroopers in advance about upcoming events such as the announcement about the dissolution of Parliament which paved the way to the 13th General Election or the release of Barisan Nasional manisfesto. Beruang Biru also seemingly had information about national security issues related to the insurgency in Lahad Datu, Sabah. Besides this, the Beruang Biru emails included specific instructions for teams handling the official social media accounts for leaders, including cabinet ministers, and government agencies, which further link Beruang Biru to the ruling coalition. The Prime Minister's Department itself had organised cybertrooper workshops, which directly connects the practice to the government as well. Together, this shows how the lines between the two are blurred in Malaysia, which scholars refer to as an 'electoral one-party state' (Wong et al., 2010).

The news reports analysed and presented in Chapter Five—many of which are owned by parties that make up Barisan Nasional—have featured admissions by party leaders as to the existence of cybertrooper teams both explicitly and implicitly, such as by officiating the launch of cybertrooper teams, where some are provided mobile devices to conduct their activities. These claims of payment in kind were confirmed by current Foreign Minister Saifuddin Abdullah—part of the Pakatan Harapan government—in a direct interview, while answering questions regarding his knowledge of cybertrooping activities from the time when he was still in UMNO (S. Abdullah, personal communication, July 14, 2018).

Contextualising the above findings within the political history of Malaysia as presented in Chapter 4, I have asserted throughout this thesis that cybertroopers are part of a larger communication strategy adopted by Barisan Nasional and the government, operated alongside efforts of media control through ownership and legislation, on-ground mobilisation with proxy groups such as the Red Shirts, as well as information operations like DDoS attacks. This argument is further supported by the numerous message themes found in the #bersih and #bersih4 datasets that are similar to the narratives commonly used by Barisan Nasional to demonise the opposition in traditional media before the emergence of the internet, and social media. These narratives include questioning the legality of the Bersih rallies, invoking the chilling effect such as calling for police intervention and threatening the return of the Internal Security Act, and the politicising of race, religion and nationalism.

9.2 Characteristics of cybertrooping

The discussion above can also be used to describe the first characteristic of cybertrooping identified in this thesis, that is, that the activities they engaged in were 'state-linked'. I have chosen this term over 'state sponsored'—which is commonly found in descriptions of cybertrooping-like practices in existing literature—because there were was no direct evidence in the empirical evidence to suggest that cybertroopers are paid. This is despite accusations by other opposition politicians, such as those from the Democratic Action Party (DAP) found in the news reports analysed in Chapter 5, that Barisan Nasional cybertroopers are on a payroll. Instead, based on the argument that Beruang Biru is one of the ways in which cybertroopers are mobilised, then it is possible to posit that their materials do not only reach to paid

agents because some people among those who received the emails questioned why they were included in the mailing list. This suggests that they were not expecting such information; as mentioned in Chapter 1, I too received those emails unsolicited.

What is more, that the Prime Minister's Department organised workshops to recruit cybertroopers from among civil service employees could also suggest that they are not on a separate payroll. Indeed, King, Pan and Roberts' (2017) study on China found that members of the 50 Cent Army were in fact already working for the government, and not paid directly for their pro-government online activities. The specific mentions of "official accounts" in the ODS emails also speaks to this similarity. That is not to say that some Malaysian cybertroopers are not paid. The former UMNO MP Saifuddin Abdullah confirmed during the interview that cybertroopers were indeed paid—either in cash or kind (S. Abdullah, personal communication, July 14, 2018)—while the former UMNO Youth leader Khairy Jamaluddin had made a reference to some cybertroopers being on a payroll in new reports.

This argument may also be contentious, considering that scholars have previously argued that both Barisan Nasional and its opposition have their respective teams of cybertroopers. However, there were no patterns found in any datasets—aside from the accusations of DAP's alleged Red Bean Army in news reports—which matched those found involving pro-Barisan Nasional cybertroopers. Just as none of the news reports discussed in Chapter Five produced evidence of the Red Bean Army's existence, so the analysis of the datasets analysed for this thesis did not find any instances of pro-opposition cybertrooping.

If they do indeed exist, then they use different strategies and tactics to the Barisan Nasional cybertroopers. This would support the claim by DAP's Liew Chin Tong that Barisan Nasional's imagination of the Red Bean Army relies on their own model of cybertrooping, as mentioned in Chapter Five. On the basis that the understanding of cybertrooping presented in this thesis is developed from the findings of these particular sets of empirical evidence, the online activities adopted by the opposition parties should not be considered cybertrooping.

Perhaps due to the fact that they are state-linked, another significant characteristic of cybertrooping is that the activities are conducted in a covert manner. This characteristic allows the party or government mechanism to dissociate themselves from the practice, essentially gifting them plausible deniability. This distance is important to any government because cybertrooping's shaping and influencing perception of the public can be considered 'non-consensual organized persuasive communication' (Bakir et al., 2018), making it manipulative and therefore, fundamentally deceitful. It is more significant if the country, like Malaysia, is one that has spent many decades attempting to portray an image of being a legitimate democracy despite its semi-authoritarian credentials.

In this regard, cybertroopers operate essentially as front groups—a common public relations technique—allowing third-parties to perform the sort of politics a party in a democratic government tend to avoid engaging with. Cybertrooping enables Barisan Nasional to outsource the seeding of controversial messages, whether to do with extent of spin, message style or topics discussed. In Chapter Eight, for example, cybertroopers were described as having engaged using language and tones that are often not considered appropriate in deliberative political discourse. This is further

supported by the fact that Beruang Biru has been explicit that official accounts are not to use any material categorised as grey or black, which I have argued includes material that are negatively spun or which might cause controversy if addressed directly by Barisan Nasional.

Collectively, the insights discussed above explain why Beruang Biru—in itself a pseudonym to hide the identity of those behind it—said in its early emails that its role is consistent with Barisan Nasional's, that is, to "assist" the coalition win the general election. By claiming simply to be "a Malaysian who wants to help the country move forward", Beruang Biru gives the impression that its operations are a grassroots campaign, although the fact that the emails include strategies, "compulsory action" and record keeping via hashtags, belies that claim.

Building on this, it is possible to identify the third characteristic of cybertrooping, that is, the reliance on fake accounts, which I have described as sockpuppetry in action. This characteristic was evidenced in both the Beruang Biru and Twitter datasets. Indeed, the two names that this investigation has uncovered as linked to Beruang Biru themselves can be linked to sockpuppetry. This was identified through the three emails similar to those from Beruang Biru which were sent using the names Ameera Arini and Ah Boon. Chapter Three described how the two names may actually belong to the same person. In addition, Ameera Arini's name was also found in the #bersih dataset as part of the pool of suspected cybertroopers. As revealed in Chapter Six, these fake accounts differ from legitimate alt accounts that are commonly created as part of internet culture. These assertions are further supported by accusations that accounts found supporting Prime Minister Najib used images of photos belonging to other people, including the deceased. While sockpuppetry is

suspected among the smaller pool of cybertrooper accounts found in the Twitter datasets, it was more obvious where social bots are concerned. The creation of multiple fake accounts forms the foundation of bot activity in order to achieve its strategic aims of disseminating information or disrupting communication practices through large volume automation.

9.3 The activities cybertroopers engage in

The discussions in Chapter Six related to the most easily identifiable activity from the Beruang Biru emails—that is, scripted messages crafted for cybertroopers to disseminate—served as a starting point to answer the second research question. Specifically, it indicated the use of astroturfing as a cybertrooping tactic. The analysis of the Twitter datasets also showed similar patterns of identical tweets being disseminated from different accounts. Some of the other tactics identified in Chapter Seven further support the assertion that a key activity that cybertroopers engage in is the dissemination of information, whether in the form of text, images of videos. Spamming and sockpuppetry, for example, involved the distribution of cybertrooping content in large quantities; the former dealing with the volume of messages (force multiplication of messages), while the latter refers to the volume of accounts (multiplication of message forces).

The use of memetic signifiers is another indication that the distribution of pro-Barisan Nasional and pro-government material (and indeed, spamming) involves different forms of media texts. The example of the personalised badges that can be created from the Better Nation website shows how images are also used. Other examples include those created as part of the #RespectMyPM campaign—

personalised to a lesser degree—where it was easier to execute through the distribution of over a dozen images (representing the various Malaysian states) that cybertroopers would attempt to make 'viral'. A so-called personalised campaign such as this one could be created in a short amount of time—perhaps similar to how the ad hoc strategies found in the Beruang Biru emails were crafted—to distract from the significant event where Mahathir Mohamad collaborated with his former foes in the Save Malaysia campaign.

Depending on how these tactics are used, they can serve one or more propagandistic strategies. The examples above, for instance, indicate how useful these tactics can be for dissemination and distraction. Depending on what the contents of the messages are, they can also be used to defend from, or demonise, their opponents. One of the tactics involved in demonising those critical of Barisan Nasional, for instance, is by taking advantage of social media's mark-up culture such as through the weaponising of hashtags. For example, hashtags like #AgendaYahudi were used as a priming tool to associate movements such as Bersih to the supposed 'Jewish agenda' in attempts to repudiate the movement. Hashtags were also created for the purpose of character assassination against political personalities, such as the use of #tolakTianChua (reject Tian Chua) and #pengkhianatnegara (national traitor) against the National Justice Party (PKR) politician.

Cybertroopers also engage in activities involving the appropriation of hashtags from its intended use to push through Barisan Nasional's agenda. The series of "joining #bersih" tweets, which were crafted to list out why the public should not participate in the street rally, is an example of how the #bersih hastag has been hijacked. The use of this tactic has several implications: it can render a hashtag unusable, especially

when hijacked in large volumes (automated accounts like social bots makes this easier to achieve); it changes the dominant narrative associated with the hashtag in question; and may have implications on Twitter's algorithms.

The gaming of algorithms is another clear tactic used by cybertroopers, as examples found in the Beruang Biru instructions illustrate. This activity takes the form of brigading, where cybertroopers are mobilised to disrupt the ranking systems of social media posts, including the 'Like' functions on YouTube and Facebook, and the retweet function of Twitter. These activities have both visible and non-visible consequences; the former allows cybertroopers to manipulate, for example, instances of negative feedback of pro-Barisan Nasional content by encouraging cybertroopers to 'Like' a particular post, while the latter may affect how content are distributed and made available on social media timelines of users through algorithmic ranking.

Similar efforts at mobilising cybertroopers to take action on another platform can also be seen in the use of coordinated trolling. This tactic can serve to both demonise and disrupt the social media accounts of members of the opposition, such as when Anwar Ibrahim and Khalid Ibrahim were subjected to requests by Beruang Biru to be tagged on Twitter and flooded with questions or abuse. The discussion above also shows that strategies and tactics used to execute the various activities are not mutually exclusive.

The findings from this typology can also be seen as building on existing political communication tools with which cybertrooping-like practices has been associated. The distribution of content such as talking points is a common practice used by PR consultants and spin doctors. While some of the content can be considered positive (or white) propaganda, it remains problematic due to the lack of transparency as

indicated by the murkier PR tactics of astroturfing, front groups and third party proxies. Psyops is also clearly used in cybertrooper operations, particularly where they take on the roles of multipliers of message forces involved in the force multiplication of messages. That Barisan Nasional views their online efforts in militaristic terms—as discussed in Chapter Five—also suggests that psyops is one of the existing methods of information manipulation that underlies the practices of cybertrooping. Collectively, the reliance on these known tools for information manipulation shows that cybertrooping should be considered a 'non-consensual' persuasive communication.

These activities also show how much cybertroopers rely on internet affordances in their efforts to manipulate the flow of information and disrupt communication practices. As such, it is possible to argue—at this stage of the thesis—that cybertrooping builds on those techniques but have adapted them for the digital space. Chapter 2 warned about the 'digital dazzle' in understanding the practice, but these findings do indeed illustrate how cybertroopering differs from existing techniques for information manipulation that pre-dates the internet. Having said that, it is pertinent that cybertrooping is not understood as a separate phenomenon of the digital age but instead as an extension of other modes of political communication used in Malaysia and the rest of the world. Indeed, the findings from this study suggest that cybertrooping is part of a larger communications ecosystem—both online and offline—that is used in efforts to win political battles. In the Malaysian case at least, Barisan Nasional cybertroopers are just one of many methods of information management and control. Chapter Five discussed the use of media ownership to influence media reports to demonise the opposition as seen with the apparent invention of the Red Bean Army. In addition, Chapters Seven and Eight

also showed how priming is used by cybertroopers to perpetuate notions that have long been used in the government-controlled mainstream media, such as the use of the protest paradigm to discredit the Bersih movement. This multi-pronged approach suggests that cybertroopers are just one aspect of the media control apparatus of the ruling party.

Taking all of the above activities into consideration, it is possible to look at cybertrooping as another evolved form of propaganda, relying on some of the affordances of the internet to achieve its strategic goals.

9.4 Generalising the Malaysian case

The discussions in the previous three sections of this conclusion have so far addressed the first two aims of this study. The final aim is to use the findings discussed above to understand better and contextualise the global phenomenon of online manipulation of political information. As explained in Chapter Two, this practice has been the subject of research by scholars for over a decade but the mainstream discussions on this issue at global level only really emerged following allegations of Russian interference in the EU Referendum in the United Kingdom and the US Presidential Election in 2016. The latter two events raise another element of online manipulation of information not previously discussed in this thesis, and that is of transnational intervention. I believe that this thesis can contribute to further understanding these sorts of practices in a general way which transcends either domestic or transnational contexts.

Chapter Two made the case for offering the descriptors cybertroopers and cybertrooping to the existing lexicon related to online manipulation of information to fill some of the existing gaps in the literature. The chapter argued that terms such as astroturfing, computational propaganda (which generally refers only to automation and algorithmic related activities such as bots and brigading), and trolling, do not capture the extent of the complexities related to the practices that are the focus of this study. I believe that the addition of cybertrooping and cybertroopers is useful because they were created specifically to refer to online practices of information manipulation. Additionally, the findings in this thesis show that these terms capture the nuances and varying elements of the practice which the other terms in the lexicon respectively do not.

As such, expanding on the Oxford Internet Institute's definition of "cyber troops"[1], this thesis offers the following:

> *Cybertroopers are state-linked agents mobilised in a top-down manner to manipulate information and disrupt communication practices in the political sphere.*
>
> *Cybertrooping refers to the activities that are conducted by cybertroopers as online extension of the state's information management and control mechanism to secure or retain power.*

The following are three ways the term cybertroopers can be conceptualised and used in general. Operationally, cybertroopers are individuals who are generally part of a larger communications strategy (that also involves non-digital media operations), who engage in the practice of cybertrooping. Cybertrooping involves a number of activities which include the dissemination (in various volume sizes) of information—

[1] As mentioned in Chapter 1, the OII defines 'cyber troops' as "government, military or political party teams committed to manipulating public opinion over social media" (Bradshaw & Howard, 2017, p. 3)

whether as texts, images or videos—and also the disruption of communication practices such as the gaming of algorithms and the targeting of hashtags.

Practically, cybertroopers and cybertrooping are not explicitly identifiable to the public through their activities. In whatever styles that they perform as part of the public personas they adopt, cybertroopers usually portray themselves as genuine citizens who are supportive of the state. While they may look like content producers, in actuality, they are very much part of the state's control mechanisms. Cybertroopers in general do not admit to being cybertroopers, and there is no acknowledgement from their public profiles that link them to this.

Theoretically**,** cybertroopers are agents mobilised by state-linked political actors who rely on the internet affordances to engage in activities related to the manipulation of information and the disruption of communication practices to assist the state to secure its power.

####

REFERENCES

#RespectMyPM: Online war breaks out in Malaysia. (2016, March 7). *BBC News*. Retrieved from https://www.bbc.co.uk/news/world-asia-35742118

#RespectMyPM campaign gains traction. (2016, March 7). *Malaysiakini*. Retrieved from https://www.malaysiakini.com/news/333010

Abbott, J., Macdonald, A. W., & Givens, J. W. (2013). New Social Media and (Electronic) Democratization in East and Southeast Asia. *Taiwan Journal of Democracy*, *9*(2), 105–137.

Abbott, J. P. (2000). Bittersweet victory: The 1999 Malaysian general election and the Anwar Ibrahim affair. *Round Table*, (354), 245–258. https://doi.org/10.1080/750459438

Ahead of election, cyber-attacks cripple online media. (2011). Retrieved February 7, 2016, from https://cpj.org/2011/04/ahead-of-election-cyberattacks-cripple-online-medi.php

Ai, W. (2012, October 17). China's Paid Trolls: Meet the 50-Cent Party. *New Statesman*. Retrieved from https://www.newstatesman.com/politics/politics/2012/10/china's-paid-trolls-meet-50-cent-party

Al-Rawi, A. K. (2014). Cyber warriors in the Middle East: The case of the Syrian Electronic Army. *Public Relations Review*, *40*(3), 420–428. https://doi.org/10.1016/j.pubrev.2014.04.005

Alatas, S. H. (1977). *Intellectuals in developing societies*. London: F. Cass.

Albayrak, A., & Parkinson, J. (2013, September 16). Turkey's Government Forms 6,000-Member Social Media Team. *The Wall Street Journal*. Retrieved from https://www.wsj.com/articles/turkeys-government-forms-6000member-social-media-team-1379351399

Ambiga gets death threats. (2011, June 24). *The Star*. Retrieved from https://www.thestar.com.my/news/nation/2011/06/24/ambiga-gets-death-threat

Ananthalakshmi, A. (2018, April 20). Ahead of Malaysian polls, bots flood Twitter with pro-government messages. *Reuters*. Retrieved from https://uk.reuters.com/article/uk-malaysia-election-socialmedia/ahead-of-malaysian-polls-bots-flood-twitter-with-pro-government-messages-idUKKBN1HR2AH

Andrews, L. (2006). Spin: from tactic to tabloid. *Journal of Public Affairs*, *6*(1), 31–45. https://doi.org/10.1002/pa.37

Aro, J. (2016). The cyberspace war: propaganda and trolling as warfare tools. *European View*, *15*(1), 121–132. https://doi.org/10.1007/s12290-016-0395-5

Arora, S. K., Li, Y., Youtie, J., & Shapira, P. (2016). Using the wayback machine to mine websites in the social sciences: A methodological resource. *Journal of the Association for Information Science and Technology*, *67*(8), 1904–1915. https://doi.org/10.1002/asi.23503

Azlan, N. A. (2018). *Seditious Spaces*. *A+BE | Architecture and the Built Environment*. Retrieved from https://superheroscitech.tudelft.nl/index.php/abe/article/view/2661

Badrul Azmier, M. B., Mohammad Agus, Y., & Zaliha, H. H. (2014). The paradox of social media: The De-Democratization of Malaysia. *International Review of Basic and Applied Sciences*, *2*(7), 104–112.

Bakir, V., Herring, E., Miller, D., & Robinson, P. (2018). Organized Persuasive Communication: A new conceptual framework for research on public relations, propaganda and promotional culture. *Critical Sociology*, *45*(3), 1–18. https://doi.org/10.1177/0896920518764586

Bandu, S. H., & Ahmad, A. R. (2015). Patriotism: Issues and Challenges In Malaysia. In *International Conference on Current Issues in Education 2015*.

Barstow, D. (2008, April 20). Behind TV Analysts, Pentagon's Hidden Hand. *The New York Times*. Retrieved from https://www.nytimes.com/2008/04/20/us/20generals.html

Beckett, C. (2012). *Wikileaks : the threat of the new news*. Cambridge: Polity Press.

Benkler, Y., Farris, R., & Roberts, H. (2018). *Network Propaganda*. New York: Oxford University Press. Retrieved from http://www.oapen.org/download?type=document&docid=1001606

Benner, K., Mazzetti, M., Hubbard, B., & Isaac, M. (2018, October 20). Saudis' Image Makers: A Troll Army and a Twitter Insider. *The New York Times*. Retrieved from https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html

Bennett, W. L., & Livingston, S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. *European Journal of Communication*, *33*(2), 122–139. https://doi.org/10.1177/0267323118760317

Benoit, W. L., & Holbert, R. L. (2008). Empirical Intersections in Communication Research: Replication, Multiple Quantitative Methods, and Bridging the Quantitative–Qualitative Divide. *Journal of Communication*, *58*(4), 615–628. https://doi.org/10.1111/j.1460-2466.2008.00404.x

Berghel, H. (2018). Malice Domestic: The Cambridge Analytica Dystopia. *Computer*, *51*(5), 84–89. https://doi.org/10.1109/MC.2018.2381135

Bradshaw, S., & Howard, P. N. (2017). *Troops, trolls and troublemakers: A global inventory of organized social media manipulation*. Retrieved from http://phibetaiota.net/wp-content/uploads/2017/07/Troops-Trolls-and-Troublemakers.pdf

Bradshaw, S., & Howard, P. N. (2018). *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*. Retrieved from http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brown, G. K. (2013). MALAYSIA IN 2012: Promises of Reform; Promises Met? *Southeast Asian Affairs*, 155–167. Retrieved from http://www.jstor.org/stable/23471142

Bruns, A., & Burgess, J. (2015). Twitter hashtags from ad hoc to calculated publics. In N. Rambukkana (Ed.), *Hashtag Publics: The Power and Politics of Discursive Networks* (pp. 13–28). New York: Peter Lang. Retrieved from https://eprints.qut.edu.au/90461/

Bruns, A., & Liang, Y. E. (2012). Tools and methods for capturing Twitter data during natural disasters. *First Monday*, *17*(4). https://doi.org/10.5210/fm.v17i4.3937

Buang, S. (2016, July 29). Lodge a report, minister tells family of deceased whose photo was hijacked. *Malaysiakini*. Retrieved from https://www.malaysiakini.com/news/350453

Buku Harapan. (2018). Pakatan Harapan. Retrieved from http://kempen.s3.amazonaws.com/manifesto/Manifesto_text/Manifesto_PH_EN.pdf

Calingaert, D. (2010). Authoritarianism vs. the Internet. *Policy Review*, *160*(63), 63–75.

Cammaerts, B. (2013). Networked Resistance: The Case of WikiLeaks. *Journal of Computer-Mediated Communication*, *18*(4), 420–436. https://doi.org/10.1111/jcc4.12024

Campbell, M., & Lane Keller, K. (2003). Brand Familiarity and Advertising Repetition Effects. *Journal of Consumer Research*, *30*, 292–304. https://doi.org/10.1086/376800

Carman, M., Koerber, M., Li, J., Choo, K. R., & Ashman, H. (2018). Manipulating Visibility of Political and Apolitical Threads on Reddit via Score Boosting. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications* (pp. 184–190). https://doi.org/10.1109/TrustCom/BigDataSE.2018.00037

Case, W. (1993). Semi-Democracy in Malaysia: Withstanding the Pressures for Regime Change. *Pacific Affairs*, *66*(2), 183–205. https://doi.org/10.2307/2759366

Case, W. (1999). Politics beyond Anwar: What's new? *Asian Journal of Political Science*, *7*(1), 1–19. https://doi.org/10.1080/02185379908434134

Case, W. (2017). Stress testing leadership in Malaysia: the 1MDB scandal and Najib Tun Razak. *The Pacific Review*, *30*(5), 633–654. https://doi.org/10.1080/09512748.2017.1282538

Castells, M. (2015). *Networks of outrage and hope : social movements in the internet age*. Cambridge: Polity Press.

Chan, C. (2003). Breaking Singapore's Regrettable Tradition of Chilling Free Speech with Defamation Laws. *Loyola of Los Angeles International and Comparative Law Review*, *26*(2), 315–340.

Chan, T. C. (2018). Democratic Breakthrough in Malaysia – Political Opportunities and the Role of Bersih. *Journal of Current Southeast Asian Affairs*, *37*(3), 109–137. Retrieved from https://journals.sub.uni-hamburg.de/giga/jsaa/article/view/1150/1157

Cheah, W. H., & Singaravelu, H. (2017). The Coming-Out Process of Gay and Lesbian Individuals from Islamic Malaysia: Communication Strategies and Motivations. *Journal of Intercultural Communication Research*, *46*(5), 401–423. https://doi.org/10.1080/17475759.2017.1362460

Chen, A. (2015, June 2). The Agency. *The New York Times Magazine*. Retrieved from https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Cheong, N. (2012). *Information flow and social ties on Twitter: A Bersih 3.0 rally case study*. King's College London.

Chew, A. (2016, March 9). Twitter humiliation for Malaysia's Najib Razak, as 'RespectMyPM' morphs into 'SuspectMyPM.' *South China Morning Post*. Retrieved from https://www.scmp.com/news/asia/southeast-asia/article/1922671/twitter-humiliation-malaysias-najib-razak-respectmypm

Chin, J. (1997). Malaysia in 1996: Mahathir-Anwar Bouts, UMNO Election, and Sarawak Surprise. *Asian Survey*, *37*(2), 181–187. https://doi.org/10.2307/2645486

Chin, J. (2016). The 2015 Singapore Swing: Depoliticised Polity and the Kiasi/Kiasu Voter. *The Round Table*, *105*(2), 141–148. https://doi.org/10.1080/00358533.2016.1154383

Chin, J. (2017, July 19). Why Mahathir is at the centre of Malaysia's opposition power play. *The Interpreter*. Retrieved from https://www.lowyinstitute.org/the-interpreter/why-mahathir-centre-malaysia-s-opposition-power-play-0

China denounces "ridiculous" US claims of election meddling. (2018, October 5). *Al-Jazeera*. Retrieved from https://www.aljazeera.com/news/2018/10/china-denounces-ridiculous-claims-election-meddling-181005025606837.html

Cho, C. H., Martens, M. L., Kim, H., & Rodrigue, M. (2011). Astroturfing Global Warming: It Isn't Always Greener on the Other Side of the Fence. *Journal of Business Ethics*, *104*(4), 571–587. https://doi.org/10.1007/s10551-011-0950-6

Chooi, C. (2011, April 24). Najib repeats promise of no Internet censorship. *The Malaysian Insider*. Retrieved from http://www.themalaysianinsider.com/malaysia/article/najib-repeats-promise-of-no-internet-censorship

Clayton, R., Murdoch, S. J., & Watson, R. N. M. (2006). Ignoring the Great Firewall of China. In G. Danezis & P. Golle (Eds.), *Proceedings of the 6th Workshop on Privacy Enhancing Technologies, UK* (pp. 20–35). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/11957454_2

Coleman, G. (2015). *Hacker, hoaxer, whistleblower, spy : the many faces of Anonymous*. London: Verso.

Comninos, A. (2011). *Twitter revolutions and cyber crackdowns. User-generated content and social networking in the Arab spring and beyond.*

Cormac, R., & Aldrich, R. J. (2018). Grey is the new black: covert action and implausible deniability. *International Affairs*, *94*(3), 477–494. https://doi.org/10.1093/ia/iiy067

Cormack, G., & Lynam, T. (2005). Spam corpus creation for TREC. *Second Conference on Email and Anti-Spam (CEAS2005)*, 0–1. Retrieved from ftp://ftp.research.microsoft.com/Users/joshuago/papers-2005/162.pdf

Cyber attack on Harakahdaily; A message to readers. (2011, April 15). *Harakah Daily Online*. Retrieved from http://en.harakahdaily.net/index.php?option=com_content&view=article&id=2624:cyber-attack-on-harakahdaily-a-message-to-readers&catid=34:primary&Itemid=56

Dean, J. (2010). Affective Networks. *MediaTropes EJournal*, *2*(2), 19–44.

Delaney, S. (2016, January 20). How Lynton Crosby (and a dead cat) won the election: "Labour were intellectually lazy." *The Guardian*. Retrieved from https://www.theguardian.com/politics/2016/jan/20/lynton-crosby-and-dead-cat-won-election-conservatives-labour-intellectually-lazy

Dennis, J. (2019). *Beyond Slacktivism : Political Participation on Social Media*. Palgrave Macmillan.

Dinan, W., & Miller, D. (2007). *Thinker, faker, spinner, spy : corporate PR and the assault on democracy*. London; Ann Arbor, Mich.: Pluto Press.

Ding, J.-A., Koh, L. C., & Surin, J. A. (2013). *Mapping Digital Media: Malaysia*.

DiResta, R. (2018). Computational Propaganda: If you make it trend, you make it true. *The Yale Review*, *106*(4), 12–29. https://doi.org/10.1111/yrev.13402

Disinformation and 'fake news': Interim Report. (2018). London. Retrieved from https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36302.htm

Edgar, T. H. (2017). *Beyond Snowden privacy, mass surveillance, and the struggle to reform the NSA*. Washington D.C.: Brookings Institution Press.

Eko, B. L., Kumar, A., & Yao, Q. (2011). Google This : The Great Firewall of China , the IT Wheel of India, Google Inc., and Internet Regulation. *Journal of Internet Law*, (September).

Elazar, D. J. (1985). Federalism and Consociational Regimes. *Publius: The Journal of Federalism*, *15*(2), 17–34. https://doi.org/10.1093/oxfordjournals.pubjof.a037543

Ellis-Petersen, H. (2018, May 16). Malaysia: Anwar Ibrahim released from prison. *The Guardian*. Retrieved from https://www.theguardian.com/world/2018/may/16/malaysia-anwar-ibrahim-released-from-prison

Esser, F. (2013). Spin Doctor. In *The International Encyclopedia of Communication* (First). John Wiley & Sons, Ltd. https://doi.org/doi:10.1002/9781405186407.wbiecs088.pub2

Fake #RespectMyPM account busted for stealing another Malaysian's profile picture. (2017, February 11). *World of Buzz*. Retrieved from https://www.worldofbuzz.com/fake-respectmypm-account-busted-stealing-another-malaysians-profile-picture/

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

Fitzpatrick, K. R., & Palenchar, M. J. (2006). Disclosing Special Interests: Constitutional Restrictions on Front Groups. *Journal of Public Relations Research*, *18*(3), 203–224. https://doi.org/10.1207/s1532754xjprr1803_1

Fox, K. (2014). *Watching the English : [the hidden rules of English behaviour]*. London: Hodder et Stoughton.

Gaber, I. (2000). Government by spin: an analysis of the process. *Media, Culture & Society*, *22*(4), 507–518. https://doi.org/10.1177/016344300022004008

Gabriel, S. P. (2015). The meaning of race in Malaysia: Colonial, post-colonial and possible new conjunctures. *Ethnicities*, *15*(6), 782–809. https://doi.org/10.1177/1468796815570347

Gallagher, K. (2014). *Astroturfing : 21 st Century False Advertising*.

George, C. (2005). The internet's political impact and the penetration/participation paradox in Malaysia and Singapore. *Media, Culture and Society*, *27*(6), 903–920. https://doi.org/10.1177/0163443705057678

George, C. (2006). *Contentious journalism and the internet : towards democratic discourse in Malaysia and Singapore*. Singapore : Singapore University Press, 2006. Retrieved from http://ezlibproxy1.ntu.edu.sg/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=cat00103a&AN=ntu.a398527&site=eds-live&scope=site

George, C. (2007). Media in Malaysia: Zone of Contention. *Democratization*, *14*(5), 893–910. https://doi.org/10.1080/13510340701635712

George, C. (2016). *Hate spin : the manufacture of religious offense and its threat to democracy*. Cambridge, MA: Press, MIT.

Gerbaudo, P. (2012). Tweets and the streets : social media and contemporary activism. London: Pluto.

Gerbaudo, P. (2015). Protest avatars as memetic signifiers: political profile pictures and the construction of collective identity on social media in the 2011 protest wave. *Information, Communication & Society*, *18*(8), 916–929. https://doi.org/10.1080/1369118X.2015.1043316

Gerbaudo, P. (2018). *The digital party. Political organisation and online democracy*. London: Pluto Press.

Gerlitz, C., & Rieder, B. (2013). Mining One Percent of Twitter: Collections, Baselines, Sampling. *M/C Journal*, *16*(2). Retrieved from http://journal.media-culture.org.au/index.php/mcjournal/article/view/620

Gero, M., & Kopper, Á. (2013). Fake and Dishonest: Pathologies of Differentiation of the Civil and the Political Sphere in Hungary. *Journal of Civil Society*, *9*(4), 361–374. https://doi.org/10.1080/17448689.2013.844449

Gillmor, D. (2006). *We the media : grassroots journalism by the people, for the people*. Sebastopol, CA: O'Reilly.

Glenski, M., & Weninger, T. (2017). Rating Effects on Social News Posts and Comments. *ACM Transactions on Intelligent Systems and Technology (TIST)*, *8*(6), 1–19. https://doi.org/10.1145/2963104

Gomez, J., & Chan, H. L. (2010). *New Media and General Elections: Online Citizen Journalism in Malaysia and Singapore. Malaysia and Singapore Workshop: Media, Law, Social Commentary, Politics*. Melbourne. Retrieved from https://www.academia.edu/242554/New_Media_and_General_Elections_Online_Citizen_Journalism_in_Malaysia_and_Singapore

Gong, R. (2011). Internet Politics and State Media Control: Candidate Weblogs in Malaysia. *Sociological Perspectives*, *54*(3), 307–328. https://doi.org/10.1525/sop.2011.54.3.307

Goode, L. (2009). Social news, citizen journalism and democracy. *New Media and Society*, *11*(8), 1287–1305. https://doi.org/10.1177/1461444809341393

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

Greenwald, G., & Fishman, A. (2015, June 22). Controversial GCHQ Unit Engaged In Domestic Law Enforcement, Online Propaganda, Psychology Research. *The Intercept*. Retrieved from https://theintercept.com/2015/06/22/controversial-gchq-unit-domestic-law-enforcement-propaganda/

Grimme, C., Assenmacher, D., & Adam, L. (2018). Changing Perspectives: Is It Sufficient to Detect Social Bots? (pp. 445–461).

Grimshaw, C. (2007). A Tour of the United Kingdom's Public Relations Industry. In W. Dinan & D. Miller (Eds.), *Thinker, faker, spinner, spy : corporate PR and the assault on democracy* (pp. 33–50). London; Ann Arbor, Mich.: Pluto Press.

Grudgings, S. (2014, September 7). With sedition dragnet, Malaysia takes step back to Mahathir era. *Reuters*. Retrieved from https://uk.reuters.com/article/malaysia-sedition-idINKBN0H204C20140907

Guest, P. (2018, May 9). "Queen of Dragons": The inside story of Malaysia's election fixer. *Wired*. Retrieved from https://www.wired.co.uk/article/election-malaysia-2018-general-fake-news-day-2008-syarul-ema

Hah, F. L. (2012). *New Media and Old Politics: The role of blogging in the 2008 Malaysian general election*. University of Canterbury.

Hah, F. L. (2016). *Power games : political blogging in Malaysian national elections*. Singapore: ISEAS-Yusof Ishak Institute. Retrieved from https://muse.jhu.edu/book/47831/

Hall, M. (2014, July 18). Israeli propaganda war hits social media. *The Sydney Morning Herald*. Retrieved from https://www.smh.com.au/technology/israeli-propaganda-war-hits-social-media-20140717-ztvky.html

Hannan, J. (2018). Trolling ourselves to death? Social media and post-truth politics. *European Journal of Communication*, *33*(2), 214–226. https://doi.org/10.1177/0267323118760323

Hardy, K. (2015). National Security Reforms and Freedom of the Press. *Griffith Journal of Law & Human Dignity*, *3*(1), 1–29.

Harold, C. (2004). Pranking rhetoric: "culture jamming" as media activism. *Critical Studies in Media Communication*, *21*(3), 189–211. https://doi.org/10.1080/0739318042000212693

Hashtag backfires in Malaysia PM's campaign. (2016, March 8). *Al Jazeera*. Retrieved from https://www.aljazeera.com/news/2016/03/hashtag-backfires-malaysia-campaign-160307164532002.html

Hassan, A. (2004). One Hundred Years of Language Planning in Malaysia. *Language in India*, *4*(November). Retrieved from http://www.languageinindia.com/nov2004/abdulla1.html

Hiebert, R. E. (2003). Public relations and propaganda in framing the Iraq war: a preliminary review. *Public Relations Review*, *29*(3), 243–255. https://doi.org/10.1016/S0363-8111(03)00047-X

Highfield, T. (2018). Emoji hashtags // hashtag emoji: Of platforms, visual affect, and discursive flexibility. *First Monday*, *23*(9). https://doi.org/10.5210/fm.v23i9.9398

Ho, Y. Y., & Woo, C. K. (2016). When Censorship is not an option: Internet Trolling by National Intelligence Agency of S. Korea. In *The 17th Annual Conference of the Association of Internet Researchers*. Berlin: The 17th Annual Conference of the Association of Internet Researchers. Retrieved from https://journals.uic.edu/ojs/index.php/spir/article/view/9012

Hookway, N. (2012). "Entering the Blogosphere": Some Strategies for Using Blogs in Social Research. In B. Dicks (Ed.), *Digital Qualitative Research Methods*. London: SAGE.

Hopkins, J. (2014). Cybertroopers and tea parties: government use of the Internet in Malaysia. *Asian Journal of Communication*, *24*(1), 5–24. https://doi.org/10.1080/01292986.2013.851721

Hounshell, B. (2008, May 1). Mahathir Mohamad has a blog. *Foreign Policy*. Retrieved from https://foreignpolicy.com/2008/05/01/mahathir-mohamad-has-a-blog/

Howard, P. N., Agarwal, S. D., & Hussain, M. M. (2011). When Do States Disconnect Their Digital Networks? Regime Responses to the Political Uses of Social Media. *The Communication Review*, *14*(3), 216–232. https://doi.org/10.1080/10714421.2011.597254

Hung, C. (2010). China's Propaganda in the Information Age: Internet Commentators and the Weng'an Incident. *Issues & Studies*, *46*(4), 149–180.

Jack, C. (2017). *Lexicon of Lies : Terms for Problematic Information*. *Data & Society Research Institute*. Retrieved from https://datasociety.net/output/lexicon-of-lies/

Jackson, S. J., & Foucault Welles, B. (2015). Hijacking #MYNYPD: Social Media Dissent and Networked Counterpublics. *Journal of Communication*, *65*(6), 932–952. https://doi.org/10.1111/jcom.12185

Jenkins, T. (2009). How the Central Intelligence Agency works with Hollywood: An interview with Paul Barry, the CIA's new Entertainment Industry Liaison. *Media, Culture & Society*, *31*(3), 489–495. https://doi.org/10.1177/0163443709102721

Jensen, K. B. (2002). The Qualitative Research Process. In K. B. Jensen (Ed.), *A Handbook of Media and Communication Research* (pp. 235–253). London: Routledge.

Johns, A., & Cheong, N. (2019). Feeling the Chill: Bersih 2.0, State Censorship, and "Networked Affect" on Malaysian Social Media 2012–2018. *Social Media + Society*, *5*(2), 1–12. https://doi.org/10.1177/2056305118821801

Johnson, B. (2013, March 3). This cap on bankers' bonuses is like a dead cat – pure distraction. *The Telegraph*. Retrieved from https://www.telegraph.co.uk/news/worldnews/europe/eu/9906445/This-cap-on-bankers-bonuses-is-like-a-dead-cat-pure-distraction.html

Johnston, R., & Pattie, C. (2011). Where Did Labour's Votes Go? Valence Politics and Campaign Effects at the 2010 British General Election. *The British Journal of Politics and International Relations*, *13*(3), 283–303. https://doi.org/10.1111/j.1467-856X.2011.00454.x

Jordan, T. (2015). *Information politics : liberation and exploitation in the digital society*. London: London : Pluto Press.

Jordan, T., & Taylor, P. A. (2004). *Hacktivism and cyberwars : rebels with a cause?* London: Routledge.

Jowett, G., & O'Donnell, V. (2012). *Propaganda and persuasion*. London: London : SAGE.

Kamal, S. M. (2016, October 18). Ambiga: Death threats 'act of terrorism.' *The Malay Mail*. Retrieved from https://www.malaymail.com/news/malaysia/2016/10/18/ambiga-death-threats-act-of-terrorism/1230237

Kanyakumari, D. (2016, March 12). Chaos when wife of late PI Bala tries to apologise to Rosmah. *The Star*. Retrieved from https://www.thestar.com.my/news/nation/2016/03/12/chaos-wife-of-pi-bala-apologise-to-rosmah

Karpf, D., Kreiss, D., Nielsen, R. K., & Powers, M. (2015). The Role of Qualitative Methods in Political Communication Research: Past, Present, and Future. *International Journal of Communication*, *9*, 1888–1906. Retrieved from https://ijoc.org/index.php/ijoc/article/view/4153

Kasmani, M. F., Sabran, R., & Ramle, N. A. (2014). Who is tweeting on #PRU13? *Asian Social Science*, *10*(18), 144–157. https://doi.org/10.5539/ass.v10n18p144

Kassim, Y. R. (2016). Mahathir & Anwar vs Najib: How Will It End? *RSIS Commentaries*, (54), 1–3. Retrieved from http://hdl.handle.net/10220/40284%0D

Keller, F. B., Schoch, D., Stier, S., & Yang, J. (2017). How to Manipulate Social Media: Analyzing Political Astroturfing Using Ground Truth Data from South Korea. *International AAAI Conference on Web and Social Media; Eleventh International AAAI Conference on Web and Social Media*. Retrieved from https://aaai.org/ocs/index.php/ICWSM/ICWSM17/paper/view/15638

Kelly, S., & Cook, S. (2011). *Freedom of the Net 2011*. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2011

Kelly, S., Cook, S., & Truong, M. (2012). *Freedom of the Net 2012*. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2012

Kelly, S., Truong, M., Shahbaz, A., Earp, M., & White, J. (2017). *Freedom On The Net 2017*. Retrieved from https://freedomhouse.org/report/freedom-net/freedom-net-2017

Kenny, M. (2009). Taking the Temperature of the British Political Elite 3: When Grubby is the Order of the Day … . *Parliamentary Affairs*, *62*(3), 503–513. https://doi.org/10.1093/pa/gsp015

Kenyon, A. T. (2010). Investigating Chilling Effects: News Media and Public Speech in Malaysia, Singapore and Australia. *International Journal of Communication*, *4*, 440–467. Retrieved from http://pirate.24nieuwe.nl/http://ijoc.org/index.php/ijoc/article/view/728

Kessler, C. (1999). A Malay diaspora? Another side of Dr Mahathir's Jewish problem. *Patterns of Prejudice*, *33*(1), 23–42. https://doi.org/10.1080/003132299128810470

Khoo, G. C. (2014). Bersih dan Ubah: Citizenship rights, intergenerational togetherness, and multicultural unity in Malaysia. In *Worlding Multiculturalisms: The Politics of Inter-Asian Dwelling* (pp. 109–126). https://doi.org/10.4324/9781315770192

Kim, S. W., & Douai, A. (2012). Google vs. China's "Great Firewall": Ethical implications for free speech and sovereignty. *Technology in Society*, *34*(2), 174–181. https://doi.org/10.1016/j.techsoc.2012.02.002

King, G., Pan, J., & Roberts, M. E. (2017). How the Chinese government fabricates social media posts for strategic distraction, not engaged argument. *American Political Science Review*, *111*(3), 484–501. https://doi.org/10.1017/S0003055417000144

Klotz, R. J. (2007). Internet Campaigning for Grassroots and Astroturf Support. *Social Science Computer Review*, *25*, 3–12. https://doi.org/10.1177/0894439306289105

Kovic, M., Rauchfleisch, A., Sele, M., & Caspar, C. (2018). Digital astroturfing in politics : Definition, typology, and countermeasures. *Studies in Communication Sciences*, *1*, 69–85. https://doi.org/doi.org/10.24434/j.scoms.2018.01.005

Kumar, K. (2015, December 12). Government agency justifies booklet extolling "Red Shirt" rally, vilifying Bersih 4. *The Malay Mail*. Retrieved from https://www.malaymail.com/news/malaysia/2015/12/12/government-agency-justifies-booklet-extolling-red-shirt-rally-vilifying-ber/1021791

Kumar, K. (2016, January 12). IGP: Immature Internet users forcing cops to crack down on social media. *The Malay Mail Online*. Retrieved from https://www.malaymail.com/news/malaysia/2016/01/12/igp-immature-internet-users-forcing-cops-to-crack-down-on-social-media/1039171#sthash.8Mb1owX1.dpuf

Lasswell, H. D. (1995). Propaganda. In R. Jackall (Ed.), *Propaganda* (pp. 13–25). New York, N.Y.: New York Univ. Press.

Lee, C. W. (2010). the Roots of Astroturfing. *Contexts*, *9*(1), 73–75. https://doi.org/10.1525/ctx.2010.9.1.73

Lee, F. L. F. (2014). Triggering the Protest Paradigm: Examining Factors Affecting News Coverage of Protests. *International Journal of Communication*, *8*, 2725–2746. Retrieved from https://ijoc.org/index.php/ijoc/article/view/2873/1215

Lee, J. C. H. (2008). The Fruits of Weeds: Taking Justice at the Commemoration of the Twentieth Anniversary of Operasi Lalang in Malaysia. *The Round Table*, *97*(397), 605–615. https://doi.org/10.1080/00358530802207435

Lee, J. C. H. (2014). Jom Bersih! Global Bersih and the enactment of Malaysian citizenship in Melbourne. *Citizenship Studies*, *18*(8), 900–913. https://doi.org/10.1080/13621025.2014.964553

Lee, R. M. (1993). *Doing Research on Sensitive Topics*. London: Sage.

Lemière, S. (2018). The Downfall of Malaysia's Ruling Party. *Journal of Democracy*, *29*(4), 114–128. https://doi.org/10.1353/jod.2018.0067

Leong, P. P. Y. (2015). Political Communication in Malaysia: A study on the Use of New Media in Politics. *JeDEM - EJournal of EDemocracy and Open Government*, *7*(1), 46–71. https://doi.org/10.29379/jedem.v7i1.372

Lian, K. F. (2001). The Construction of Malay Identity across Nations: Malaysia, Singapore, and Indonesia. *Bijdragen Tot de Taal-, Land- En Volkenkunde*, *157*(4), 861–879. Retrieved from http://www.jstor.org/stable/27865781

Lievrouw, L. A. (2011). *Alternative and activist new media*. Cambridge; Malden (MA): Polity.

Lim, J. B. Y. (2017). Engendering civil resistance: Social media and mob tactics in Malaysia. *International Journal of Cultural Studies*, *20*(2), 209–227. https://doi.org/10.1177/1367877916683828

Lim, M. (2013). Many Clicks but Little Sticks: Social Media Activism in Indonesia. *Journal of Contemporary Asia*, *43*(4), 636–657. https://doi.org/10.1080/00472336.2013.769386

Lim, M. K. (2009). *Blogging and Democracy: Blogs in Malaysian Political Discourse. PhD Dissertation*. The Pennsylvania State University. https://doi.org/10.1017/CBO9781107415324.004

Liow, J. C. (2012). Malaysia ' s March 2008 general election : *The Pacific Review*, *25*(3), 293–315. https://doi.org/10.1080/09512748.2012.685096

Liu, Y. (2014). *Competitive political regime and Internet control : case studies of Malaysia, Thailand and Indonesia*. Newcastle upon Tyne: Newcastle upon Tyne : Cambridge Scholars Publishing.

Lyon, T. P., & Maxwell, J. W. (2004). Astroturf: Interest group lobbying and corporate strategy. *Journal of Economics and Management Strategy*, *13*(4), 561–597. https://doi.org/10.1111/j.1430-9134.2004.00023.x

MacKinnon, R. (2012). *Consent of the networked : the world-wide struggle for Internet freedom*. New York: Basic Books.

Macwhirter, I. (2014). Scotland's saloon-bar smears. *Public Finance*, *18*(7/8), 18. https://doi.org/10.7208/chicago/9780226394732.001.0001

Mahathir's Dark Side. (2003, October 24). *The Telegraph*. Retrieved from https://www.telegraph.co.uk/comment/telegraph-view/3597972/Mahathirs-dark-side.html

Malaysian news portal crippled by cyberattacks. (2011, April 13). *Agence France-Presse*. Retrieved from https://news.abs-cbn.com/business/tech-biz/04/13/11/malaysian-news-portal-crippled-cyberattacks

Malnick, E. (2018, February 25). Tory hire army of tweeters to take social media fight to Labour. *The Sunday Telegraph*, p. 4. Retrieved from https://www.telegraph.co.uk/politics/2018/02/24/tories-hire-army-tweeters-take-social-media-fight-labour/

Manifesto Rakyat: Pakatan, the People's Hope. (2013, February 26). *The Rocket*. Retrieved from https://www.therocket.com.my/en/manifesto-rakyat-pakatan-the-peoples-hope/

Markham, A. N., Tiidenberg, K., & Herman, A. (2018). Ethics as Methods: Doing Ethics in the Era of Big Data Research—Introduction. *Social Media + Society*, *4*(3), 1–9. https://doi.org/10.1177/2056305118784502

Massanari, A. (2015). #Gamergate and The Fappening: How Reddit's algorithm, governance, and culture support toxic technocultures. *New Media & Society*, *19*(3), 329–346. https://doi.org/10.1177/1461444815608807

Massof, A. (2004). Spam-Oy, What a Nuisance. *Berkley Technology Law Journal*, *19*(2), 625–666. https://doi.org/10.3868/s050-004-015-0003-8

Massoumi, N., Mills, T., & Miller, D. (2019). Secrecy, coercion and deception in research on 'terrorism' and 'extremism.' *Contemporary Social Science*, 1–19. https://doi.org/10.1080/21582041.2019.1616107

Matalin, M., Carville, J., & Knobler, P. (1994). *All's fair : love, war, and running for president*. London: Hutchinson.

Maurer, T. (2015). Cyber Proxies and the Crisis in Ukraine. In K. Geers (Ed.), *Cyber war in perspective : Russian aggression against Ukraine* (pp. 79–86). Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_full_book.pdf

McCauley, T. (2015). The war of ideas on the Internet: An asymmetric conflict in which the strong become weak. *Dynamics of Asymmetric Conflict*, *8*(1), 79–90. https://doi.org/10.1080/17467586.2014.1002511

McNair, B. (2004). PR must die: spin, anti-spin and political public relations in the UK, 1997–2004. *Journalism Studies*, *5*(3), 325–338. https://doi.org/10.1080/1461670042000246089

McNair, B. (2012). *An introduction to political communication*. London; New York: Routledge ;

Meraz, S., & Papacharissi, Z. (2013). Networked Gatekeeping and Networked Framing on #Egypt. *International Journal of Press/Politics*, *18*(2), 138–166. https://doi.org/10.1177/1940161212474472

Miller, D. (2004). *Tell me lies : propaganda and media distortion in the attack on Iraq*. London: Pluto Press.

Miller, D., & Dinan, W. (2008). *A century of spin : how public relations became the cutting edge of corporate power*. London; Ann Arbor, MI: Pluto Press.

Mohamad, M. B. (2002). From Nationalism to Post-Developmentalism: The Intersection of Gender, Race and Religion in Malaysia. *Macalester International*, *12*, 80–102. Retrieved from https://digitalcommons.macalester.edu/macintl/vol12/iss1/12

Mohamed, B. A., Muis, M. A., Salamat, A. S. A., Kamarunzaman, N. Z., Ibrahim, S., Harun, R., & Harun, Z. H. (2011). Control and usage of the virtual space in facing the upcoming 13th general election - a critical evaluation of space and opportunities for Barisan Nasional. *Asian Social Science*, *7*(12), 14–21. https://doi.org/10.5539/ass.v7n12p14

Mohd Azizuddin, M. S. (2014). The Social Media Elections in Malaysia: The 13th General Election in 2013. *Kajian Malaysia*, *32*(1), 119–148.

Mohd Sani, M. A. (2009). *The public sphere and media politics in Malaysia*. Newcastle upon Tyne: Cambridge Scholars Pub.

Morozov, E. (2012). *The net delusion : the dark side of Internet freedom*. New York: Public Affairs.

Moses, B. (2002). Ethnic Reporting in the Malaysian Media. *Media Asia*, *29*(2), 102–106. https://doi.org/10.1080/01296612.2002.11726671

Moten, A. R., & Mokhtar, T. M. (2006). The 2004 General Elections in Malaysia: A Mandate to Rule. *Asian Survey*, *46*(2), 319–340. https://doi.org/10.1525/as.2006.46.2.319

Muhamad, R. (2015). Online opposition and elections in Malaysia. *Asian Social Science*, *11*(10), 281–291. https://doi.org/10.5539/ass.v11n10p281

Murthy, D., Powell, A. B., Tinati, R., Anstead, N., Carr, L., Halford, S. J., & Weal, M. (2016). Bots and Political Influence: A Sociotechnical Investigation of Social Network Capital. *International Journal of Communication*, *10*, 4952–4971. Retrieved from https://ijoc.org/index.php/ijoc/article/view/6271

Nair, S. (2007). The Limits of Protest and Prospects for Political Reform in Malaysia. *Critical Asian Studies*, *39*(3), 339–368. https://doi.org/10.1080/14672710701527345

Navarria, G. (2016). To censor or not to censor: Roots, current trends and the long-term consequences of the Chinese Communist Party's fear of the internet. *Communication, Politics & Culture*, *49*(2), 82–110.

Ndoma, I., & Tumin, M. (2011). Virtual Civil Society: Malaysia's 2008 General Elections Revisited. *Global Journal of Human Social Science*, *11*(8), 1–10.

Net Value: Cyber Wars. (2008, February 25). *The Edge*.

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

Ngeow, C. B. (2017). Barisan Nasional and the Chinese Communist Party: A Case Study in China's Party-Based Diplomacy. *China Review*, *17*(1), 53–82. Retrieved from http://www.jstor.org/stable/44160409

Noor, F. A. (2004). *Islam embedded : the historical development of the Pan-Malaysian Islamic Party PAS, (1951-2003) Vol. 1*. Kuala Lumpur: Malaysian Sociological Research Institute.

Noor, N. M., & Leong, C. H. (2013). Multiculturalism in Malaysia and Singapore: Contesting models. *International Journal of Intercultural Relations*, *37*(6), 714–726. https://doi.org/10.1016/j.ijintrel.2013.09.009

Nowell, L. S., Norris, J. M., White, D. E., & Moules, N. J. (2017). Thematic Analysis: Striving to Meet the Trustworthiness Criteria. *International Journal of Qualitative Methods*, *16*, 1–13. https://doi.org/10.1177/1609406917733847

Nurul Huda, J. (2014). *Malaysia's "social media" Election 2013: Are Voters Becoming Less Cynical?* Universiti of Amsterdam. https://doi.org/10.1177/0739456X9401300405

Oates, S. (2007). The neo-Soviet model of the media. *Europe-Asia Studies*, *59*(8), 1279–1297. https://doi.org/10.1080/09668130701655150

Ooi, K. G. (2017). *Historical Dictionary of Malaysia*. Rowman & Littlefield Publishers, Incorporated.

Osman, M. N. M. (2017). The Islamic conservative turn in Malaysia: impact and future trajectories. *Contemporary Islam*, *11*(1), 1–20. https://doi.org/10.1007/s11562-016-0373-3

Pang, E.-S. (2000). The Financial Crisis of 1997–98 and the End of the Asian Developmental State. *Contemporary Southeast Asia*, *22*(3), 570–593. Retrieved from http://www.jstor.org/stable/25798512

Pearce, K. E. (2015). Democratizing kompromat: the affordances of social media for state-sponsored harassment. *Information, Communication & Society*, *18*(10), 1158–1174. https://doi.org/10.1080/1369118X.2015.1021705

Pepinsky, T. B. (2013). The New Media and Malaysian Politics in Historical Perspective. *Contemporary Southeast Asia*, *35*(1), 83–103. https://doi.org/10.1355/cs35-1d

Petley, J. (2014). The state journalism is in: Edward Snowden and the British press. *Ethical Space: The International Journal of Communication Ethics*, *11*(1/2), 9–18. Retrieved from http://bura.brunel.ac.uk/handle/2438/9676

PI retracts declaration. (2008, July 4). *The Star*. Retrieved from https://www.thestar.com.my/news/nation/2008/07/04/pi-retracts-declaration-updated/

PM left red nosed by censorship protest. (2016, February 3). *BBC News*. Retrieved from https://www.bbc.co.uk/news/blogs-trending-35486530

Pomerantsev, P. (2015). The Kremlin s Information War. *Journal of Democracy*, *26*(4), 40–50. https://doi.org/10.1353/jod.2015.0074

Postill, J. (2014). A Critical History of Internet Activism and Social Protest in Malaysia, 1998-2011. *Asiascape: Digital Asia*, *1*(1–2), 78–103. https://doi.org/10.1163/22142312-12340006

Purdam, K., & Elliot, M. (2015). The Changing Social Science Data Landscape. In P. Halfpenny & R. Procter (Eds.), *Innovations in Digital Research Methods* (pp. 25–58). London: Sage Publications Ltd.

Qualter, T. H. (1962). *Propaganda and psychological warfare*. New York: Random House.

Ramzy, A. (2015, July 24). Malaysia Suspends 2 Newspapers Covering Scandal at State-Owned Fund. *The New York Times*. Retrieved from https://www.nytimes.com/2015/07/25/world/asia/malaysia-suspends-2-newspapers-covering-scandal-at-state-owned-fund.html

Ratkiewicz, J., Conover, M. D., Meiss, M., Gonc, B., Flammini, A., & Menczer, F. (2011). Detecting and Tracking Political Abuse in Social Media. *Artificial Intelligence*, 297–304. Retrieved from http://www.aaai.org/ocs/index.php/ICWSM/ICWSM11/paper/viewFile/2850/3274

Razak, N. (2016, February 26). Netizens for the greater good. *Najibrazak.Com*. Retrieved from https://www.najibrazak.com/bm/blog/netizens-for-the-greater-good/

Reinl, J. (2018, November 23). "Fake news" rattles Taiwan ahead of elections. *Al-Jazeera*. Retrieved from https://www.aljazeera.com/news/2018/11/news-rattles-taiwan-elections-181123005140173.html

Rheingold, H. (2008). *Smart mobs : the next social revolution*. Cambridge, MA: Basic Books.

Robards, B., & Lincoln, S. (2017). Uncovering longitudinal life narratives: scrolling back on Facebook. *Qualitative Research*, *17*(6), 715–730. https://doi.org/10.1177/1468794117700707

Rodan, G. (1998). The Internet and Political Control in Singapore. *Political Science Quarterly*, *113*(1), 63–89. https://doi.org/10.2307/2657651

Rogers, R. A. (2009). Post-democraphic machines. In A. Dekker & A. Wolfsberger (Eds.), *Walled Garden* (pp. 29–39). Amsterdam: Virtueel Platform.

Roozenbeek, J., & van der Linden, S. (2018). The fake news game: actively inoculating against the risk of misinformation. *Journal of Risk Research*, *9877*, 1–11. https://doi.org/10.1080/13669877.2018.1443491

Rozario, K. (2015, July 16). What Malaysia bought from spyware maker Hacking Team. *The Malay Mail Online*. Retrieved from https://www.malaymail.com/news/malaysia/2015/07/16/what-malaysia-bought-from-spyware-maker-hacking-team/934509

Saka, E. (2018). Social Media in Turkey as a Space for Political Battles: AKTrolls and other Politically motivated trolling. *Middle East Critique*, *27*(2), 161–177. https://doi.org/10.1080/19436149.2018.1439271

Salmons, J. (2016). *Doing qualitative research online*. Los Angeles: SAGE.

Samadi, F. (2016, March 7). Social media campaign aims to defend embattled Malaysian PM. *PRWeek*. Retrieved from https://www.prweek.com/article/1386275/social-media-campaign-aims-defend-embattled-malaysian-pm

Sandell, R. (1977). *Linguistic style and persuasion*. London: Academic Press.

Sanderson, J., Barnes, K., Williamson, C., & Kian, E. T. (2016). 'How could anyone have predicted that #AskJameis would go horribly wrong?' public relations, social media, and hashtag hijacking. *Public Relations Review*, *42*(1), 31–37. https://doi.org/https://doi.org/10.1016/j.pubrev.2015.11.005

Sanfilippo, M. R., Fichman, P., & Yang, S. (2018). Multidimensionality of online trolling behaviors. *The Information Society*, *34*(1), 27–39. https://doi.org/10.1080/01972243.2017.1391911

Sanyal, S. (2013). *Mapping the World's Prices 2013*. Retrieved from http://cbs.db.com/new/pdf/Random_Walk_Mapping_Prices_2013.pdf

Saravanamuttu, J., & Mohamad, M. (2019). The Monetisation of Consent and its Limits: Explaining Political Dominance and Decline in Malaysia. *Journal of Contemporary Asia*, 1–18. https://doi.org/10.1080/00472336.2019.1569710

Sarawak Report suffers massive cyber attack. (2011, April 10). *Malaysiakini*. Retrieved from https://www.malaysiakini.com/news/161156

Scheufele, D. A., & Tewksbury, D. (2007). Framing, agenda setting, and priming: The evolution of three media effects models. *Journal of Communication*, *57*(1), 9–20. https://doi.org/10.1111/j.1460-2466.2006.00326.x

Shiozaki, Y. (2007). Formation of public spheres and Islamist movements in Malay Muslim society of Malaysia. *Journal of the Interdisciplinary Study of Monotheistic Religions*, *3*, 98–122.

Shirky, C. (2011). The Political Power of Social Media: Technology, the Public Sphere, and Political Change. *Foreign Affairs*, *90*(1), 28–41. Retrieved from http://www.jstor.org/stable/25800379

Singh, H. (1991). Political Change in Malaysia: The Role of Semangat 46. *Asian Survey*, *31*(8), 712–728. https://doi.org/10.2307/2645225

Sisson, D. C. (2017). Inauthentic communication, organization-public relationships, and trust: A content analysis of online astroturfing news coverage. *Public Relations Review*, *43*(4), 788–795. https://doi.org/10.1016/j.pubrev.2017.05.003

Slater, D. (2003). Iron Cage in an Iron Fist: Authoritarian Institutions and the Personalization of Power in Malaysia. *Comparative Politics*, *36*(1), 81–101. https://doi.org/10.2307/4150161

Smeltzer, S. (2017). Biotechnology, the Environment, and Alternative Media in Malaysia. *Canadian Journal of Communication*, *33*(1), 5–20. https://doi.org/10.22230/cjc.2008v33n1a1865

Soha, M., & McDowell, Z. J. (2016). Monetizing a Meme: YouTube, Content ID, and the Harlem Shake. *Social Media + Society*, *2*(1), 2056305115623801. https://doi.org/10.1177/2056305115623801

Solorio, T., Hasan, R., & Mizan, M. (2013). Sockpuppet Detection in Wikipedia: A Corpus of Real-World Deceptive Writing for Linking Identities. Retrieved from http://arxiv.org/abs/1310.6772

Stauber, J. C., & Rampton, S. (2004). *Toxic sludge is good for you : lies, damn lies and the public relations industry*. London: London : Constable & Robinson.

Steele, J. (2009). Professionalism Online: How Malaysiakini Challenges Authoritarianism. *The International Journal of Press/Politics*, *14*(1), 91–111. https://doi.org/10.1177/1940161208326927

Stoehrel, R. F., & Lindgren, S. (2014). For the Lulz: Anonymous, aesthetics, and affect. *TripleC*, *12*(1), 238–264.

Streckfuss, D. (1995). Kings in the age of nations: The paradox of lese-majeste as political crime in Thailand. *Comparative Studies in Society and History*, *37*(3), 445–475.

Subramaniam, S. (2000). The Asian Values Debate: Implications for the Spread of Liberal Democracy. *Asian Affairs: An American Review*, *27*(1), 19–35. https://doi.org/10.1080/00927670009598827

Suffian, I. (2008). Hintergrundpapier The Successful Role of the Internet in the 2008 Malaysian General Elections, (9), 1–19.

Suffian, I. (2010). *Democratisation & new voter mobilisation in Southeast Asia : reflections of the 2008 Malaysian general election : role of the internet in political communications Reflections of the 2008 Malaysian General Election : Role of the Internet in Political Commu*. (N. Kitchen, Ed.), *IDEAS reports - special reports*.

Sumpter, R., & Tankard, J. W. (1994). The spin doctor: An alternative model of public relations. *Public Relations Review*, *20*(1), 19–27. https://doi.org/10.1016/0363-8111(94)90111-2

Surborg, B. (2008). On-line with the people in line: Internet development and flexible control of the net in Vietnam. *Geoforum*, *39*(1), 344–357. https://doi.org/10.1016/j.geoforum.2007.07.008

Tan, K. (2013, January 13). Cybertroopers, Social Media and the State of Media in Malaysia. *BFM*. Retrieved from https://www.bfm.my/podcast/morning-run/current-affairs/current-affairs-190112-cybertroopers-tun-faisal-hishamudin-rais

Tang, H. W. (2005). Let a Hundred Flowers Bloom: Digital Speech in Malaysia. In *20th BILETA Conference: Over-Commoditised; OverCentralised; Over-Observed: the New Digital Legal World?* De Gruyter. https://doi.org/10.2202/1932-0205.1012

Tapsell, R. (2013a). Negotiating Media "Balance" in Malaysia's 2013 General Election. *Journal of Current Southeast Asian Affairs*, *32*(2), 39–60.

Tapsell, R. (2013b). The Media Freedom Movement in Malaysia and the Electoral Authoritarian Regime. *Journal of Contemporary Asia*, *2336*(June), 1–23. https://doi.org/10.1080/00472336.2013.765138

Tapsell, R. (2018). The Smartphone as the "Weapon of the Weak": Assessing the Role of Communication Technologies in Malaysia's Regime Change. *Journal of Current Southeast Asian Affairs*, *37*(3), 9–29. Retrieved from https://journals.sub.uni-hamburg.de/giga/jsaa/article/view/1146/1153

Tayeb, A. (2013, May 5). Islam at GE13. *New Mandala*.

The Post Stays Up. (2016). Retrieved January 26, 2016, from https://blog.medium.com/the-post-stays-up-d222e34cb7e7

Thomson, O. (1999). *Easily led: a history of propaganda*. Thrupp, Stroud, Gloucestershire: Sutton Pub.

Tourists impressed with Merdeka Day celebration. (2015, August 31). *New Straits Times*.

Tsui, L. (2007). An inadequate metaphor: The great firewall and chinese internet censorship. *Global Dialogue*, *9*(1/2), 60–68. Retrieved from http://www.worlddialogue.org/content.php?id=400%5Cnhttp://search.proquest.com/docview/211504402

Tucker, J. A., Theocharis, Y., Roberts, M. E., & Barberá, P. (2017). From Liberation to Turmoil: Social Media And Democracy. *Journal of Democracy*, *28*(4), 46–59. https://doi.org/10.1353/jod.2017.0064

Ufen, A. (2015). Laissez-faire versus Strict Control of Political Finance: Hegemonic Parties and Developmental States in Malaysia and Singapore. *Critical Asian Studies*, *47*(4), 564–586. https://doi.org/10.1080/14672715.2015.1082263

Uihua. (2016, August 14). What does it take to be a "macai" online? An ex-cybertrooper confesses... *Cilisos*. Retrieved from https://cilisos.my/what-does-it-take-to-be-a-macai-online-an-ex-cybertrooper-confesses/

UMNO leader in bid to oust govt. (2015, August 16). *New Straits Times*, p. 3.

Umno Youth goes on cyber-war footing. (2004, February 25). *New Straits Times*, p. 4.

van der Nagel, E. (2018). Alts and Automediality: Compartmentalising the Self through Multiple Social Media Profiles. *M/C Journal*, *21*(2). Retrieved from http://journal.media-culture.org.au/index.php/mcjournal/article/view/1379

Varkkey, H. (2017). Malaysia in 2016: Persistent Crises, Rapid Response, and Resilience. *Southeast Asian Affairs*, *2017*, 203–219. https://doi.org/10.1355/9789814762878-015

Vendil Pallin, C. (2017). Internet control through ownership: the case of Russia. *Post-Soviet Affairs*, *33*(1), 16–33. https://doi.org/10.1080/1060586X.2015.1121712

Verkamp, J.-P., & Gupta, M. (2013). Five Incidents, One Theme: Twitter Spam as a Weapon to Drown Voices of Protest. In *The 3rd USENIX Workshop on Free and Open Communications on the Internet* (pp. 1–7). Retrieved from https://www.usenix.org/conference/foci13/technical-sessions/papers/verkamp

Vie, S. (2014). In defense of "slacktivism": The Human Rights Campaign Facebook logo as digital activism. *First Monday*, *19*(4). https://doi.org/10.5210/fm.v19i4.4961

Weiss, M. L. (2009). Edging Toward a New Politics in Malaysia: Civil Society at the Gate? *Asian Survey*, *49*(5), 741–758. https://doi.org/10.1525/as.2009.49.5.741

Weiss, M. L. (2012). *Politics in Cyberspace: New Media in Malaysia. fesmedia Asia*. Berlin: fesmedia Asia. Retrieved from http://library.fes.de/pdf-files/iez/09068.pdf

Weiss, M. L. (2013). Malaysia's 13th General Elections: Same Result, Different Outcome. *Asian Survey*, *53*(6), 1135–1158. https://doi.org/10.1525/as.2013.53.6.1135

Weiss, M. L. (2017). Going to the ground (or AstroTurf): a grassroots view of regime resilience. *Democratization*, *24*(2), 265–282. https://doi.org/10.1080/13510347.2016.1160059

Welsh, B. (2011). People Power in Malaysia: Bersih Rally and Its Aftermath. *Asia Pacific Bulletin*, (128). Retrieved from EastWestCenter.org/APB

Whitley, G. L. (2000). *PsyOp Operations In The 21st Century*.

Willnat, L., Wong, W. J., Tamam, E., & Aw, A. (2013). Online Media and Political Participation: The Case of Malaysia. *Mass Communication and Society*, *16*(4), 557–585. https://doi.org/10.1080/15205436.2012.734891

Wong, C.-H. (2018). The Rise, Resilience and Demise of Malaysia's Dominant Coalition. *The Round Table*, *107*(6), 755–769. https://doi.org/10.1080/00358533.2018.1545942

Wong, C.-H., Chin, J., & Othman, N. (2010). Malaysia – towards a topology of an electoral one-party state. *Democratization*, *17*(September 2014), 920–949. https://doi.org/10.1080/13510347.2010.501179

Wong, C.-H., & Ooi, K. B. (2018). Introduction: How Did Malaysia End UMNO's 61 Years of One-Party Rule? What's Next? *The Round Table*, *107*(6), 661–667. https://doi.org/10.1080/00358533.2018.1545944

Wong, C. W. (2011, January 30). Loosen up, not tighten up. *The Star*. Retrieved from https://www.thestar.com.my/opinion/columnists/on-the-beat/2011/01/30/loosen-up-not-tighten-up/

Wong says sorry over 'burn Lynas' threat. (2013, February 9). *The Star*. Retrieved from https://www.thestar.com.my/news/nation/2013/02/09/wong-says-sorry-over-burn-lynas-threat/

Woolley, S. C. (2016). Automating power: Social bot interference in global politics. *First Monday*, *21*(4). https://doi.org/10.5210/fm.v21i4.6161

Woolley, S. C., & Howard, P. (2017). *Computational propaganda*. Retrieved from http://comprop.oii.ox.ac.uk/publishing/working-papers/computational-propaganda-worldwide-executive-summary/

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

Yang, L. F., & Ishak, M. S. A. (2012). Framing Interethnic Conflict in Malaysia: A Comparative Analysis of Newspapers Coverage on the Hindu Rights Action Force (Hindraf). *International Journal of Communication*, *6*(24), 166–189. Retrieved from https://ijoc.org/index.php/ijoc/article/view/1307/690

Yegar, M. (2006). Malaysia: Anti-semitism without Jews. *Jewish Political Studies Review*, *18*(3/4), 81–97. Retrieved from http://www.jstor.org/stable/25834698

Yom, S. L. (2009). Jordan: Ten More Years of Autocracy. *Journal of Democracy*, *20*(4), 151–166. https://doi.org/10.1353/jod.0.0125

Zakaria, N. (2011). Modeling political belief and its propagation , with Malaysia as a driving context, *3*.

Zakaria, N. (2014). Modeling Political Belief and Its Propagation, with Malaysia as a Driving Context. *Open Journal of Political Science*, *4*(2), 58–75. https://doi.org/10.4236/ojps.2014.42008

Zakaria, R. (2017, December). Umno on war footing to face Mother of all elections. *New Straits Times*. Retrieved from https://www.nst.com.my/news/politics/2017/12/311797/umno-war-footing-face-mother-all-elections

Zelenkauskaite, A., & Niezgoda, B. (2017). "Stop Kremlin trolls:" Ideological trolling as calling out, rebuttal, and reactions on online news portal commenting. *First Monday*, *22*(5). https://doi.org/https://doi.org/10.5210/fm.v22i5.7795

Zhang, J., & Carpenter, D. (2013). Online Astroturfing : A Theoretical Perspective. In *19th Americas Conference on Information Systems*.

APPENDIX I

Publication Date	Headline	Publication
25 February 2004	Umno Youth goes on cyber-war footing	New Straits Times
19 March 2004	New generation cyber troopers fight information war	New Straits Times
1 October 2004	Women want the power	New Straits Times
26 July 2007	Raja Petra defiant after eight-hour grilling	The Sun
26 July 2007	A comedy of errors	Malaysia Today
27 July 2007	Umno officials 'behind seditious postings'	The Straits Times Singapore
11 October 2007	Face to face: Raja Petra Kamarudin	Malaysia Today
17 February 2008	Cyber troopers battle for voters	New Straits Times
25 February 2008	Of 'badangs' and 'blogoticians'	Malaysiakini
25 February 2008	Net Value: Cyber Wars	The Edge
7 March 2008	Khairy reaches out to netizens	The Star
25 March 2009	Melayu bukan UMNO lagi, Melayu sudah minoriti…	Utusan Malaysia
27 July 2009	Tidak sukar tawan Selangor	Sinar Harian
29 July 2009	ISA, 13 Mei 1969 dan notebook Beng Hock	Utusan Malaysia
22 August 2009	Mud-slinging goes on despite Ramadan	New Straits Times
28 December 2009	Blogosphere guide	The Star
11 January 2010	The long fuse leading to the church fire bombings	Malaysia Today
26 January 2010	Aide: CM's name used to post seditious remarks	The Star
6 February 2010	Commission probes YouTube clips	The Star
6 August 2010	Education without wisdom	FMT
18 August 2010	Only way for MCA, Gerakan to teach Umno respect is leave BN	Malaysia Chronicle
3 September 2010	MCMC slammed for picking on blogger Irwan, cracking down on Net	Malaysia Chronicle
20 September 2010	Guan Eng nafi wang ihsan hasil judi	Sinar Harian
5 October 2010	Teo's surau visit: 'Police probe a comedy'	FMT
20 October 2010	Youth needs to do more	The Star
9 November 2010	Why I almost choked on my pizza	Malaysia Chronicle
16 November 2010	More than one hand in the cookie jar	The Sun
7 February 2011	Politicians marshal cyberspace 'forces'	New Straits Times
8 February 2011	Political Net will grow bigger	New Straits Times
11 February 2011	There once was a dream called Malaysia: Now a gap between image and reality	Malaysia Chronicle
22 February 2011	Hala tuju MCA, masyarakat Cina masih samar	Sinar Harian
8 April 2011	Masing to ensure more roads in Baleh	The Star
11 April 2011	Expect more crashes on the Net	FMT
3 May 2011	With truth comes credibility	The Sun
13 June 2011	Umno cybertroopers told to act	The Star
10 July 2011	ALERT: Guidance on BERSIH rally (RAHSIA)	Malaysia Today
27 July 2011	TBH inquisition reveals racist underpinnings	Malaysia Today
7 August 2011	You need brains to do it (UPDATED)	Malaysia Today

15 August 2011	Penang govt did not bribe The Economist, says Lim	The Star
15 August 2011	Article was publisher's initiative: Lim	The Sun
21 August 2011	More calls for Sivarraajh's suspension to be lifted	The Star
29 August 2011	Is MCA in its death throes?	FMT
1 September 2011	Managing information in the cyber age	Malaysian Business
15 October 2011	Media baru pro-PR dilarang fitnah lawan	Sinar Harian
26 October 2011	Guan Eng under siege	Malaysia Today
29 October 2011	Prove me wrong Soi Lek, sack Tee Keat	Malaysia Chronicle
1 November 2011	The challenge of neo-politics	Malaysian Business
22 November 2011	The rising Net value	The Star
23 November 2011	Guan Eng a hypocrite, says MCA man	The Star
2 December 2011	Two thumbs up from Dr M	The Star
5 December 2011	From tweets to public debate	The Star
5 December 2011	Umno versus Najib	The Edge
15 December 2011	iStrategi dan Perang Alam Maya	Utusan Malaysia
18 December 2011	Khalid: DAP itself cannot shed anti-Malay image	The Star
28 December 2011	Shahrizat's next move: Will it trigger an all-out Umno revolt against Najib	Malaysia Chronicle
2 February 2012	Social media power not to be down-rated	Malay Mail
14 February 2012	'Social media changes politics'	Malay Mail
15 February 2012	John Soh, the brains behind Anwar	FMT
19 February 2012	Make greater use of digital media, Barisan parties urged	The Star
8 March 2012	MCA-DAP debate evokes request for more	New Straits Times
8 March 2012	Chief: We're no cyber troopers	The Star
13 March 2012	CAP: We will not back down	New Straits Times
14 March 2012	'Old man' Idris vows to fight on	The Star
15 March 2012	An old man and street fighter lock horns	The Star
16 March 2012	CM blames daily over spat	New Straits Times
17 March 2012	It takes courage to ask the right questions	New Straits Times
18 March 2012	Big plans, even bigger dreams	The Star
20 March 2012	Integrity the order of the day	The Star
20 March 2012	Era keterbukaan dan pendedahan	Sinar Harian
20 March 2012	R&D on the rise	Malay Mail
22 March 2012	Going for online battle	The Star
1 April 2012	Resolving issue with sincerity	New Straits Times
3 April 2012	The ugly side of TwitterJaya	The Star
7 April 2013	Malaysian politicians go all a-Twitter	The Straits Times Singapore
9 April 2012	Cyber troopers 'out to tarnish image'	New Straits Times
13 April 2012	Pembangkang hina Raja Melayu?	Utusan Malaysia
13 April 2013	PAS dismisses sex video as 'fake'	The Straits Times Singapore
25 April 2012	Newspaper's motive in question	The Star
27 April 2012	Transformasi PM mampu 'tawan' pengundi	Berita Harian
29 April 2012	Cracking the 'eggs' in Penang	The Star
3 May 2012	Taiwan-style politics may backfire on opposition	New Straits Times
9 May 2012	Lim Teck Ghee responds to Chandra Muzaffar's refusal to engage on the Net and his threat	Malaysia Today
10 May 2012	Sentiasa berusaha dekati golongan muda	Utusan Malaysia

10 May 2012	'Enemy' within facing a fallout	The Star
20 May 2012	Perak BN fans set up site to fight slander	New Straits Times
21 May 2012	Bung Mokhtar a hit in Twitterjaya	The Star
30 May 2012	The gentleman in Aziz gives way	The Star
5 June 2012	BN sounds election siren	Malay Mail
5 June 2012	Penang Barisan reveals strategy for general election	The Star
6 June 2012	Uncertainties of the Evidence Act	The Sun
6 June 2012	BN turns to 10,000 cyber-troopers	Malay Mail
11 June 2012	Penang BN beats the war drums	The Star
13 June 2012	Najib leads in social media catch-up with opposition	The Straits Times Singapore
18 June 2012	From 'court-appointed' to people's MB	Malay Mail
29 June 202	Penang BN in gear for cyber war	The Star
4 July 2012	SUPP all set to face polls, says Youth sec-gen	The Star
15 July 2012	On the wrong side of the media	The Star
15 July 2012	Kerajaan PKR, DAP gagal sedia tapak sekolah	Berita Harian
9 August 2012	PM's cyberfans can help win votes	Malay Mail
9 August 2012	BN Youth seeks to reclaim cyberspace	Financial Daily
12 August 2012	'My approach is to never let people down'	New Straits Times
16 August 2012	Changing rule of information war	Malaysian Business
17 August 2012	The day the Tweets went silent	The Star
19 August 2012	Hate-and-blame game goes on	The Star
23 August 2012	Up close and personal with Saifuddin	The Sun
28 August 2012	Umno denies link to controversial Facebook fan page	The Sun
16 September 2012	Talking politics	New Straits Times
19 September 2012	Why should politics be in black and white?	FMT
23 September 2012	Political feuds ala Ah Long in Penang	The Star
11 October 2012	Online political campaign: Friend or foe?	Malay Mail
13 October 2012	Integral social tool	The Star
14 October 2012	'Win or lose, MCA is always there to serve'	New Straits Times
22 October 2012	Stop working against our graft busters	Malay Mail
31 October 2012	Congrats Guan Eng, you can actually become PM	Malay Mail
12 November 2012	Better content will sway the voter	Financial Daily
15 November 2012	'Little kid' with big ambitions	The Star
20 November 2012	Campaigning goes the digital way	Financial Daily
20 November 2012	Martabat bangsa jadi agenda Puteri	Utusan Malaysia
26 November 2012	Media perdana tidak bersatu punca BN kalah PRU12	Sinar Harian
28 November 2012	Creating avenues for youths	New Straits Times
29 November 2012	Puteri syor skuad penggerak	Berita Harian
29 November 2012	Call to arms	The Sun
1 December 2012	Umno's new terms of engagement	New Straits Times
24 December 2012	How to win the social media war	The Star
6 January 2013	Troubling diatribes	The Star
13 January 2013	An unholy mix	The Star
27 January 2013	Tunku Aziz: DAP tried to lure prince with MB post	The Star
6 February 2013	Low press ranking a 'hatchet job'	New Straits Times
10 February 2013	Najib limbers up for the final lap	The Star

15 February 2013	It was 'YES' to PM	Malay Mail
22 February 2013	Terengganu BN confident of victory	New Straits Times
24 February 2013	'We are here to help win hearts'	New Straits Times
4 March 2013	Our first social media general election	Malay Mail
7 March 2013	Stand together	New Straits Times
10 March 2013	Mega project under scrutiny	The Star
15 March 2013	NGO acts against online bullies	The Star
15 March 2013	The show must go on	The Star
16 March 2013	Cops deserve our gratitude, loyalty	New Straits Times
16 March 2013	It's a social media world	Malaysian Business
17 March 2013	BN gears up for cyber war	The Star
18 March 2013	Jacel excitement for cybertroopers	New Straits Times
23 March 2013	CM under fire for tunnel move	New Straits Times
23 March 2013	Cyberspace bullying getting out of hand	The Star
25 March 2013	Guan Eng faces more protests	New Straits Times
26 March 2013	Penang DAP revamps website, goes into campaign mode	The Star
29 March 2013	DAP has little success to show	New Straits Times
31 March 2013	The battle starts in the cyber world	The Star
31 March 2013	Taking on the opposition in their home ground	The Star
1 April 2013	Teng: Barisan united on wresting Penang	The Star
4 April 2013	War begins officially but battle began two years ago	Malay Mail
4 April 2013	The role of tech in the polls	The Star
5 April 2013	Grooming leaders of tomorrow	The Sun
8 April 2013	War of promises' on road to Putrajaya	Malay Mail
11 April 2013	Selangor MCA uses political videos to attract youths	The Star
12 April 2013	Online campaigns get nasty	The Star
12 April 2013	This week's tag: #Cybertroopers	The Star
12 April 2013	Political troopers	The Star
12 April 2013	Barisan all ready to slug it out in cyberspace	The Star
12 April 2013	Un-faking it	The Star
12 April 2013	Don't cross the line, MCMC warns Netizens	The Star
18 April 2013	Tee Yong on song in Labis	The Star
20 April 2013	Fighting in the fields, streets, hills – and now in cyberspace	The Star
22 April 2013	Servant attitude worthy of your vote	The Edge
22 April 2013	Kit Siang: Beware of cyber-troopers	The Star
24 April 2013	Chua: Stop using scare tactics	The Star
27 April 2013	Setting the record straight	The Star
28 April 2013	Matriarch's blessing keeps Ronald Gan going	The Star
28 April 2013	Cyber bullies take it out on 'traitors'	The Star
28 April 2013	Are we not a tolerant society?	The Star
30 April 2013	Is social media being used to incite violence?	FInancial Daily
1 May 2013	Actor lodges report over FB bullying	New Straits Times
1 May 2013	DAP sabotaging me, says Lee	New Straits Times
1 May 2013	'I believe in the 1Malaysia vision'	New Straits Times
2 May 2013	Beware of DAP's cyber troopers	New Straits Times
2 May 2013	Love is still in the air	New Straits Times
2 May 2013	Jawi campaigner hopes to turn town into logistics hub	The Star

3 May 2013	DAP's 'Red Bean Army' firing on all cylinders	The Star
3 May 2013	Being fair to all parties	The Star
3 May 2013	Don't be caught in the crossfire, public advised	The Star
3 May 2013	It's a dirty war in cyberspace	The Star
3 May 2013	Southern tsunami 'not happening'	New Straits Times
3 May 2013	'Red Bean spells trouble'	New Straits Times
4 May 2013	Opposition's desperate tactics	New Straits Times
4 May 2013	Of DAP's hairstyles and hypocritical viciousness	New Straits Times
4 May 2013	A vibrant political landscape	New Straits Times
4 May 2013	'Un-friending' over politics	The New Paper Singapore
5 May 2013	The mother of all battles	The Star
5 May 2013	The Quotes	The Star
7 May 2013	Barisan needs to improve cyber war strategy, says Tan	The Star
10 May 2013	DAP miscasts free speech and ideas as racism	New Straits Times
12 May 2013	Zin blames PR cybertroopers	The Star
12 May 2013	Dakyah 'dunia siber' punca pengundi Cina tolak BN	Utusan Malaysia
13 May 2013	EC to get tough	New Straits Times
13 May 2013	A fraudelent culture?	The Sun
14 May 2013	Election body to get tough on those claiming electoral fraud	The New Paper Singapore
14 May 2013	Social Media win for Malaysia's opposition	The New Paper Singapore
15 May 2013	'Hypocrites' must face the music	The Sun
18 May 2013	BN terima keputusan Joseph	Utusan Malaysia
19 May 2013	Anwar patut bersara	Utusan Malaysia
19 May 2013	Yap: MCA must discard its political baggage	New Straits Times
19 May 2013	Waytha says he will prove critics wrong	New Straits Times
21 May 2013	Straightening out social media fables	New Straits Times
21 May 2013	The best ways to national unity	The Star
21 May 2013	Naluri anak muda PRU-14?	Utusan Malaysia
25 May 2013	Cynicism can't fight corruption	New Straits Times
25 May 2013	Gambar 'black out' lakonan: SPR	Sinar Harian
25 May 2013	Sekat sebelum parah	Utusan Malaysia
25 May 2013	Segera bertindak terhadap Red Bean Army	Utusan Malaysia
26 May 2013	KDN tangani fitnah siber	Utusan Malaysia
26 May 2013	Home Ministry to check on unlawful online content	New Straits Times
26 May 2013	Net a game-changer in politics	New Straits Times
26 May 2013	'Anwar using Red Bean Army to incite hatred'	New Straits Times
26 May 2013	KDN, SKMM kerjasama pantau media sosial	Sinar Harian
27 May 2013	Noose tightens	Malay Mail
27 May 2013	Campaign of lies, deception	New Straits Times
27 May 2013	Remaja perlu celik undang-undang	Utusan Malaysia
27 May 2013	Red Bean Army serang Ahmad Zahid	Utusan Malaysia
28 May 2013	Daim: Anwar tetap mahu jadi PM hingga saat kematian	Utusan Malaysia
28 May 2013	Red Bean Army serang kerajaan	Utusan Malaysia
29 May 2013	Hotel says it does not know of group's activities	New Straits Times
29 May 2013	DAP reps stage walkout, say minister's political tirade abuse of position	The Star

29 May 2013	Who's the enemy of our land?	Malay Mail
1 June 2013	Penglibatan syarikat elektronik Taiwan disiasat	Utusan Malaysia
1 June 2013	Polis kenal pasti	Utusan Malaysia
2 June 2013	Ambil tindakan terhadap Red Bean Army - NGO	Utusan Malaysia
2 June 2013	Deputy IGP aims guns at cyber criminals	The Star
2 June 2013	Red Bean Army semakin gelisah	Utusan Malaysia
3 June 2013	Lim: Panel boss must be from the Opposition	The Star
3 June 2013	Guan Eng: DAP did not finance Red Bean Army	Malay Mail
3 June 2013	Pakatan denies link with 'army'	New Straits Times
4 June 2013	Father of Pendrive' mulls legal action against Utusan over report	Malay Mail
4 June 2013	Police to crack down on seditious postings	New Straits Times
5 June 2013	Trust deficit exists when there is no level playing field	Malay Mail
5 June 2013	Youth chief: We need more votes from bumiputras to create balanced electoral roll	The Star
5 June 2013	Illegal hill clearing culprit will pay the price, says Guan Eng	The Star
5 June 2013	The abuse of social media	The Star
5 June 2013	Tindakan pengecut Ketua Menteri Pulau Pinang alih isu Red Bean Army	Utusan Malaysia
8 June 2013	'Going it alone' not right	New Straits Times
9 June 2013	Red Bean Army makin berani atau makin panik?	Utusan Malaysia
9 June 2013	Bean me up, Red Army	The Star
9 June 2013	No beans about it	The Star
9 June 2013	Derived from Mao's 'Red Guards'	The Star
10 June 2013	PR must take heat for 'Red Bean Army', says activist	Malay Mail
10 June 2013	'Boleh hancurkan negara'	Utusan Malaysia
10 June 2013	Dua pemimpin DAP didakwa dalang Red Bean Army	Utusan Malaysia
11 June 2013	Glowing tribute to Latifah	The Star
18 June 2013	Defending a venerable institution	New Straits Times
19 June 2013	Flashmob cabar tindak balas PDRM	Utusan Malaysia
20 Jun 2013	Statements on ISA by ministers worrying, says Mas Gading PKR	The Star
22 June 2013	Tubuh Suruhanjaya Diraja	Utusan Malaysia
25 June 2013	Report lodged over insulting FB posting	New Straits Times
26 June 2013	'Sally Yen' in big trouble	The Star
30 June 2013	'Transforming MCA is a do-or-die mission now'	New Straits Times
3 July 2013	RCI on Red Bean Army being mulled	New Straits Times
3 July 2013	'Cyber crime court' formation suggested	The Sun
3 July 2013	Leave the country, says Bung	The Star
3 July 2013	Umno cybertroopers' conspiring to rake in millions, says Kit Siang	Malay Mail
4 July 2013	'Loss will be big blow for Najib'	Malay Mail
4 July 2013	Utusan pertahan hak, kepentingan Melayu	Utusan Malaysia
5 July 2013	What Red Bean Army HQ?	Malay Mail
6 July 2013	Millennials are here to stay	New Straits Times
11 July 2013	Red Bean Army may face action	New Straits Times
16 July 2013	EC not happy over way postal ballots are delivered	The Star
22 July 2013	Menteri sokong Semut	Sinar Harian
27 July 2013	'We will fight any attempt to de-register DAP'	The Star

22 July 2013	Volunteers welcome to monitor seditious posts	The Star
23 July 2013	Group lodges report over 'insulting' FB posting	The Star
14 August 2013	No show by 'Father Augustus', Kit Siang seeks public inquiry	Financial Daily
18 November 2013	Koyak usul: Bung terima serangan cybertrooper	Sinar Harian
21 November 2013	Call to beef up PAS 'red army'	The Star
26 November 2013	Perak MB hosts dinner for media	New Straits Times
8 December 2013	Much ado over handling of floods	New Straits Times
19 December 2013	Ong agrees to debate, says election should not be about teams	New Straits Times
21 December 2013	21 resolutions passed at wing's assembly	New Straits Times
31 December 2013	A year in R.AGE	The Star
19 January 2014	BN lebih bersopan hadapi tohmahan pembangkang	Berita Harian
23 January 2014	Vernon: Existing legislation sufficient to penalise cyber offenders	The Star
3 February 2014	All abuzz over 'Kajang Move'	The Star
24 February 2014	Countering false information	The Star
2 March 2014	Mengapa rakyat perlu bangkit menentang RBA	Utusan Malaysia
2 March 2014	Tentera Kacang Merah dan 'blogger hantu raya'	Utusan Malaysia
7 March 2014	Kit Siang: Explain action against extremists	Malay Mail
10 March 2014	Cybertroopers rapped over MH370 stories	New Straits Times
12 March 2014	Opposition cybertroopers rapped for being insensitive	New Straits Times
14 March 2014	'Red Bean Army insensitive'	New Straits Times
18 March 2014	'Stop insensitive postings on MH370'	New Straits Times
20 March 2014	Red Bean Army rapped	New Straits Times
21 March 2014	RBA sudah sampai peringkat menghina negara	Utusan Malaysia
23 March 2014	Act over postings, cops told	New Straits Times
28 March 2014	Red Bean Army 'syaitan' siber - NGO	Utusan Malaysia
29 March 2014	RBA penjenayah siber gugat keamanan negara	Utusan Malaysia
30 March 2014	Red Bean Army behind 'nasty' postings	New Straits Times
3 April 2014	MCA sokong nama Red Bean Army diserah kepada Kementerian Dalam Negeri	Utusan Malaysia
3 April 2014	'Red Bean Army posts can hurt ties with China'	New Straits Times
4 April 2014	800 senarai nama RBA sudah diserah kepada KDN	Utusan Malaysia
4 April 2014	Lim: Don't leave Opposition out of MH370 briefing	The Star
9 April 2014	Banning in age of the Internet	The Star
12 April 2014	Kubu RBA di laman sosial perlu dirobohkan	Utusan Malaysia
14 April 2014	Wujudkan Blue Wave Army lawan fitnah jahat RBA	Utusan Malaysia
15 April 2014	Tubuh Suruhanjaya Siasatan Diraja cari dalang RBA	Utusan Malaysia
16 April 2014	Penubuhan RCI mampu tangani isu RBA	Utusan Malaysia
18 April 2014	Stop hudud agenda or quit, DAP told	The Star
22 April 2014	Segerakan Suruhanjaya Diraja siasat ancaman RBA	Utusan Malaysia
29 April 2014	RBA boleh didakwa pelbagai akta	Utusan Malaysia
30 April 2014	NGO: Where does Red Bean Army get funds?	New Straits Times
1 May 2014	Red Bean Army tiada beza dengan kumpulan militan?	Utusan Malaysia
3 May 2014	'Find out RBA's role in rally'	New Straits Times
10 May 2014	Segera kekang aktiviti RBA	Utusan Malaysia
26 May 2014	The lady Dyana and other political updates	The Edge
10 June 2014	Our economy is robust, no matter what others say	New Straits Times

15 July 2014	Mukhriz enggan layan, ambil sikap berdiam diri	Sinar Harian
26 July 2014	The cyber lynching of Kiki Kamarudin	The Heat
31 August 2014	Campaign success an MCA boon	The Star
21 September 2014	Berhemah tegur presiden	SInar Harian
14 October 2014	MP left red-faced after raising hoax about armoured car for Guan Eng	Malay Mail
18 November 2014	Beri peluang orang muda tonjol bakat kepemimpinan	Berita Harian
27 November 2014	Instilling fighting spirit in leaders	New Straits Times
5 December 2014	Sambutlah kerja keras Najib…	Utusan Malaysia
7 January 2015	Siapa ganti Mohamed Sharil?	Utusan Malaysia
12 January 2015	IGP should not take orders from third party sources	Malay Mail
13 January 2015	LFL co-founder detained	New Straits Times
1 February 2015	Doing it her (moderate) way	The Star
11 March 2015	US govt site removes Anwar petition	New Straits Times
6 March 2015	'Cooperation needed to combat IS on social media'	The Star
12 March 2015	White House petition reinstated, hits 100,000-signature goal	Malay Mail
20 March 2015	Police urge scholars to counter IS ideologies	New Straits Times
27 March 2015	My sympathies for G100	Malay Mail
4 April 2015	Govt posts in high demand	New Straits Times
11 April 2015	Internet challenge for media owners	The Star
14 April 2015	Taking anti-terror fight to schools	Malay Mail
21 June 2015	Pakatan's 'seven-year itch'	The Star
17 July 2015	Leaders relay heartfelt messages for racial harmony	The Star
1 August 2015	Blowing the whistle on whistleblowers	Focus Malaysia
14 August 2015	Hackers want attention, say experts	The Star
16 August 2015	'UMNO leader in bid to oust govt'	New Straits Times
31 August 2015	'Bersih fails to attract Malays'	New Straits Times
25 October 2015	Saifuddin: It's just a rumour	The Star
24 January 2016	Banking on the basics	Sunday Star
30 January 2016	'Nafas baru' Penerangan UMNO	Utusan Malaysia
27 February 2016	PM: Be cautious in using social media	New Straits Times
14 March 2016	Rats, it's an epidemic problem	The Star
21 April 2016	Traditional media still a crucial tool for BN	The Star
9 May 2016	A rude wake-up call for DAP	The Star
11 May 2016	DAP rapped for not censuring rep ober 'racist' speech	The Star
12 May 2016	Lim slammed for backing Hew over statement	The Star
12 May 2016	DAP is better off without foul-mouthed Hew	New Straits Times
11 July 2016	'Saya jadi mangsa cyber troopers'	Sinar Harian
11 July 2016	MCA supports wiping our terrorists	The Star
14 July 2016	'DAP should be tactful'	The Star
14 July 2016	Nazri: Two wrongs don't make a right	Malay Mail
17 July 2016	Think before you leap	Sunday Star
5 August 2016	IS eyes Southeast Asia after Mideast losses	New Straits Times
27 November 2016	'Party is strong at its core'	New Sunday Times
29 November 2016	'Tangkis serangan luar, dalam'	Sinar Harian
7 December 2016	'Propaganda UMNO, BN'	SInar Harian
11 December 2016	Hipokrasi pemimpin DAP	Mingguan Malaysia

21 December 2016	Waspada jalan fitnah	Utusan Malaysia
8 January 2017	Vote for MCA, Chinese told	Sunday Star
23 January 2017	Zahid: Learn to master social media	New Straits Times
23 January 2017	Zahid: Public perception of govt low	The Sun
23 January 2017	'Umno will crumble if not online savvy'	The Star
25 February 2017	Who's driving Sabah's election campaign?	The Star
25 March 2017	Last eight delight for Smart Focus	The Star
17 April 2017	JR Plus to centre on people's interest	New Straits Times
27 April 2017	Politikus tunggu impak muktamar	Sinar Harian
14 June 2017	Hafiz kesal sertai Bersatu	Sinar Harian
7 July 2017	Selangor DAP rapped for mocking Chong	The Star
7 July 2017	Selangor DAP rapped for mocking Chong	The Star
8 July 2017	MCA protests Selangor's lack of action over shops' relocation	The Star
2 September 2017	'Citizen' producer all praise for Liow	The Star
6 September 2017	Ti: 'Citizens' parody shows DAP's true face	The Star
1 October 2017	Dr M fishes in Sarawak waters	Sunday Star
25 October 2017	'No issues with funding'	The Star
5 November 2017	'Dr M photo taken last year'	New Sunday Times
5 November 2017	'Cybertroopers should have acted earlier on Sarawak Report story'	New Sunday Times
12 November 2017	Wanted: Leaders who listen	Sunday Star
8 December 2017	Najib: 5 key thrusts to win polls	New Straits Times
17 December 2017	Zahid: We're ready for dirty attacks	Sunday Star
25 December 2017	AI poised to dominate general election	The Star
27 December 2017	'We're ready to counter misinformation'	The Star
30 December 2017	Gazing into the crystal ball for 2018	The Star
9 January 2018	Ready to engage in GE cyberwar	The Star
10 January 2018	Mah: Politicians are prime targets as GE14 nears	The Star
31 January 2018	Wipe out the menace of corruption through death penalty	The Star
7 February 2018	State: 'White' lanterns were yellow at first	The Star
20 March 2018	The silly season has arrived	The Star
18 April 2018	Santhara hopes to upset Subra in Segamat	The Star
25 April 2018	Nurul Islam: I am not a Bangladeshi	The Star
22 April 2018	Facebooking the election	Sunday Star
2 May 2018	Elderly man pushed off stage suffers fractured ribs	The Star
9 May 2018	Big data and the big day: Tech's effect on GE14	The Star
9 May 2018	State BN hopes for breakthrough of winning more than 10 seats	The Star
16 May 2018	Stop the scaremongering tactics	The Star
26 July 2018	SMS Your Views	The Star
21 August 2018	There's fear of reprisal for speaking up	The Star
10 September 2018	'Ruler and I being monitored'	The Star
11 September 2018	Cops: We're not keeping tabs on Johor royal family	The Star
23 September 2018	A tale of two heads	Sunday Star
4 February 2019	The divide will break us apart	The Star
7 February 2019	Subtle smear campaign launched against Warisan	The Star
8 February 2019	People's problems highlighted on social media are real, says Yong	The Star

APPENDIX II

This version of the organogram of former Prime Minister Najib Razak's alleged communication operations is recreated here for clarity. The layout has been changed to accommodate formatting for this thesis.