Competitive Political Regime and Internet Control

Competitive Political Regime and Internet Control: Case Studies of Malaysia, Thailand and Indonesia

By

Liu Yangyue

CAMBRIDGE
SCHOLARS

PUBLISHING

Competitive Political Regime and Internet Control:
Case Studies of Malaysia, Thailand and Indonesia
By Liu Yangyue

This book first published 2014

Cambridge Scholars Publishing

12 Back Chapman Street, Newcastle upon Tyne, NE6 2XX, UK

British Library Cataloguing in Publication Data
A catalogue record for this book is available from the British Library

ISBN (10): 1-4438-5694-0, ISBN (13): 978-1-4438-5694-2

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF MAPS

LIST OF TABLES

ACKNOWLEDGEMENTS

This book appears in its current form due to the assistance and guidance of a great many people, though some of them may not be mentioned here. I owe my deepest debt of gratitude to my PhD supervisor, Professor William Case, who brought me into this fascinating field and guided me with great patience and valuable insights. Every conversation with him (as well as the occasional debates about a number of conceptual and theoretical issues) is of extraordinary value for me. I also enjoyed a lot when he kindly showed me around the historical sites in Jakarta during my field trip.

Numerous colleagues and friends provided comments and suggestions on various parts of the manuscript. Graeme Lang and Jonathan London in City University of Hong Kong carefully read my annual reports and gave me important advice. He Zhou and Jason Abbott offered valuable advice and criticism, and I have worked hard to implement their suggestions. Many teachers in the Department of Asian and International Studies (CityU) helped me in various ways. I am indebted to Paul Cammack, Chan Yuk Wah, Federico Ferrara, Kyaw Yin Hlaing, Lee Tae-dong, Justin Robertson, Nicholas Thomas, Mark Thompson and Robert Taylor. David Zweig at Hong Kong University of Science and Technology also supported my study at various stages, for which I'm extremely grateful. I also received useful feedback from audiences at seminars or conferences where I presented material from the book. These include talks at CityU, the Chinese University of Hong Kong, the Shue Yan University and Massey University. My new institution at the National University of Defense Technology (NUDT) in China provided generous support and encouragement.

For financial support, I wish to acknowledge the CityU and AIS which generously supported my field trips as well as other research-related activities. Center of International Studies and Group of Cultural Security Studies at the NUDT also provided support in this publication. My editor at the Cambridge Scholars Publishing offered substantive feedback, guidance, and encouragement, for which I am grateful.

This book would not have been possible without the cooperation of my interviewees in Malaysia, Thailand and Indonesia, who were so generous with their time and information, and made my field research so rewarding

and enjoyable. Special thanks to Elok Robert Tee who treated me cordially in Kuala Lumpur.

As always, my parents, Liu Jifeng and Yang Baifang, and other family members have given me their unequivocal support throughout my life. My wife, Wu Haijing, has stayed with me throughout the years. This book would not have been completed without her love, patience, and support. For their love and sacrifice, I dedicate this book to them.

CHAPTER ONE

INTRODUCTION

Politics in the Information Age

When Malaysia became the first country in Southeast Asia to offer Internet access to the public in 1994, the aim of transforming Malaysia into a global IT hub and building an Asian Silicon Valley was considered so important and strategic by its Prime Minister Mahathir Mohamad, that his government pledged in 1996 that there would be no censorship of the Internet (Rodan 2004). However, as the Internet penetration rate increased exponentially in the following decade, not only was Malaysia's social-political structure dramatically affected by the unequal empowerment of Internet communications, but the ambitious and attractive rhetoric by the government also changed. On the one hand, flexible yet effective use of the Internet in the 2008 electoral campaign by opposition parties forced Mahathir's successor, Abdullah Badawi, to admit afterwards that the de facto single dominant party-alliance BN (Barison Nasional) "lost the Internet war" (*New York Times* 2008). On the other hand, in addition to increasing surveillance of Internet content and harassment of dissident bloggers and online activists, an Internet filtering project, similar to China's proposed "Green Dam", was under consideration by the Malaysian Ministry of Information (Koswanage 2009).

Meanwhile, another story in China is noteworthy. On 13th January 2011 the Internet giant, Google, announced on its blog that it would end its operations in China since it was no longer willing to censor, as the government required, its Chinese version of the search engine, google.cn (BBC 2010). Although the Chinese government attempted to depoliticise this discord and label it as a pure business event, US Secretary Hilary Clinton's remark supporting Google, together with the worldwide public discussion and debate on the Internet, sovereignty, and security, has endowed the Google issue with much political significance. Much speculation has been made on whether this transnational magnate should coordinate with China's regulatory system, or vice versa. Nonetheless, these two stories are just the epitome of various conflicts and struggles between ever-rising Internet developments and diverse political systems.

The last two decades have witnessed a tremendous expansion of the Internet all over the world, especially in Asia where economies experienced the most rapid growth. It was reported that the number of global users of the Internet in 2009 climbed to 1,734 million in total, and the average penetration rate has reached 25.6%, with 74.2% in North America and 52.0% in Europe (Internet World Stats 2009). By contrast, Internet user distribution in East Asia mapped a striking discrepancy between extremely high levels of Internet penetration in countries such as Japan (75.5%), South Korea (77.3%), and Singapore (72.4%), as compared to some latecomers such as Cambodia (0.5%), Laos (1.9%), and Burma (0.2%). As a rising player in the international arena and one of the most influential powers in Asia, China has expanded its Internet user number from around 17 million in 2000 to 591 million in 2013, and is currently the largest population in the world with Internet accessibility (CNNIC 2000; 2013).

As information technologies evolved gradually and accessibility to the Internet increased dramatically, this newly developed technical system is reshaping people's life style and habits, restructuring economic structures, and most importantly, reforming politics all over the world. The era of the Internet has at least a fourfold political implication: first, national governments all over the world have to deal with a technological system which is, to some extent, internationally uniform and standardised by several leading companies and organisations; second, almost every state seeks to promote Internet development as a symbol of modernisation and globalisation, and as a means to obtain political legitimacy and public support for its leadership; third, the Internet has greatly influenced the political and social systems both domestically and globally by empowering different social groups and political parties, giving rise to the changing nature of political participation and the flexible expression of dissident, even extremist outlooks; last, Internet development has been distorted by persistent efforts by governments to control it politically. Such methods of control vary from specific content filtering to a general regulatory framework.

This phenomenon of Internet politics, or more precisely, the political Internet, reflects underlying conflicts and interactions between two systems: the socio-technological Internet system and the political regime. The primary objective of this book is to investigate and explain these conflicts and interactions. More specifically, it focuses on the last of the four aspects discussed above — political control of the Internet. This aspect has particular importance not only because Internet controls often mirror the political impact the Internet can have as well as strategic choices of national development (and is, thus, strongly related to other aspects of Internet politics) but also because discussions on Internet controls increasingly resonate with those on authoritarian resilience and democratic transition, subjects in which political scientists have long been engaged. Therefore, it highlights the relationship between a type of political regime, as the most distinct feature of a political system, and Internet control practice. It is interesting and important to investigate whether regime type (especially among democratic and semi-authoritarian regimes) affects the intensity of Internet controls, and if not, to identify the major factors that cause Internet controls. To narrow it to a viable scope, this book focuses on the region of Southeast Asia, where diverse political regimes exist and are frequently transitioning and transforming. It further narrows its focus on competitive political regimes, thus excluding fully authoritarian regimes which are conventional subjects in the study of Internet control. It hopes that, by studying Internet control practices, it would not only enhance and substantiate our understanding of politics in an Internet-dominant era, but also help to explain the role of technology in political analysis.

What is Internet Control?

Probably the most influential technology over the past two decades, the Internet has its roots "in the darkness of the Cold War" (Rosenzweig 1998, 1533). The first computer network, Advanced Research Projects Agency Network or ARPANET, was invented in 1969 against a backdrop of US–USSR technological competition (Carr 2009), enabling the research scientists working for US defence agencies to exchange data and information through a "packet-switching"[1] process (Abbate 2000). Due to the fact that the access to ARPANET was initially limited to defence, science and academia, it is possible that security and authoritative control of the network was not the priority of those engineers and technicians, and thus the anarchical nature was embedded into the Internet from its inception. As Jayne Rodgers (2003, 42) put it, "whether by design or default, the result was an inherently decentralised communications technology which could be used to establish direct or indirect links between individuals and institutions".

Because of the history of Internet development, the essential technologies and infrastructures of the Internet have, for decades, been under the tight monopoly of the United States. The root servers, which store the addresses and technical standards databases and serve as the crucial nucleus of the international networking system, consist of 13 sets of colossal computer systems, 10 out of which are located within the United States (Cukier 2005). As for the overall administration of, and supervision over, the Internet system, Jon Postel, a computer science professor at the University of Southern California, oversaw the relevant affairs almost exclusively until 1998, when his role was superseded by a private-sector non-profit organisation called the Internet Corporation for Assigned Names and Numbers (ICANN). Nonetheless, the United States has retained much power over Internet governance, as ICANN was established under the law of the state of California and responsible only to the US Department of Commerce (Mathiason 2009). While the United States has dominated the global structure of the Internet at an international level, the *Pax Americana*, anticipated by many Internet enthusiasts, did not occur since cyberspace, instead of being entirely free and borderless, was further controlled by various means at a national, domestic level. The subordinate servers deployed by national governments, functioning as transshipment stations that deliver and exchange packets between internal users and external destinations, make it feasible and effective that nation states can claim sovereignty over their cyberspace.

The nature of the Internet is not as borderless and anarchical as many early users had anticipated. In fact, governments, no matter whether authoritarian or democratic or somewhere in between, have at their disposal a large pool of various feasible methods and policies for Internet control. This diversity of control strategies is perhaps best illustrated by Zittrain and Palfrey (2008, 31) in the following words:

> Sometimes the law pressures citizens to refrain from performing a certain activity online, such as accessing or publishing certain material. Sometimes the state takes control into its own hands by erecting technological or other barriers within its confines to stop the flow of bits from one recipient to another. Increasingly, though, the state is turning to private parties to carry out the control online. Many times, those private parties are corporations chartered locally or individual citizens who live in that jurisdiction.

In general, the various methods that compose the overall repertoire of Internet control can be divided into four groups: methods that (1) censor the Internet content, (2) exploit legal framework, (3) monopolise network infrastructure, and (4) enforce psychological self-censorship. The first method involves restraining netizens from accessing certain kinds of content. The most direct and economical control of online content always involves technological means through which sensitive content is filtered and "detrimental" websites blocked. However, the exact mechanisms of filtering or blocking content may vary from case to case, depending upon the motivation and capability of the organisation deploying them. Common types of technical blocking/filtering include TCP/IP address blocking, Domain Name System (DNS) tampering, Uniform Resource Locator (URL) filtering (Murdoch and Anderson 2008), and keywords filtering. Besides the conventional blocking mechanisms, websites can also be made inaccessible by overloading the target server or network connection. For instance, it was reported that ahead of Myanmar's national elections in November 2010 — which had not been held since 1990 — a massive Distributed Denial of Service (DDoS) attack occurred that almost crippled the Internet traffic throughout the country (BBC 2010). The technical report from Craig Labovitz (2010), an expert in Arbor Networks, showed that the sudden influx of Internet traffic was "several hundred times more than enough to overwhelm" the country's network capacity. Similar incidents occurred in Malaysia — this time, DDoS attacks on several prominent newssites — before the critical Sarawak state election in April 2011 (Reporters without Borders 2011). None of these attacks could be traced directly to any government agency, but the timing has proved beneficial principally to governments in Myanmar and Malaysia.

In the second method, in order to rationalise and legitimise the supervision of online content as well as to moderate the radical, provocative, and oppositional voices of Internet users, legal and regulatory frameworks are necessary for governments who attempt to politically control the Internet. In general, three types of regulations can be identified. The first involves rules stipulating under what conditions and in what manner Internet Service Providers (ISPs) could be organised and websites registered. The second strand of regulations addresses different types of web-based activities, including online posts, emails, and blogs and so on, which are not permitted on the Internet. For instance, in Thailand, the law against lèse-majesté is broadly used in the online regulation that prosecutes behaviours insulting, defaming, or threatening the Thai royal family. The last type stipulates how illegal online activities are penalised. In Myanmar for example, the State Peace and Development Council demanded that all network-ready computers must be registered with Myanmar Posts and Telecom (MPT), with fines and prison sentences of between seven and fifteen years if the requirement was not met. The actual punishment for online Burmese activists and dissidents is even tougher: Nay Phone Latt, a famous blogger who was nominated for a "Cyber-Dissident or Blogger" Award, was arrested by the Burmese authorities for posting information about the September 2007 demonstrations on his personal website and sentenced to twenty years in jail. Incidents like this are almost ubiquitous across the whole region.

Apart from targeting infringing content online, nation states also attempt to control the overarching infrastructure that creates and supports the Internet fundamentally. On this score, states could purposely deploy Internet accessibility geographically and manipulate the Internet service when necessary. A more direct and effective way is to "switch off" (part of) the entire network. Referring to the Internet shutdown in Burma in 2007, researchers in the OpenNet Initiative (2007) explained that "a switch off could therefore be conducted at the top by shutting off the border router(s), or a bottom up approach could be followed by first shutting down routers located a few hops deeper inside the AS (Burmese Autonomous System)". The fourth method of Internet control occurs psychologically. On the one hand, states may use intimidatory actions of monitoring and punishing "untamed" online activities, encouraging an atmosphere of "self-censorship". For example, as Terence Lee (2010) argued, the Singaporean government was continuously seeking to create a "culture of self-censorship" in its cyberspace that could govern the mindset and conduct of Internet users. Moreover, governments may actively participate in online activities for propaganda and ideological purposes. Political leaders as well as hired commentators attempting to (re)shape online public opinion have been a crucial part of the "cyber troopers" in many Southeast Asian countries.

The discussion above illustrates how Internet control is technically feasible and empirically practiced. Internet control takes various forms, ranging from content censorship to the chilling effect of psychological manipulation. In this book, the level of Internet control is measured by observing the occurrence, frequency, and scale of these various forms. Meanwhile, different forms of Internet control share a common feature. They point to state repressive actions particularly associated with Internet usage that threatens established interests in the political system. Therefore, it is reasonable to conceptualise Internet control as a component or form of political repression, which broadly refers to "government regulatory action directed against those challenging existing power relationships" (Davenport 1995, 683), or "the systematic violation of the civil liberties and human rights of groups and/or individuals" (Regan and Henderson 2002, 120). The importance of this conceptualisation is that it allows us to draw lessons from political repression studies (which is reviewed in the next chapter) to identify the key factors behind Internet control policies.

Internet control has been a hotspot in the study of Internet politics. Based on the belief that the Internet poses an insurmountable threat to authoritarian rule, most of the work in this aspect reflects Internet control in authoritarian countries. On this score, Garry Rodan (1998; 2004) revealed how the ruling party of Singapore, as well as that of Malaysia, promoted Internet development while seeking to control it politically. Even more studies cite the case of China (Kalathil and Boas 2003; Wacker 2003). Meanwhile, several studies have found that political control of the Internet occurs not only in authoritarian regimes, but also in democratic states. Lessig (1999) argued that governments everywhere can regulate the Internet both by controlling its underlying code and by shaping the legal environment in which it operates. Furthermore, a study by Giacomello (2008) indicated that the different types of Internet control in democratic countries, such as the US, Germany, and Italy, were determined by the different relations between governments and societies.

However, current studies on Internet control suffer from several weaknesses. Firstly, although these studies often provide detailed accounts of *how* Internet controls are designed and implemented, especially technically (see, for example, Goldsmith and Wu 2006; Murdoch and Anderson 2008), they give few answers as to *why* political control of the Internet occurs. While the forms, processes, and techniques of Internet control have been carefully examined, allowing us to assess the intensity and diversity of Internet controls, we still need theoretical explanations that identify the driving and constraining forces behind Internet control. Secondly, much literature is devoted to the single case study which aims to only examine the impact of the Internet and government responses in a given circumstance (see, for example, Rodan 1998; Wacker 2003; Hill and Sen 2005; Zheng 2008; Morozov 2011a). By contrast, comparative research, built on an explicit and coherent theoretical framework that highlights the major determinants of Internet control, is infrequent and inadequate (see, for example, Kalathil and Boas 2003; Howard 2010).

More importantly, most studies, though sometimes implicitly, attribute Internet control practices to the resistance, or inherent nature, of authoritarian political regime, thus implying a linear relationship between Internet control and regime type (see, for example, Rodan 1998; Kalathil and Boas 2003; Wacker 2003; Gomez 2004; Morozov 2011a). This presumed relationship, however, has been made without careful examination. Some empirical evidence has revealed that democratic countries also implement Internet control policies, while some authoritarian states leave their cyberspace uncensored (Giacomello 2008; Deibert and Rohozinski 2010; Howard 2010). These deviant cases necessitate re-examination of the supposed “regime–control” relationship. To what extent can regime type determine the level of Internet censorship? Addressing this question, the following section will evaluate the “regime–control” thesis and present the major puzzle that renders an alternative framework necessary.

Presenting the Puzzle

As previously mentioned, Internet control strategies have been widely considered as a natural, inevitable response of authoritarian political regimes, thus implying a linear relationship between Internet control and regime type. While deploying this relationship as the underlying premise of their analyses, these studies seldom question the validity of this relationship per se. This section provides a brief examination of this relationship which is more complicated than a simple linear dependence.

We first test the correlation between the level of Internet control and the degree of democracy. Although so far a comprehensive index of Internet control (covering a large sample of countries as well as a full repertoire of Internet control measures) is barely available, Freedom House (2011) has made an important effort to quantify the level of Internet freedom, recording and measuring governmental regulations in 37 countries. Despite using only a small number of samples (already a sharp increase from the 15 countries in the previous version), this report has covered countries at varying levels of political and economic development. It is therefore, to some extent, representative. The scoring system contains three sub-groupings: “obstacles to access,” “limits on content,” and “violations of user rights”. Countries are scored from 0 (best) to 100 (worst) to describe a “free” (0–30), “partly free” (31–60), or “not free” (61–100) Internet environment (Freedom House 2011, 386–388). To enable comparison between Internet freedom and democraticness, scores on the democraticness of these same countries are extracted from Economist Intelligence Unit’s Democracy Index 2010 and Polity IV Country Reports 2010 respectively.[2] Under EIU’s index, a score of 10 represents the highest level of democracy and 0 the lowest. Meanwhile, Polity IV’s scheme envisages a regime spectrum ranging from -10 (most autocratic) to +10 (most democratic).[3]

The results are shown in Fig.1-1 and 1-2. Despite slight differences, the two figures demonstrate similar relations between variables. There are two major observations to be made from the data. Firstly, a statistical correlation can be observed between the level of democracy and that of Internet freedom, indicating that regime types do matter. As democraticness increases, countries in these surveys have higher probability of allowing greater Internet freedom, and vice versa.

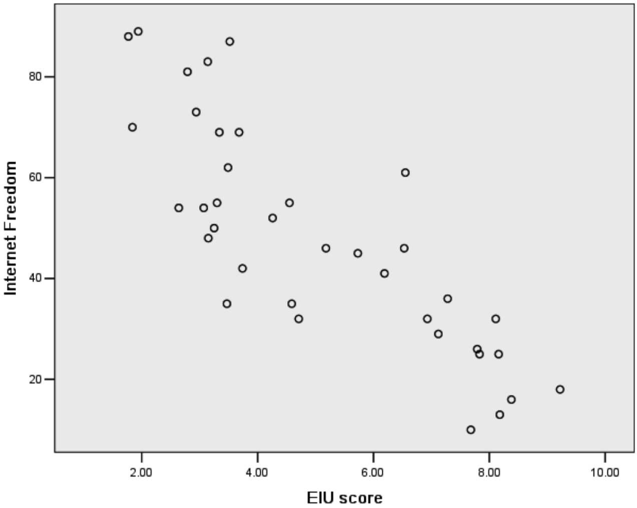

Fig. 1-1: Correlation between political regime and Internet freedom
Source: EIU 2010

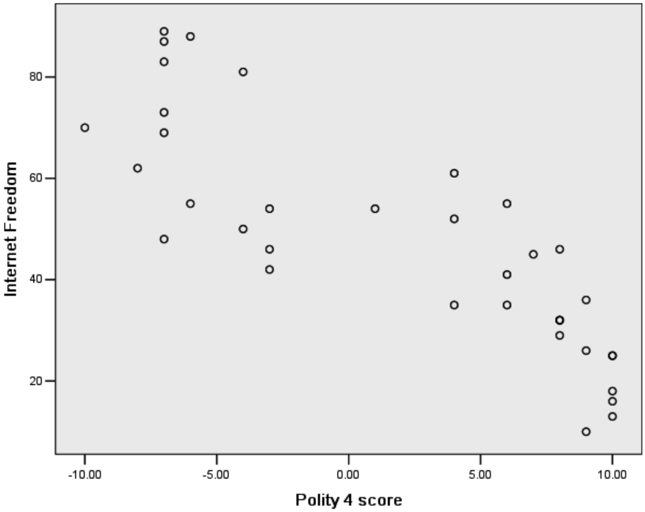

Fig. 1-2: Correlation between political regime and Internet freedom
Source: Polity IV 2010

Nonetheless, the correlation is much stronger at either end of the equation than in the middle. In general, fully democratic regimes impose far fewer restrictions on Internet freedom, while politically closed regimes control the Internet system in a pervasive and systematic way. But among those intermediate political regimes, the level of democraticness appears inadequate in explaining Internet control outcomes. With similar degree of democracy, countries may substantially vary in their respective level of Internet freedom. For instance, scored in the range of 4–5 under EIU's index, Pakistan (with a score of 55 in Internet freedom), Russia (52), Georgia (35), and Kenya (32) appear quite different in protecting Internet freedom. Similarly, the same score under Polity IV's classification produces dissimilar results — a score of 4 (indicating "open anocracy") leads to a "partly free" status (Nigeria and Russia) as well as a "not free" status (Thailand) in Internet freedom. Such mismatch persists when we move along the regime continuum. Contrary to our expectations, one degree of increase in democracy may be accompanied by a decrease in Internet freedom, and vice versa. Therefore, the purported relationship between regime type and Internet control turns out to be much more complicated and confusing than originally assumed, at least within the intermediate range of regime types.

In fact, it is recognised that the role played by political regime type in shaping repressive actions is highly ambiguous (Davenport 2007). On this score, Davenport and Armstrong (2004) have found that above a certain level of democracy the relationship between democracy and repression is linear, but below that threshold state coercive actions are not influenced by regime type. The significance of their finding is that "the level of democracy thus retains its importance for theory as identified within most of the literature relevant to the topic, but only at the very end of the democratic continuum" (Davenport and Armstrong 2004, 551–552). This finding corresponds to what we have observed above. Therefore, it is possible that regime type is not the direct determinant of Internet control. In this sense, we should look at other factors in addition to regime type to better understand Internet control, especially in semi-democratic and semi-authoritarian contexts.

Based on the discussion above, this study proposes two major hypotheses. The first relates to the relationship between regime type and Internet control. The other presents an alternative model of Internet control that underscores the role of online transgression and civil society. Theoretical framework used in these hypotheses will be further elaborated in Chapter 2.

Hypothesis 1 (H1)

In the intermediate range of political regimes between democracy and authoritarianism, regime type does not correlate closely with the level of Internet control. Online transgressiveness and the power or capacity of online civil society better account for Internet control outcomes than do regime types.

Hypothesis 2 (H2)

While online transgression encourages the state to respond with Internet controls, online civil society capacity enables society to resist and overcome such control.

Selecting the Case

This research is designed to address the "regime–control" puzzle and identify the major factors that better account for Internet control practices among intermediate political regimes. It also attempts to illustrate the trajectories in which different countries develop their Internet control strategies. Instead of taking a cross-regional approach which risks facing not only divergent outcomes, but also a great variety of potential causes, this study focuses on the region of Southeast Asia, distinguished by its "remarkable range of political forms" (Hewison 1999, 224). The various types of semi-democratic and semi-authoritarian regimes that Southeast Asian countries have would enable us to identify the major determinants of Internet control among intermediate political systems. Moreover, by narrowing our focus on a specific region, we may better control potential differential factors such as cultural and geographical differences, level of development, and historical legacies (Slater 2008).

A comparative in-depth case study methodology is used as the main approach for several reasons. Firstly, since Internet politics is a relatively new research subject, there are few established theories of Internet control to be tested. In this sense, this study is as much about generating new hypotheses as about confirming or disconfirming existing theories, a task that case study techniques better address (Lijphart 1971). By closely examining the internal political dynamics of a few cases, this study attempts to develop a grounded theory upon which further large-scale, quantitative investigations can draw.

Secondly, although case study techniques, unlike statistical testing, cannot quantify precise causal relations, they are able, as a first step, to identify and investigate casual mechanisms. On this score, case studies allow us to see how different variables interact and thus better understand the causality between them (Gerring 2004). In addition, case study techniques enable us to trace the historical development of Internet control institutions and strategies in selected countries. Last but not least, there are also some practical reasons for avoiding a large-N research design. The most critical reason is the unavailability of comprehensive, large-scale data sets on Internet control. As noted above, the first report quantitatively measuring Internet freedom, released by Freedom House in 2009, only covered 15 countries, while its 2011 updated version, despite its valuable and path-breaking effort, merely boosted the sample size to 37. Other important efforts in this regard either remain small-scale and qualitative (such as reports released by Reporters Without Borders), or concentrate only on a particular strategy of Internet control without taking into account the full repertoire (such as Open Net Initiative's Internet filtering reports). All these factors provide rationale for a comparative case study approach. The validity and weakness of this approach will be further examined in the final chapter.

As mentioned above, the "regime–control" puzzle is most evident in the intermediate range of regime types. Therefore, the usual dichotomy between democracy and non-democracy needs modification. This book utilises existing regime typologies that treat political regime as a continuum ranging from liberal democracy at one end to politically closed regimes at the other (Diamond 2002). In between these two ends are different types of hybrid regimes, including — according to their levels of democraticness — electoral democracy (Diamond 1999), competitive authoritarianism (Levitsky and Way 2010) and electoral authoritarianism (Schedler 2006). These hybrid regimes are labelled competitive political systems so that we can distinguish them from either full democracies or full autocracies. This intermediate area is the focus of our research interest. Since this study focuses on competitive political regimes in Southeast Asia, six countries fall into our sample list: these are Cambodia, Indonesia, Malaysia, Philippines, Singapore, and Thailand.[4] None of them can be further qualified as liberal democracies, but democratic traits do exist to different extents (see Freedom House 2012; Economist Intelligence Unit 2011; Polity IV 2010).

Malaysia, Thailand and Indonesia have been selected as in-depth case studies because these countries represent an evident mismatch — their regime types do not correlate with their respective extent of Internet control. Competitive authoritarianism in Malaysia, although amounting to less democratic politics than in the other two countries, is accompanied by low-medium intensity of Internet control practice. Electoral democracy in Thailand is associated with the most repressive environment for the Internet. Meanwhile, electoral democracy in Indonesia, currently the most democratic state in the region, implements Internet controls at a medium level. Freedom House's (2011) recent report quantified the level of Internet control in these countries by establishing an index of Internet freedom. It showed that Thai people enjoyed much less Internet freedom, with a score of 61 (a status of "not free") compared with 46 ("partly free") in Indonesia, and 41 ("partly free") in Malaysia. In other words, regime type in Malaysia would lead us to expect Internet controls there to be more intense than they actually are, while regime types in Thailand and Indonesia would suggest that Internet controls should be less intense than they are.

Moreover, we take a closer look at one specific controlling method — the extent to which governments in Southeast Asia censor sensitive websites. On this score, the Open Net Initiative has technically tracked the Internet filtering situation across the world. In a recent research report, they scrutinised, among other countries in Asia, the filtering and blocking practices in Burma, Indonesia, Malaysia, Thailand, and Vietnam (Deibert et al. 2012). The results show that Burma and Vietnam represent two of "the most pervasive regimes of Internet filtering in the region, primarily targeting independent media and content related to politically sensitive issues, human rights, and political reform" (Deibert et al. 2012, 226). However, while both Indonesia and Thailand adopted selective filtering on websites with political content and websites for Internet tools (such as those websites offering circumvention software), no evidence of filtering practices was found in Malaysia (see Fig.1-3). Again, the democraticness of political regime and the level of Internet filtering did not match in the intermediate zones of the political regime spectrum.

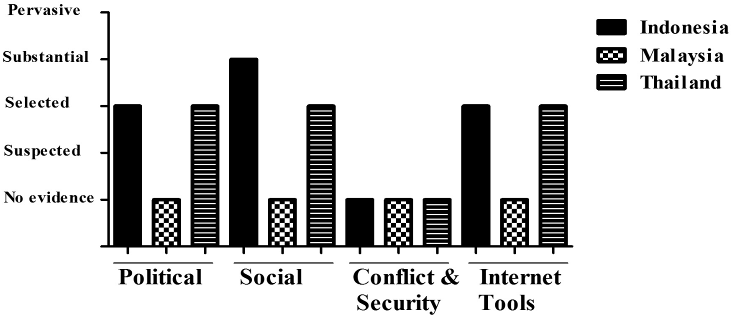

Fig. 1-3: Internet filtering in hybrid regimes
Source: Deibert et al. 2012

This mismatch refutes the commonly perceived “regime–repression” causal relationship, and thus, necessitates in-depth examination of alternative explanations of Internet control in these countries. By closely exploring the abnormal cases that negate the “regime–repression” model, this book attempts to construct an alternative model of Internet control.

By contrast, the remaining three Southeast Asian countries, Cambodia, Singapore, and the Philippines, operate authoritarian and democratic regimes within the competitive spectrum that correlate, as would be expected, with the level of Internet control. These country-cases are given less attention, since it is the anomalous cases that this book has sought most to explain. But they are worthy of at least cursory examination, due to the possibility that in these cases, regime types mask other factors that are more fundamentally at work. Therefore, while this research chooses three countries as case studies for in-depth analysis, the remaining three countries will be briefly investigated in Chapter 6 to see whether our alternative model can still be applied.

In order to obtain first-hand information on Internet controls, field research has been conducted in Malaysia, Thailand and Indonesia. Appendix A details the process, rationale, and strategy of interviewee selection, and provides the question lists.

Overview of the Book

This book is structured as follows. Chapter 2 theoretically constructs the alternative model used in this study. It draws insights from existing studies on political repression to find out which factor(s) truly affects Internet control outcomes. Specifically, it identifies two major variables — intensity of online transgressiveness and capacity of online civil society — that are most important in explaining Internet control in competitive political systems. This alternative model argues that online transgressiveness serves as the impetus which defines the necessity of Internet controls, while online civil society represents an inhibiting force, the cohesiveness of which determines the extent to which societal resistance against Internet control might succeed. Criteria of measuring these variables are developed, supplemented by a detailed measurement scheme in Appendix B. In addition, the theoretical model also highlights the role of historical and contextual conditions.

Chapters 3, 4 and 5 apply the alternative model to in-depth case studies, investigating Internet control practices in Malaysia, Thailand, and Indonesia respectively. These case studies present first-hand information collected through several field trips, including interviews with relevant government officials, politicians, scholars and activists. Each case starts with a brief summary of the historical development of the political system in question as well as the Internet system in that country, followed by a discussion on how the Internet facilitates political change and how governments respond by controlling it politically. These cases reveal that it is the intensity of online transgressiveness and the capacity of online civil society, instead of regime type, that collectively affect the level of Internet control.

In Malaysia, although a moderate-high level of transgressiveness has provided a stimulus for the government to suppress online activism and opposition campaigns, the online civil society, which often coordinates with opposition parties and other social forces, has effectively prevented the government from upgrading its Internet control arsenal. In Thailand, the combination of a high level of transgressiveness and a fragmented online civil society gives rise to extensive and systemic Internet control measures. Meanwhile, Indonesia faces moderate online transgression and modest civil society capacity. Internet control there operates, accordingly, at a moderate level. The findings from these country-cases bear out this study's theoretical framework.

Chapter 6 deals with other democratic and semi-democratic countries in Southeast Asia. Internet control practices in Cambodia, Singapore, and the Philippines are explored to supplement our inquiry of why competitive political regimes control the Internet. This chapter uses mainly secondary but reliable information obtained from scholarly research and NGO reports. The concluding chapter synthesises the insights drawn from case studies and makes comparison across these cases. It then raises and briefly tests several alternative explanations of Internet control, including the rate of Internet penetration, media environment, and foreign investment dependency. These factors are found to be much less decisive in Internet control practice. Finally this chapter also discusses how these insights make theoretical contributions to political science as well as Internet studies.

CHAPTER TWO

TRANSGRESSION, CIVIL SOCIETY AND INTERNET CONTROL

This chapter attempts to construct an alternative framework that better accounts for Internet control outcome. In previous chapter we conceptualised Internet control as a form of political repressive action. Analysis in the following section returns to this theme, drawing upon existing literature on political repression to identify the major factors that determine Internet control policies.

What do Studies on Political Repression Say and Not Say?

Agency-level explanations: The central role of threat

How should we use existing knowledge about political repression to explain Internet control? What are the factors leading to political repression in general? Are these factors the same as those that lead to Internet control? Perhaps one of the most significant relationships that has withstood rigorous investigation is between domestic threats — the challenges made to existing authorities in the form of political dissent — and political repression. This suggests that when political threats are present, government authorities frequently use repression as a means to restrict or eliminate these threats in order to preserve their interests (Davenport 2000). More importantly, the nature of political threats strongly affects how governments respond (Gurr and Lichbach 1986; Davenport 1995; 2007; Gartner and Regan 1996; Moore 2000). Political dissent that involves large-scale mobilisation and uses unconventional or unconstitutional tactics is more likely to provoke government repression than the contentiousness that involves smaller populations and is confined within conventional strategic options. On this score, McAdam, Tarrow, and Tilly (2001) distinguish between two types of political contentiousness — a transgressive one and a contained one. While conflicts in the former type involve almost exclusively parties "previously established as constituted political actors", the latter brings in at least some "newly selfidentified political actors", and exhibits some innovative collective actions (McAdam et al. 2001, 7–8). Transgressive contention is generally considered as larger, systemic political threats while contained contention is associated with less critical, and often individual or organisational-based threats. Besides scale and intensity, threat can also be measured by the political content of dissenting groups (Gartner and Regan 1996). The opposition's demands indicate the concession that the political leadership is called upon to make. Therefore, political claims to replace the current political system are more threatening than claims to redistribute resources or challenge individual politicians/institutions.

Based on the observation above, this book will measure political threat in terms of the trangressiveness of political dissent. To transgress is to cross the limits or boundaries that the political establishment has prescribed for conducting political activities. Transgressiveness refers to the extent to which political contentiousness and activities stand in contradiction, inversion, or as alternatives to the status quo (Stallybrass and White 1986). It includes, in general, two attributes: (1) to what extent the dissent (contentiousness) mobilises new political players that were previously tranquil and employs new strategies and (2) whether its political demand is targeted at the systemic level or at the individual/organisational level. The adoption of transgressiveness in measuring Internet threat will be explored in a later section.

As an independent variable, transgressiveness, or the level of threats, should be effectively separated from other plausible factors such as regime type. It would be tempting to argue that democracies are less likely to experience political threats than autocracies are, and thus the level of threats merely reflects the degree of democracy. In this sense threat is only a secondary factor, unworthy of special attention. However, studies on political repression acknowledge the distinction between political threat and regime type and argue that the conventional perception of a linear relationship between them is misleading (Regan and Henderson 2002; Davenport 2007). Instead, empirical findings reveal an inverted-U relationship, with semi-democracies facing the highest level of threats, due to the fragility of state institutions and the limited range of available options (Regan and Henderson 2002, 124). Therefore, it is not the regime type, but other factors embedded in the political system instead, that directly affect the level of threat. If the linear covariance of threat and regime type does not exist empirically, it is reasonable to treat the level of threat as an independent factor. In fact, it has been argued that the level of threat is more useful than regime type in explaining the likelihood of repression (Regan and Henderson 2002; Earl 2003). In a similar vein, this study considers transgressiveness and regime type as separate variables, while recognising their complicated, non-linear connections.

Meanwhile, related to the "threat" factor is the capacity of civil society to resist repression. A strong civil society often leads to better human rights protection, and thus less state repression (Neumayer 2005; Hathaway 2007). When substantial (or potential) violation of civil rights occurs, civil society organisations could exert pressure upon governments to withdraw repressive actions. They do so through promoting public deliberation, mobilising social movements, and allying with media and oppositional forces. As Dan Slater (2012, 27) recently argued, restraints on coercive actions "may well depend, in turn, on the capacity of opposition forces to muster a sufficient challenge to press leaders to reconsider their patterns of rule". Particularly in competitive political systems, the political costs of repression would exponentially heighten if civil society is well institutionalised, consolidated, and coordinated within itself. On the other hand, the fragmented civil society (or highly isolated from elite politics) brings far less pressure against state repressive actions. Factional conflicts among civil organisations may even exacerbate political repression as some repressive policies are in accord with the interest of a particular civil group. Under such circumstances, an "uncivil society" occurs that ails rather than heals democratic institutions and practices (Thompson 2008). In other words, government authorities could garner greater public support in their coercive (regulatory) measures when the attitudes of civil society towards such policies are divided or antithetic. Therefore, I hypothesise that the capacity of online civil society in its diverse forms, such as new media, the blogger community, and online movements, also affects government decisions on Internet control.

These variables — the level of threats and the capacity of civil society — underscore the strategic interaction at the agent level. This model considers state repressive actions as cost-benefit calculations concerning the necessity as well as repercussions of government decisions. However, this agency-level discussion is still insufficient in two aspects. Firstly, while government behaviour may stem directly from agency-level interactions, it remains unclear how a particular form of political threat is shaped and what governs the state–society relationship. In other words, we have to investigate why transgressiveness of online contentiousness is much greater, and why the capacity of online civil society is higher, in one country than another. In this sense, it is necessary to identify the conditioning factors that frame the character of agency-level variables. Secondly, while threat and online civil society may be sufficient in explaining current Internet control outcomes in Southeast Asia, it appears