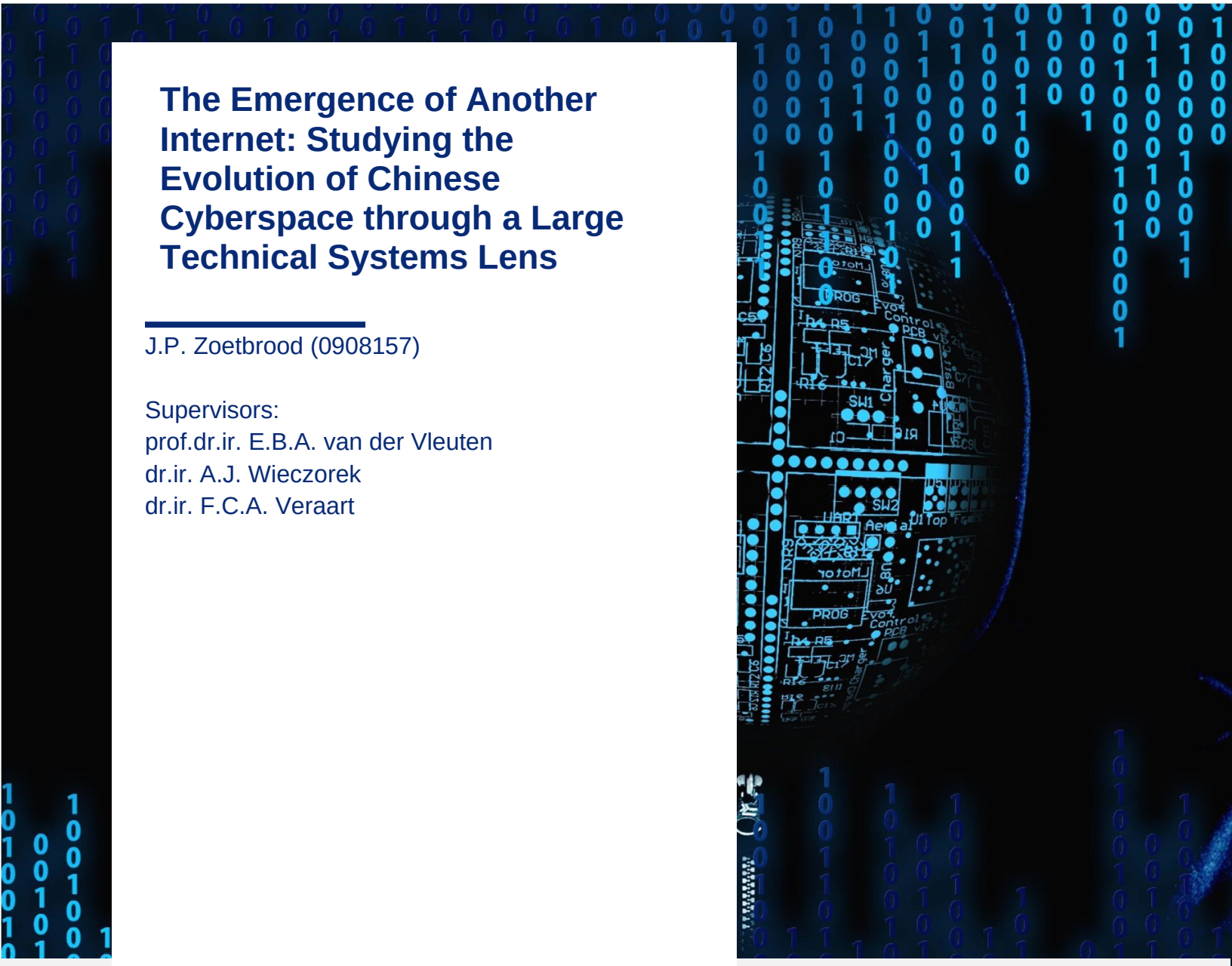
The Emergence of Another Internet

Studying the Evolution of Chinese Cyberspace through a Large Technical Systems Lens

Zoetbrood, J.P.

Award date:
2021



The Emergence of Another Internet: Studying the Evolution of Chinese Cyberspace through a Large Technical Systems Lens

J.P. Zoetbrood (0908157)

Supervisors:
prof.dr.ir. E.B.A. van der Vleuten
dr.ir. A.J. Wieczorek
dr.ir. F.C.A. Veraart

22 JUNE 2021

Innovation Sciences – Master Thesis

TU/e
EINDHOVEN UNIVERSITY OF TECHNOLOGY

Abstract

The Internet is highly uniform across the globe. An important exception to this uniformity can be found in China, where over the last decades a distinct cyberspace has emerged and grown so much that it now also significantly influences the dominant US-based cyberspace. This thesis investigates how this alternative cyberspace could emerge, and how it evolved over time. To do so, the Large Technical Systems framework was applied. Information from a large variety of written sources was gathered, in which system building activities of actors in Chinese cyberspace were identified, as well as the developments in Chinese cyberspace that altered the system momentum, thereby directing future developments. This thesis shows that the evolution of Chinese cyberspace can be interpreted as a sociotechnical and evolutionary process, in which earlier developments created the conditions for later developments to occur. Especially the creation of the Great Firewall, the decision of many large US tech companies to leave the Chinese market due to the censorship regulations, and the rapid domestic growth that Chinese companies enjoyed due to having no foreign competitors can be identified as impactful developments on how Chinese cyberspace evolved. Additionally, through its focus on system building, this thesis shows that governmental actors and private companies both played a large role in the development of Chinese cyberspace. This thesis increases our understanding of how actors in Chinese cyberspace responded to the challenges they faced, while also showing the added benefit of studying Chinese cyberspace from a sociotechnical lens and providing a comprehensive and holistic explanation for the successful growth of Chinese cyberspace.

Keywords: China, Cyberspace, Large Technical Systems, LTS, Momentum, System Building

Executive summary

The Internet is highly similar across the world. However, an important exception can be found in China, where instead of the globally dominant US-based tech companies, domestic alternatives can be found, which also offer different products and services. In addition, Chinese cyberspace is characterized by the strictest content regulation system in the world, and it places much stronger emphasis on the central role of national governments in regulating cyberspace. While during its early years, the Chinese Internet model remained confined to China itself, in recent years the influence of Chinese cyberspace can be experienced across the globe, in areas such as Internet governance, technological standardization and the economic expansion of Chinese tech companies. While these developments all occurred during the last decade, they are deeply rooted in the longer history of Chinese cyberspace. They are the result of a long process of deliberation and contestation between various actors, who sought solutions to the problems they faced, and in the process shaped Chinese cyberspace, resulting in the system we know today.

Chinese cyberspace has already been studied extensively from a wide range of perspectives, ranging from privacy to business models and ecosystems to geopolitical implications. However, as Chandel et al. (2019) remarked, most studies focus either on technological, social and economic, or on regulatory and policy matters. However, the interconnections between these various elements often remain obscured. As such, some authors (e.g., Y. Hong & Harwit, 2020) have made a call for more holistic historical research on Chinese cyberspace. This thesis responds to that call by studying the emergence and evolution of Chinese cyberspace from a sociotechnical perspective, using the Large Technical Systems (LTS) framework to analyze these developments. Therefore, the research question that is answered in this thesis is the following:

"How can the emergence and evolution of an alternative cyberspace in China be explained from a Large Technical Systems perspective?"

Theoretical Approach

To provide an answer to the research question, this thesis makes use of the Large Technical Systems (LTS) framework. LTS is a highly flexible framework that seeks to untangle the complexity of a sociotechnical system by analyzing it through a follow-the-actor approach. Two theoretical concepts are of particular importance for this thesis. The first of these is system building. This concept was developed as a means to study agency in the development of sociotechnical systems. A system builder is involved in transdisciplinary problem solving, thereby creating new connections that together shape this sociotechnical system. Studying system builders allows for a more detailed analysis of the exact ways in which a sociotechnical system is shaped by the actions and decisions of individual actors, as well as the challenges and dilemmas that actors faced when making these actions and decisions. As such, this study uses the concept of system building to conceptualize the emergence and evolution of Chinese cyberspace as a multi-actor game, with various actors being involved in the shaping of this system. A second important concept for this thesis is momentum. As the interconnections between the various elements of a system become deeper and the scale of the system increases, it acquires mass, and it tends to develop into a certain direction with a certain velocity. Once a system has gained momentum, it becomes difficult to change its trajectory. Identifying the momentum of a system helps explain the behavior of actors, as they tend to follow the momentum of the system. Additionally, it is a useful instrument to evaluate the impact that certain developments have on the system, as highly influential developments can change the momentum of the system, and thereby shape and steer future developments.

Methodology

To answer the research question and the subquestions, this thesis follows a qualitative exploratory constructivist approach. It analyzes the emergence and evolution of Chinese cyberspace using a single case study design, in which the emergence and evolution of Chinese cyberspace is defined as its case. A wide range of written source material is analyzed, ranging from academic literature to newspaper articles and policy reports. The data collection and analysis follow an iterative process, as new unexpected elements are encountered in the process, which can then be explored in detail. As such, this iterative process allows for a more thorough exploration of the subject. The collected data is analyzed using a combination of codes stemming from the theoretical framework, the research question and its subquestions, and codes emerging organically during the process of analysis. The findings of this thesis are presented in the form of a structured narrative, in the form of a thick description in combination with a theoretical framework, namely LTS.

Period 1: Origins

In the first period, the emergence of an alternative cyberspace in China is studied. Following the introduction of the World Wide Web in China in 1994, governmental responses were divided. On the one hand, it was believed that the Internet would lead to significant economic growth. On the other hand, the governmental actors were hesitant about the ideal of a liberal, free and deregulated cyberspace that accompanied this early Internet. As such, governmental actors began to regulate the Internet, and translate pre-existing norms regarding information censorship to this new technology. This effort led to the creation of a sophisticated censorship program that came to be known as the Great Firewall. Through a combination of technological, regulatory and organizational measures, the content on the Internet became strictly regulated. In addition, companies were required to comply with the censorship norms. Many western tech companies, that were already becoming dominant across the globe, were unwilling to collaborate to these censorship norms, and hence faced repercussions from the censors, impeding their activity in China. Additionally, Chinese tech companies were able to provide products and services that better served the local preferences of Chinese users than their US competitors. As such, the Chinese market became divided between Chinese and US companies.

Period 2: A distinct Internet

Given the economic potential of the Chinese market, many major US tech companies decided to comply with the wishes of the censors. However, this choice led to fierce domestic criticisms, including a hearing by the US congress. At the same time, the Chinese censors were also not satisfied with the censorship efforts of the US companies, as the censors believed they should be more strict. In the end, the US companies came to the conclusion that they could not function effectively both within and outside China, and therefore decided to leave the Chinese market. For Chinese tech companies, the absence of foreign competitors offered them a chance to quickly grow and monopolize the Chinese market. These companies gathered momentum towards further growth, and began to innovate and diversify their products and services. In these efforts, these companies tackled problems that were specific to Chinese society, and thereby created different products and services than could be found in the US-based cyberspace. The Chinese companies also did not face the dilemma that US companies faced when they had to choose between operating in the Chinese market or the rest of the world.

Period 3: Outward expansion

Since the Chinese market was saturated, Chinese tech companies needed to expand abroad to maintain their growth. In their efforts, they were aided by the Chinese State Council, which since the accession of president Xi Jinping had begun to centralize and prioritize the governance of Chinese cyberspace. The State Council issued a series of ambitious policy plans, containing both goals for development within China and goals for foreign expansion. The State Council facilitated foreign expansion of Chinese tech companies through projects such as the Belt and Road Initiative. However, the international expansion of Chinese tech companies led to resistance abroad. Several national governments, and the US government in particular, raised security concerns about Chinese tech companies and products, and began to exclude them from their national digital infrastructure. However, the international influence of Chinese cyberspace could also be experienced in other areas. Chinese representatives began to play a stronger role in global Internet governance bodies, which they wished to reform based on the principles of 'cyber sovereignty', as advocated by the State Council. Furthermore, there was a governmental push towards China taking on a more influential role in technological standardization, in fields such as AI or high-tech appliances. Interestingly, while the influence of Chinese cyberspace on the dominant US-based cyberspace has clearly been increasing over the last years, there is also increasing speculation about a more fundamental split between Chinese cyberspace and the US-based cyberspace as a result of the recent friction between the two system and the emphasis of the Chinese government towards digital sovereignty. As such, it remains to be seen whether the increased interaction between Chinese cyberspace and the US-cyberspace will lead to integration or to further separation.

Conclusion

This thesis shows that the current state of Chinese cyberspace is the result of a long history of consecutive events and developments, in which actors confronted with certain situations made decisions based on the situation they found themselves in. By changing technological, social, economic, and legal elements in Chinese cyberspace, these actors changed the momentum of the system and thereby indirectly shaped future developments. This research has identified several developments as having had a major impact on the developmental trajectory of Chinese cyberspace. Due to conflicting norms and values between the early Internet and those already existing in Chinese society, Chinese governmental actors initiated the creation of the Great Firewall. Due to this censorship program, US companies experienced major difficulties regarding their operations in China, and as a result ultimately decided to leave the Chinese market altogether. This decision created space for Chinese tech companies to grow, thrive and innovate. Due to the momentum gained by this rapid growth, actors in Chinese cyberspace began to look towards foreign expansion, which in the end resulted in the increasing influence of Chinese cyberspace on the digital environment that can be experienced worldwide today. Both governmental actors and private companies can be identified as important actors in the emergence and evolution of Chinese cyberspace, as their system building activities had a large impact on the development of Chinese cyberspace as a whole. All in all, this thesis has shown how a sociotechnical approach can reveal details about the relationships between the various elements of a system that are usually not mentioned at all or simply assumed to be there. Additionally, this thesis has generated a deeper understanding of the origins and the motives behind the expansion of Chinese cyberspace, which can serve to mitigate disagreements and contribute to more informed decisions.

Table of Contents

List of abbreviations

AI	Artificial Intelligence
BAT	Baidu, Alibaba and Tencent
BRI	Belt and Road Initiative
CAC	Cyberspace Administration of China
CCP	Chinese Communist Party
CEO	Chief Executive Officer
CIA	Central Intelligence Agency
CNNIC	China Internet Network Information Center
DNS	Domain Name System
FBI	Federal Bureau of Investigation
GDP	Gross Domestic Product
ICANN	Internet Corporation for Assigned Names and Numbers
ICT	Information and Communications Technology
ID	Identification Card
IP	Internet Protocol

ITU	International Telecommunications Union
LTS	Large Technical Systems
MII	Ministry of Information Industry
NII	The State Council's Steering Committee on National Information Infrastructure
NSA	National Security Agency
SAC	Standardization Administration of China
TCP	Transmission Control Protocol
US	United States of America
VPN	Virtual Private Network
WIC	World Internet Conference

List of figures

List of tables

1 Introduction

This chapter serves as a general introduction for the thesis. It describes the subject and the objective of this thesis. After this, the research question is described, as well as the approach and strategy that were taken to answer this question. A discussion follows about the scientific and social relevance of the research subject. The chapter ends with an overview of the structure of this thesis.

1.1 Introduction

The Internet shows strong similarities across the globe. It works by the same technical standards, and users across the world spend most of their time using the same websites and digital platforms, which often originate from the United States. Examples are the dominance of Google in the global search engine market and Facebook as the most popular social media platform (see Figure 1). However, there is an important exception to this uniform Internet. In China, a very different digital environment can be observed. Numerous examples of these differences can be given. China is one of the few countries where US tech companies are not dominant in the market, as they instead have their own domestic companies, such as Baidu, Alibaba or Tencent, which also offer different products and services than their US counterparts (Jia & Winseck, 2018; Leskin, 2019; Yuan, 2018). The Chinese Internet is also characterized by having the most sophisticated censorship apparatus in the world (often called the 'Great Firewall' in western literature) (Tai, 2014), which enforces strict content regulation on the Internet (Chandel et al., 2019; King et al., 2013; Taubman, 1998). Furthermore, the dominant conception in China about the societal position of the Internet differs fundamentally from many other countries, placing strong emphasis on the responsibility of the national government regarding cyberspace governance.

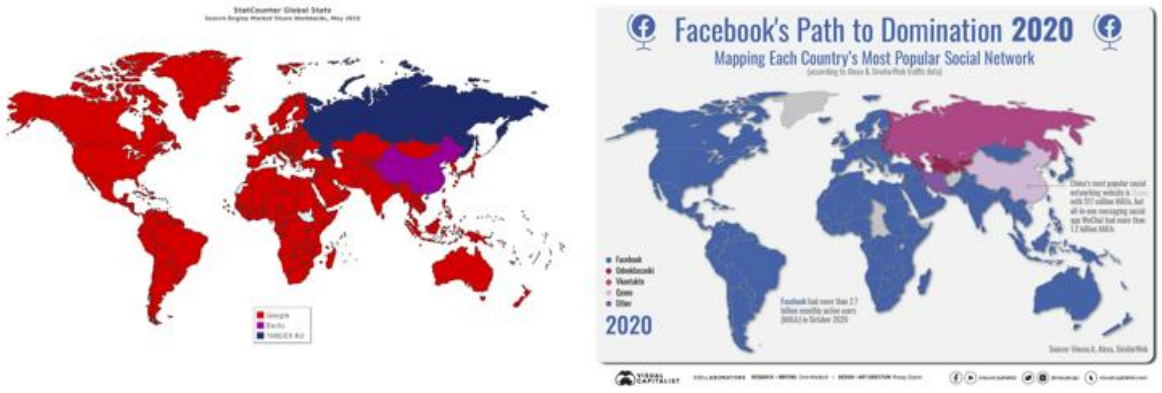


Figure 1: Most popular search engine (left, Google in red) and social network (right, Facebook in blue) by country (Serpstat, n.d.; Wallach, 2020)

The Chinese Internet started out small and confined to China itself. However, during the last decade, the influence of the Chinese Internet model on cyberspace abroad has been gradually increasing (Y. Hong & Harwit, 2020; Q. Yin & Li, 2020). Ranging from efforts by Chinese representatives to reform global Internet governance institutions (Negro, 2020), to Chinese companies such as Huawei and ZTE becoming the most important suppliers of telecommunications equipment (Mascitelli & Chung, 2019), to Chinese governmental programs aiming to become the dominant standard setter in fields such as Artificial Intelligence (Department of International Cooperation of the Ministry of Science and Technology, 2017),

the growing importance of the Chinese digital system is leaving its mark on the global Internet as a whole. Given the fundamental differences between Chinese cyberspace and the US-dominated cyberspace, these developments lead to international tensions (Xuetong, 2020), and there is increasing speculation of a global split of the Internet between the Chinese and American cyberspace models (Capri, 2020).

While the developments described above all occurred during the last decade, they are deeply rooted in the longer history of Chinese cyberspace. These developments stem from a system that was shaped by processes of deliberation and contestation between various actors, who each tried to find solutions to the problems they faced, and by doing so shaped the technological, social, economic, and regulatory characteristics of the system as a whole. As this thesis demonstrates, the evolution of Chinese cyberspace was a highly complex and multi-faceted process, in which decisions at an earlier stage created space and momentum for subsequent developments. These interactions ultimately created the conditions in which Chinese cyberspace could become more influential on a global scale. As such, in order to generate a thorough understanding of Chinese cyberspace, it is important to investigate the various developments that shaped Chinese cyberspace and the actors that drove these developments, which is hence the subject of study of this thesis. Given the increasing global influence of Chinese cyberspace, there is an empirical and theoretical need for a deeper understanding of the history of Chinese cyberspace. Understanding the emergence and evolution of this system can increase our understanding of the current behavior of actors and elements in Chinese cyberspace, and, by extension, can help actors involved in cyberspace to better mitigate disagreements with other actors and to better understand and anticipate future developments in cyberspace.

1.2 Research objective

Inspection of the existing literature on the digitalization of China and the international impacts of Chinese cyberspace shows that these subjects have been studied from a variety of academic disciplines and backgrounds, ranging from privacy and Internet freedom (Taubman, 1998; D. Wang & Mark, 2015; Xu et al., 2011) to business and ecosystem research (Arenal et al., 2020; de Kloet et al., 2019; Thomson & Sigurdson, 2008), and geopolitical analyses (Cartwright, 2020; Cheung, 2018; Xuetong, 2020). However, while these relatively narrow approaches increase our understanding of specific issues, the interconnectedness of these fields often remains unclear, and as such, the broader picture is often overlooked. As Chandel et al. (2019) observe in their study on the Great Firewall, research tends to be compartmentalized between studies about technological aspects, social and cultural aspects, or regulatory and policy analyses. While the observation of Chandel et al. concerns studies about the Great Firewall specifically, this pattern is noticeable across literature about Chinese cyberspace. As a result, some authors (e.g., Y. Hong & Harwit, 2020) have made a call for more holistic and historical research on Chinese cyberspace. Still, the amount of literature that can be found on this topic that integrates and connects these various approaches remains comparatively small.

This paper responds to this call by studying the evolution of Chinese cyberspace from a sociotechnical perspective (see Sovacool & Hess (2017) for a recent overview of the state of the art). Given that cyberspace is an area in which technological, economic, legal, social, and cultural elements all play an important role, there is a need for an approach that integrates these dimensions into a coherent structure. Exactly this understanding of how technical and non-technical elements interact and mutually shape processes of change, both in technological and societal terms, characterizes a sociotechnical approach. This paper analyzes the emergence and evolution of Chinese cyberspace to explain why an alternative system appeared

at all, and how the system could evolve from being confined to China to becoming influential across the globe. After all, the fact that Chinese companies are now expanding abroad and that actors from Chinese cyberspace are now involved in global Internet governance and standardization is the result of a myriad of complex interactions that created the conditions for these developments to take place. In addition, the manner in which these developments take place is also strongly influenced by these early interactions. As such, the objective of this paper is to identify interactions between these various elements that have so far remained relatively obscure in academic literature, by analyzing the emergence and evolution of Chinese cyberspace from a sociotechnical perspective.

More specifically, to analyze Chinese cyberspace from a sociotechnical perspective, this thesis makes use of theoretical insights of the Large Technical Systems (LTS) framework. As Sovacool & Hess (2017) show, LTS is widely regarded as one of the most prominent frameworks when studying sociotechnical change. While the details of the framework and the justification for this framework as a conceptual device are discussed in further detail in section 2.2, a brief introduction to the theory and some of its most important theoretical concepts will already be provided here, as they are necessary to develop and explain the research question of this thesis. The Large Technical Systems (LTS) framework has been developed as a means to untangle the complexity of sociotechnical systems, by focusing on the interactions between technical, social and environmental elements and by focusing on agency when analyzing the evolution of such systems (Sovacool et al., 2020). One of the most important concepts of LTS is *system building* (Sovacool et al., 2020). LTS includes the notion that sociotechnical systems are shaped by actors, each with their own incentives, expectations, and norms and values. The decisions made by these actors when encountering problems shape the eventual configuration of the system. Another important concept to introduce is *momentum*, indicating that through a combination of various phenomena, including path dependencies, lock-in effects, and economies of scale and scope, a system becomes configured such that it tends to develop into a certain direction with a certain velocity (T. P. Hughes, 1987, 1995), and due to the mass acquired as a result of these configurations, it becomes hard to divert from this trajectory (Van der Vleuten, 2009). These two concepts serve as the primary analytical devices of this thesis to analyze the evolution of Chinese cyberspace.

1.3 Research question

The considerations above bring us to the following research question:

"How can the emergence and evolution of an alternative cyberspace in China be explained from a Large Technical Systems perspective?"

Note that the word 'explain' can have multiple meanings in social science. In this thesis, the word is used in the sense of a historical explanation, which is also sometimes known as a genetic explanation. The goal of such an historical explanation is not to seek universally applicable truths, but rather to provide seeks to discover the origins and/or development of a specific subject (Brown, 1963), which in this case is the existence of an alternative cyberspace in China.

To answer the main research question, the following three subquestions are posed:

1. *"Why and how did system builders in China develop an alternative Internet model?"*

2. *"Following the emergence of an alternative Internet model in China, how did Chinese cyberspace deviate further from the US-based cyberspace?"*
3. *"How did Chinese cyberspace collide with the US-based cyberspace, and how did the resulting interaction and contestation shape both cyberspaces?"*

The three subquestions correspond to three consecutive chronological timeframes in the development of Chinese cyberspace. While periodization is always difficult in historical research (Bentley, 1996; Green, 1992), the separation of the time periods can be linked to two important developments that had a large impact on the evolution of Chinese cyberspace. The first of these developments is the completion of the Great Firewall, which created the conditions in which US companies had to choose between complying with Chinese regulatory wishes and satisfying domestic critics, while the second of these developments was the shift towards foreign expansion by Chinese companies, as this led to the collision of the Chinese and the US-based cyberspace. As this thesis follows an iterative process, these points of separation were first found from a preliminary literature review and later confirmed through the findings of this thesis.

Making a chronological division matches well with the sociotechnical approach of this thesis, because by studying the research subject chronologically, the interactions between the various co-evolving elements of the system can be emphasized more. Additionally, in a more practical sense, a separation of the research question into several timeframes allows for a better structuration of the thesis, as well as improved readability of the narrative. For each of these three periods, important concepts and notions found in LTS, such as system building, momentum, and co-evolution, are used to interpret the identified developments. The answers to the subquestions are given based on the findings from the respective periods. The conclusions from the three subquestions are then combined to formulate a general answer to the research question.

1.4 Research approach

Through its focus on system builders, this thesis aims to understand the dilemmas that actors involved in the development of Chinese cyberspace faced, by understanding the background of these actors and the broader context in which they had to make choices. In this sense, the evolution of Chinese cyberspace can be conceptualized as a series of consecutive choices made by a variety of actors, each facing a different situation in which their choices were made. This aim corresponds to a *constructivist approach*, which focuses on generating a broader understanding of the subject of study by investigating the views of relevant actors, while also focusing on the broader context in which these actors find themselves (Creswell & Creswell, 2018). In addition, this research follows a *qualitative approach*. As discussed in Creswell & Creswell (2018), a qualitative approach is most applicable if the researcher seeks to acquire a deeper understanding of a topic, especially if it is not yet known which elements are most important when studying the case. This corresponds to the aim of this thesis, as it aims to investigate how and why Chinese cyberspace evolved the way it did. In particular, a qualitative approach helps in understanding the ideas and intentions that actors had when designing the system. Furthermore, since the aim of this research is to identify causes for and relations between certain events, this thesis is *exploratory* in nature. As such, this research makes use of a *qualitative exploratory constructivist approach*.

1.5 Research strategy

As discussed, the Internet in China has developed in a fundamentally different way than it did in other countries around the world. To investigate this development, this thesis analyzes the emergence and evolution of Chinese cyberspace using a *single case study* design, in which the emergence and evolution of Chinese cyberspace is defined as its case. A case study design allows the researcher to ask questions about the "how" and the "why", while also considering the broader context in which this case was situated (Baxter & Jack, 2008). As such, a case study design can be used to truly explore a subject in depth, without a need to reduce complexity (Johannesson & Perjons, 2014). Given the non-typicality of Chinese cyberspace, the evolution of Chinese cyberspace forms an *unusual case* (R. K. Yin, 2018) compared to how the Internet developed in other countries. Given that an unusual case study design is typically used in exploratory research (Seawnght & Gerring, 2008), this design fits well to the exploratory approach of this thesis.

In qualitative research, it is common to combine sources from a variety of backgrounds to construct a broad view of the subject (Creswell & Creswell, 2018). Given that empirical reality is often messy (Parkhe, 1993), this variety of origins of sources can paint a more diverse and therefore more complete picture of the research subject than any individual source type could. However, when studying Chinese cyberspace, there are some limitations to the available types of source materials. As the scope of this thesis is by definition very broad and involves a wide range of actors, it is impossible to answer the research question using interviews or questionnaires. Moreover, some of the most important actors, such as Chinese top-level politicians or board members of large companies, would not be available for consultation. As such, this thesis makes use of a wide range of written source materials, ranging from scientific literature to policy reports and newspaper articles. The source material is analyzed and coded through a combination of predetermined codes stemming from the LTS framework, codes related to the research questions, and emergent codes following from the analysis of the source material.

The findings of this thesis are presented in the form of a structured narrative. The narrative is presented in the form of a thick description (Geertz, 1973) in combination with a theoretical framework, as can also be found in the work of T. P. Hughes (1983). Through the narrative, the most important developments in the evolution of Chinese are contextualized and explained, using LTS as a conceptual device to place the various components of the narrative in perspective. Through the narrative, the subquestions of this thesis are answered, which together contribute to answering the main research question. More details about the methodology of this thesis are provided in section 2.3.

1.6 Academic relevance

As indicated in section 1.2, prior academic research on Chinese cyberspace tends to be highly compartmented. By studying Chinese cyberspace from a sociotechnical evolutionary long-term perspective, this thesis aims to contribute to the existing body of literature about Chinese cyberspace by identifying interconnections that often remain unnoticed when studying Chinese cyberspace from the more frequently applied lenses (which are discussed in section 2.1). In particular, due to the focus of the LTS framework on sociotechnical change, this research aims to provide insight into which events and developments were most impactful in shaping the direction in which Chinese cyberspace evolved. In addition, due to the theoretical focus on system builders combined with the constructivist nature of this thesis, this thesis aims to provide a deeper understanding of how these events and developments were related to the challenges that individual

actors faced, and how their own beliefs and values were translated into characteristics of Chinese cyberspace.

Besides these contributions, this thesis also serves to explore a relatively novel application area of the LTS framework. Thus far, theories of sociotechnical change have not yet been extensively used to explain developments in Chinese cyberspace, or even cyberspace in general. Although a sociotechnical perspective has been applied to study some specific elements of Chinese cyberspace, such as the popularity of Internet cafés (Puel & Fernandez, 2012), the impacts of Chinese cybersecurity legislation on e-government services (H. Zhang et al., 2018), or the diffusion of mobile TV broadcasting in China (T. T. C. Lin, 2012), the wider dynamics that govern Chinese cyberspace remain understudied from a sociotechnical perspective. By demonstrating the applicability of the LTS framework to generate new insights about Chinese cyberspace, this thesis serves to demonstrate that the conceptualization of cyberspace as a sociotechnical system can result in innovative empirical insights and aims to encourage further applications of these theoretical frameworks in the study of digital technologies.

1.7 Societal relevance

More and more, Chinese digital technologies and products are leaving their mark on the global economy and global cyberspace (Y. Hong & Harwit, 2020; Q. Yin & Li, 2020). They increasingly influence global discussions about norms and values in Artificial Intelligence (Feijóo et al., 2020), global Internet governance (Negro, 2020), or global digital trade (Vila Seoane, 2020). Given the distinct nature of Chinese cyberspace, the Chinese ideas and visions about these matters tend to differ from those of many other countries, especially western ones. To increase our understanding of these ideas and visions, it is important to understand the background and the wider context in which these actors operated, and how this context in turn influenced decisions, as well as norms and values, of these actors. Being able to understand the broader picture of Chinese cyberspace can therefore lead to a better understanding of the wishes and concerns that Chinese actors hold regarding these matters, as well as the norms and values that underlie these wishes and concerns. Acquiring a deeper understanding of these ideas and visions is of great societal importance, given that it allows actors involved in cyberspace to better predict and anticipate behavior and wishes of Chinese actors in cyberspace. Identifying differences in norms and values or in opinion about specific aspects of cyberspace can help actors to address these differences, and to mitigate disagreements and take more informed decisions.

1.8 Structure of the thesis

In this section, an overview of the structure of this thesis is provided. Chapter 1 forms a general introduction for this thesis, introducing the subject of study and the objective of this thesis. Chapter 1 also introduces the research question, as well as the approach and strategy to provide answers to this question. Lastly, the relevance of this thesis is discussed. Chapter 2 consists of three main sections. In the first section, the state and the nature of the literature regarding this research subject is discussed. In the second section, the theoretical foundations and the most important theoretical concepts of this thesis are discussed in detail. The third section discusses the methodology of this thesis. Chapter 3 contains a structured narrative that serves to illustrate and contextualize the empirical findings of the research. Chapter 3 is divided into three sections, each corresponding to one of the three chronological timeframes as discussed when introducing the research question. For the sake of clarity of the narrative, each of these sections is again subdivided into

multiple subsections that each describe a distinct development in Chinese cyberspace. At the end of each section, the corresponding subquestion is answered. Lastly, chapter 4 combines the findings from the empirical analysis of this thesis and formulates a conclusion to the research question. Chapter 4 also contains a discussion section, in which the findings of the conclusion are placed in perspective, the limitations of this research are discussed, and recommendations for future research are made.

2 Prior research, theory & methodology

The previous chapter introduced the subject, objective, and approach of this research. In this chapter, the approach is explained in further detail. First of all, an overview of existing academic research is provided to demonstrate what elements of Chinese cyberspace have been studied so far and how these studies analyzed the case, and to identify underrepresented elements. Secondly, the lens used for the analysis in this thesis is discussed, and a justification for the applicability of this lens is provided. The chapter ends by describing the research methodology of this thesis.

2.1 Prior research

Given the broadness of Chinese cyberspace, it is a frequently studied subject in academic literature. However, academic research tends to be compartmented, and it most often either focuses on a specific aspect of cyberspace or it describes cyberspace using a narrow lens. As Chandel et al. (2019) mention in their study on the Great Firewall, "some of [the existing academic papers] focus only on the technology, some only on cultural and social impact and some only on the issues related to local laws and policy." While this quote refers to research on the Great Firewall specifically, this pattern can also be observed across papers about other aspects of Chinese cyberspace.

A literature review has been performed to identify the lenses that are most commonly found in academic literature when describing Chinese cyberspace. Through a set of search queries in the databases of Scopus and JSTOR, articles that describe developments in Chinese cyberspace were identified. These search queries contained either "China" or "Chinese", combined with terms such as "cyberspace", "Internet", "digital technology" or "digitalization". Cyberspace is a very broad and diverse concept by nature. As such, a wide variety of academic articles could be observed, both in terms of subject and of the type of conceptual lens used. Nonetheless, the majority of papers could be classified under either a *ecosystems and companies lens*, a *censorship lens*, or a *geopolitics lens*.

In the following sections, each of these lenses are described in further detail. For each of the lenses, an impression is given about the focus of the lens, subjects that are typically studied through the lens, and limitations of the lens that this thesis aims to address.

2.1.1 Ecosystems and companies lens

A significant amount of research focuses on the rapid growth of Chinese tech companies and seeks to measure and explain this growth. This is done by focusing on firms, their business models, and their interactions within a business ecosystem. Studying the reasons behind the success of Chinese tech companies is interesting and relevant because Chinese tech companies are the only companies that have been able to grow large enough to be considered competitors to the globally dominant US-based tech companies, as mentioned in section 1.1. Studying how these tech companies grew can therefore provide answers to what makes these Chinese tech companies different from their counterparts in other countries.

Within this lens, a shift over time can be noticed in terms of the studied topics. In earlier years, there is a strong focus on technology transfer (A. G. Z. Hu et al., 2005; Velasquez, 2009) and the role of globalization in the development of the Chinese tech companies (Sun et al., 2007; Thomson & Sigurdson, 2008). In later years, academic attention broadened to other topics, with for instance articles on collaborations between Chinese tech companies, government and universities (Arenal et al., 2020; J. Tan

et al., 2020; Yan & Huang, 2020), the financing of Chinese tech companies (J. Hu et al., 2017; Jia & Winseck, 2018) and the emergence of a platform economy (de Kloet et al., 2019; Q. Yang & Ji, 2016). Regarding the chosen subjects of study, no clear difference can be observed between Chinese and international scholars.

The ecosystems and companies lens provides a comprehensive and clear image of how firm dynamics, industry collaborations and business decisions have contributed to the growth of the digital economy in China. However, studies through this lens do not provide an answer to the question what the implications of this growth are. For instance, how does the rapid growth of Chinese tech companies impact the technological design of the Internet, both in China and abroad? How does the Chinese government respond to this rapid growth, both in terms of regulation and stimulation? And how does the alternative set of products produced by these Chinese tech companies change the social dimension of Chinese everyday life? These questions remain unanswered in studies using this lens. Furthermore, studies using this lens tend to underexpose elements contributing to the growth of Chinese tech companies that are not related to economics or business administration, such as the difference in norms regarding company behavior between China and many other countries, or the difficulties for foreign companies to enter the Chinese market. These are all questions for which a sociotechnical lens can provide more thorough answers by investigating these linkages.

2.1.2 Censorship lens

Since the introduction of the Internet in China, a focus on censorship has been a subject of high academic interest. Chinese digital censorship can be considered among the strictest in the world (King et al., 2013; Zittrain & Edelman, 2003). As such, Chinese cyberspace is a very suitable site for studying the effects of restricted information access, and increasingly relevant considering that the tendency towards stricter Internet control can be observed across the globe (Zittrain et al., 2017). The censorship lens can also be frequently found in western media, in which the governmental censorship program commonly referred to as ‘the Great Firewall’ has been a popular subject since the introduction of the Internet in China (Barme & Ye, 1997; Economy, 2018; Y. Wang, 2020; Wiseman, 2008) (although the term ‘Great Firewall’ conveys a certain framing, this thesis makes use of the term when describing the Chinese governmental censorship apparatus, as it is a familiar term to most readers and is also the most commonly used term in the source material used by this thesis).

In early academic literature, the combination of implementing the Internet and having strict censorship policies was seen as contradictory. As such, the main academic debate was about whether it was possible at all to fully implement the internet while keeping control of its contents (R. J. Deibert, 2002; J. L. Qiu, 1999; Taubman, 1998). In later years, the focus shifted more towards the consequences of censorship for Chinese society (Hobbs & Roberts, 2018; D. Wang & Mark, 2015) and ways to circumvent the censorship (Mina, 2014; Mou et al., 2016). There are also significant amounts of research aimed at specifying which types of contents are being censored (Hounsel et al., 2018; King et al., 2013; Zittrain & Edelman, 2003) and the technological functioning of this censorship apparatus (Chandel et al., 2019; Xu et al., 2011).

Perhaps interestingly, this lens is frequently found in papers by both Chinese and foreign scholars, and there are also frequent collaborations between scholars from within and outside China when studying the Great Firewall. However, a difference in emphasis can be identified between scholars working in China and scholars employed outside of China. Scholars employed at non-Chinese institutions often tend to

include critical wording in their paper on the Great Firewall regarding its restrictions on freedom of speech (Joyce, 2015; King et al., 2013) and freedom of information (Tsui, 2003; T. S. Wu, 1997), while scholars employed at Chinese universities tend to use more neutral and analytical language (S. Li, 2018; Z. Yang et al., 2012).

The body of literature that studies Chinese cyberspace through a censorship lens is extensive, yet as Chandel et al. (2019) have written, heavily compartmented. The number of integral studies between the various dimensions of censorship is limited, and studies positioning censorship in the wider context of Chinese cyberspace even more so. Nonetheless, due to this diversity, the existing literature can be used well to identify connections with other elements of Chinese cyberspace.

2.1.3 Geopolitics lens

Papers written through a geopolitical lens tend to describe cyberspace and digital technologies as a means through which geopolitical and geoeconomic pressures are exerted. Besides academic literature, this lens can frequently be found in newspaper articles (Bennhold & Ewing, 2020; Layton, 2020; Nicolaci da Costa, 2019) and reports by think tanks (Capri, 2020; Dekker et al., 2020). Perhaps more importantly, governmental actors from the US (Pompeo, 2019; Schmidt et al., 2021), China (Global Times, 2021), and the EU (Tamma, 2020), among others, frequently describe cyberspace through this lens in speeches and reports. This indicates that this lens also heavily influences political debates across the globe.

In academic literature, the geopolitical lens gained popularity during the second half of the 2010s, coinciding with the increased framing of the US-Chinese relationship as a rivalry (Goldstein, 2015; Kennedy & Lim, 2018; S. Zhao, 2015). Frequently studied topics using this lens are cybersecurity (Cheung, 2018; Lindsay et al., 2015; Qian, 2019), the role of digital technologies in trade wars (Ciuriak, 2019) and the decoupling of the US and Chinese cyberspheres (Xuetong, 2020). In particular, the tensions surrounding the US ban on Huawei in 2019 and 2020 are frequently studied as a case through this lens (Cartwright, 2020; Inkster, 2019).

What this lens does well is sketching the international (political) consequences of the evolution of Chinese cyberspace. However, by reducing the discussion around digitalization to competition between countries and spheres of influence, many important developments in the evolution of Chinese cyberspace and its consequences are easily overlooked. For instance, social and ethical consequences are not often described when using this lens, or at most as being instrumental to the geopolitical debate. A sociotechnical lens can also identify the non-geopolitical consequences of discussions in which geopolitics play a role.

2.1.4 Towards a sociotechnical approach

As already mentioned while discussing the previous lenses, each of them has its own strengths, yet does not provide a full explanation for the evolution of Chinese cyberspace. Of course, these three lenses do not encompass the full extent of academic literature on Chinese cyberspace. Many more can be found. Nonetheless, as Hong and Harwit (2020) argue, there is a need for more integral analysis of Chinese cyberspace by applying a broader view than can usually be found in academic literature. A well-chosen lens is vital for discovering these obscured linkages. In the next chapter, the lens that is used in this thesis for this purpose is discussed.

2.2 Theoretical approach

This section discusses the theoretical lens through which the case is studied. As mentioned in section 1.2, the theoretical approach is based on the Large Technical Systems (LTS) framework. This section starts by describing the LTS framework and some of the most important theoretical concepts that are used for the analysis. It then proceeds to explain the choice for LTS as a conceptual framework and discusses the applicability of the framework to this case. Lastly, some considerations are provided regarding the adjustment of the framework to the local context in China.

2.2.1 Large Technical Systems framework and its core concepts

As we saw in the previous section, the lens through which we analyze a case heavily influences our findings and analysis of that case. As such, it is very important to choose a theory that aligns well with the purpose of the research. Looking at the purpose of this thesis, we wish to describe the evolution of Chinese cyberspace from a sociotechnical angle, thereby considering technological, economic, organizational, cultural, and institutional elements and their mutual interconnectedness. The Large Technical Systems (LTS) framework fits this purpose well. The development of the framework began around the 1980s (T. P. Hughes, 1979, 1983, 1987). After four decades of work, the state of the art has been recently summarized in three papers authored by Sovacool and Hess (et al.) (Hess & Sovacool, 2020; Sovacool et al., 2020; Sovacool & Hess, 2017). LTS was developed as a means to untangle the complexity of sociotechnical systems, by focusing on the interactions between technical, social and environmental elements and by focusing on agency when analyzing the shaping of such systems (Sovacool et al., 2020). The framework is not meant as a strict definition of how a sociotechnical system behaves or what components it consists of, but rather as a conceptual toolbox that can aid in understanding the complex interactions and the characteristics of a sociotechnical system (T. P. Hughes, 1986). Initially, studies using the LTS framework mainly focused on regional or at most national sociotechnical systems. However, in more recent years, the framework has also been applied to study transnational sociotechnical systems (van der Vleuten & Högselius, 2012; van der Vleuten & Kaijser, 2005, 2006). Although there is no singular LTS approach (van der Vleuten, 2004), there are concepts that recur in most LTS studies, such as system building and momentum. These concepts are discussed in the following paragraphs.

System builders

The concept of *system builders* was designed as a means to study agency in the development of sociotechnical systems, which until that point were usually studied in more abstract structural terms (T. P. Hughes, 1983). A system builder is a central actor involved in the creation of a new sociotechnical system. This system builder is involved in transdisciplinary problem solving (Van der Vleuten, 2009), thereby creating new connections that together shape this sociotechnical system. Typically, a ‘follow-the-actor’ approach is chosen to scrutinize the activities of this system builder (van der Vleuten, 2004). Studying system builders allows for a more detailed analysis of the exact ways in which a sociotechnical system was shaped by the actions and decisions of individual actors, as well as the challenges and dilemmas that actors faced when making these actions and decisions.

Many studies on Chinese cyberspace define the Chinese government as the central actor, in a certain way comparable to the concept of a system builder. However, these approaches are often reductionistic and

neglect much of the agency that shaped Chinese cyberspace. As such, for this case study, system building is not studied by following a single actor, but rather by treating system building as a 'distributed, highly contested, and open-ended multi-actor game', as happens more frequently in recent LTS studies (Sovacool et al., 2020). While there is still significant attention to agency and the context in which actors face decisions, this conceptual choice allows for a broader approach to Chinese cyberspace by considering a wider variety of elements and their evolution, instead of limiting attention to the situations in which a specific actor was involved.

Momentum

After a while, an LTS has grown so much that it becomes resistant to change. Due to deep embeddedness between the various elements of the system, a system gains *momentum*, which is a term borrowed from physics. As the interconnections between the various elements of a system become deeper and the scale of the system increases, it acquires *mass*, and it tends to develop into a certain *direction* with a certain *velocity* (T. P. Hughes, 1987, 1995; Schubert et al., 2013). Once a system has gained momentum, it becomes difficult to change its trajectory. This stability is caused by matters such as vested interests, commitment of actors, sunk costs, and fixed assets (T. P. Hughes, 1987), and as the mass of a system increases, this leads to resistance to changes to the trajectory that the system is headed towards (T. P. Hughes, 1983). The concept of momentum corresponds to the concepts of *path dependency* and *lock-in effects*, as found in the economics of innovation literature (Arthur, 1989; David, 1985; Liebowitz & Margolis, 1995).

The concept of momentum is important for studying the evolution of Chinese cyberspace in two ways. Firstly, identifying the momentum of a system helps explain the behavior of actors. The momentum of a system changes the way that actors think and act. Had the momentum of the system been different, then perhaps an actor facing the same situation would have behaved differently. As such, momentum is an important concept in understanding the situation within a system, and why system elements co-evolve in a specific manner. Secondly, studying momentum is also a useful concept to evaluate the impact that certain developments have. A highly impactful development can change the momentum of the entire system, thereby altering the trajectory that this system will follow in the future, given that system elements will now co-evolve into a different direction or with a different pace. Conceptualizing momentum can help identify the most impactful developments on the evolution of the system at large. Therefore, following these two considerations, momentum can both be understood as a cause for system developments and as an effect of them.

2.2.2 Applicability of Large Technical Systems

This subsection discusses the applicability of Large Technical systems, and contains a justification for the choice of this framework as a conceptual device for this thesis.

A large portion of LTS studies focuses on the connection between material and non-material elements of a system. When defining Large Technical Systems, Joerges (1988) speaks of "complex and heterogeneous systems of physical structures and complex machineries", indicating a strong emphasis on physical components. Although the Internet is also based on a physical infrastructural network (Winseck, 2017), most important changes to cyberspace take place without a need for major changes of the physical Internet structure, as these changes are primarily made in the digital realm. In this sense, cyberspace does not fit this traditional description of an LTS well. However, more recent scholars tend to define an LTS slightly differently. For instance, Mondschein et al. (2021) reduce the requirements for when a system can

be considered a Large Technical System to two fundamental properties: they are sociotechnical, and they are networked. If we follow these two properties, then cyberspace does qualify as an LTS. There is an inseparable connection between technological elements, such as network protocols, data structures and algorithms, and social elements, such as regulations, cultural norms, and economic incentives. Cyberspace is also networked; after all, the word Internet quite literally signifies a network connecting smaller computer networks. Additionally, the Internet can be seen as connecting people across large distances. These new digital connections allow for new types of interactions between system actors. In this sense, the Internet itself also functions as the intangible infrastructure for a wide range of societal functions, ranging from communication to information supply, commerce, and banking. These considerations indicate that cyberspace can certainly be characterized as an LTS.

An advantage of using LTS to analyze this case is its 'follow-the-actor' approach (van der Vleuten, 2004). Given that digital markets tend to become monopolistic over time (Kuchinke & Vidal, 2016; Van der Aalst et al., 2019), the amount of private companies that play a large role in Chinese cyberspace is limited. Likewise, given that the number of governmental actors involved in Chinese cyberspace is also limited, no large generic actor groups can be found here either. Due to the limited number of influential actors in Chinese cyberspace, zooming in on the behavior of these actors can reveal important dynamics that shaped the evolution of Chinese cyberspace. Although actors are still at times categorized as groups (such as 'US tech companies' or 'Chinese tech companies'), this thesis frequently scrutinizes the situation that individual actors found themselves in to explain the wider system dynamics.

LTS is by far not the only framework describing sociotechnical change. Many others exist, such as Social Practice Theory, Sociotechnical Transitions, or Actor-Network Theory (Sovacool & Hess, 2017). However, after consideration, it was found that LTS most likely forms the most useful framework for the stated purpose of this thesis and the case at hand. Social practice theory focuses in depth about the reasons why actors make specific choices (Shove et al., 2012), yet appears less suitable to analyze how larger trends that shape a system change over time, which LTS covers with its conceptualization of momentum. Bridging the dynamics between micro, meso and macro levels is also a strength of the Sociotechnical Transitions framework (for a summary of the state of the art of the field, see Köhler et al., 2019). As argued by Geels (2007), a benefit of using the Sociotechnical Transitions framework is that it can be considered more specialized than LTS in describing transformations of systems that have long been established and undergo fundamental transitions at later stages of their life cycle. However, given the novelty of cyberspace, it becomes hard to identify a clear transition, as it rather entails the creation of a novel system that does not have a clear predecessor and the case focuses on the early years of this system. In addition, due to the novelty of this system, making a clear distinction between regime and niche actors (Geels, 2002; Geels & Schot, 2007) becomes difficult. Lastly, Actor-Network Theory conceptualizes the technological and social elements constructing technology as being interrelated and part of the same network, thereby making the interactions between technical and non-technical elements insightful (Latour, 1999). A major difficulty when applying Actor-Network Theory on this case, however, is that due to the scope of Chinese cyberspace and its rapidly changing nature, the number of important elements and network configurations in Chinese cyberspace is very large. Conceptualizing the entire evolution of Chinese cyberspace in an Actor-Network would either leave out relevant developments or simplify them through black-boxing (Kaghan & Bowker, 2001), or, if all relevant information would be presented, it would become highly complex for the reader to understand all the processes at hand.

As mentioned, LTS is a highly flexible framework that serves more as a conceptual toolbox for identifying and understanding the complexities of a sociotechnical system than as a strict definition of how

a sociotechnical system behaves. By design, it leaves sufficient space to investigate how the various elements of the system behave and interact. As such, the framework forms a good match with the exploratory constructivist approach of this thesis. Nonetheless, the LTS framework also has its limitations, which should be acknowledged in advance. For instance, due to the focus of LTS on larger and more structural processes (Rutherford & Coutard, 2014), there is a risk that the importance of smaller actors, such as users, is underrepresented. As such, it is important to reflect in hindsight how this limitation influenced the outcomes of the research. This reflection can be found in section 4.2.2.

All in all, the considerations above form the justification for LTS as a heuristic device for this case study. Although the amount of literature studying digital technologies from an LTS perspective is still very limited, the last paragraphs have shown that LTS forms a good match with the subject of study.

2.2.3 Adapting the lens to the local context in China

The Large Technical Systems (LTS) framework, like many other frameworks describing sociotechnical change, was developed analyzing cases situated in a western context (T. P. Hughes, 1979, 1983). As such, the framework reflects many particularities that can typically be found in this western context. However, given that the subject of this thesis is about Chinese cyberspace, it is important to question whether the concepts used in LTS are also applicable to the Chinese context, or whether they need to be slightly modified or extra attention should be paid to certain details, to be able to fully understand the case and its broader context. While most aspects of the LTS framework, such as the conceptualization of momentum or the follow-the-actor approach, function well without alterations, two empirical differences that one should be aware of are discussed below.

The first question that needs to be asked is how to conceptualize the Chinese government. In principle, this question is relevant for any national government studied in academic research, as it never consists of a single entity. However, especially in the case of the Chinese government, this question is important to ask. The Chinese government consists of large networks of ministries, cross-ministerial committees, and regional and local governments. One might also ask whether people working at a company that are active members of the Chinese Communist Party (CCP) should even be considered part of 'the government', as the line between the CCP and company executives is often blurry (Hamilton & Ohlberg, 2020; Melnik, 2019). Therefore, it is important to decipher who exactly is responsible for certain tasks within the government. This might at times be challenging to research due to limited public information on exact responsibilities, but studying specific governmental actors as system builders is likely a more accurate representation of reality than studying the government as a whole, and allows for a better understanding of the context in which actions and decisions take place.

Another important aspect to be aware of when applying the concept of system builders in the Chinese context is the way in which Chinese policy plans are usually shaped, as this also tends to differ from western contexts. Large policy plans in China are usually not fleshed out from the start. Instead, they are loosely defined, and details only emerge after a gradual process of elaboration. Typically, a central, higher-level governmental actor, formulates an ambition in high-level policy plans, which can be considered more of a goal than a means towards that goal. Even the details of the goal itself are often still up for negotiation and only specified later. An example of this process is how the concept of cyber sovereignty developed within China (Creemers, 2020b; Zeng et al., 2017), but the same pattern can be recognized in other policy plans as well. This policy cycle also fits well into the LTS framework, as it shows similarities with the analogy

of visionaries who set out a course, and then through experimentation and trial and error gradually build a system.

2.3 Methodology

This subchapter discusses the methodology of this thesis. Firstly, the collection of data for this thesis is discussed, including the origins of the source material, the different categories of source materials, and how individual sources within these categories were selected. Secondly, the analysis of the data is discussed. Thirdly, the subchapter is concluded by discussing how the analyzed data is used to formulate answers for the research question.

For the sake of clarity for the reader, the steps described above are listed in the order in which they would be expected in a linear process. However, it is important to note that, in qualitative research, data collection and analysis form an inherently iterative process (Bazeley, 2013). While the initial data collection is driven by an initial understanding and expectations about the subject of study, unexpected elements are encountered in the process. Since the goal of a qualitative exploratory study is to generate a better understanding of the studied case and its broader context, additional data is gathered to delve further into these unexpected elements if the initial data selection is not conclusive or comprehensive enough. This cycle can occur numerous times, hence the iterative nature of qualitative research (Srivastava & Hopwood, 2009). This iterative nature implies that the steps described below are not performed consecutively, but iteratively. Within the text, sometimes the distinction is made between the initial analysis (indicating the first iteration through the cycle) and further analysis (indicating subsequent iterations).

2.3.1 Data collection

As mentioned, this section describes the source material used for this thesis. The cultural background of the source material, the various categories of source material, and the selection of specific materials within these categories are discussed.

Cultural background of source material

Since I (the researcher) cannot read Mandarin, this study makes use of sources written in English. This is not a big limitation, however, as there is a large amount of source material available in English from both Chinese and international authors. This means that the limitation of using only English sources does not cause Chinese views to be underrepresented in the research. However, as has been shown by Herold and De Seta (2015), there is a regional bias in academic sources studying the Chinese Internet, with the majority of authors based either in US and China. It is important to acknowledge and critically evaluate the background of each source (Creswell & Creswell, 2018; Garraghan, 1946), especially considering the regional differences that can be noticed in the description of these source materials (as elucidated in section 2.1).

Categories of source material

In qualitative research, it is common to use a multitude of different source types, as they can complement each other and each provide additional insights (Creswell & Creswell, 2018). Therefore, this research paper uses a variety of source types. The source types that are featured most prominently are listed below.

First of all, academic literature is analyzed to identify major developments that influenced the digitalization of China. These academic sources include books and articles that apply the popular lenses described in section 2.1, but also materials that approach Chinese cyberspace from other perspectives. While these papers apply a different lens than this thesis, their analysis is still valuable to explain specific elements of Chinese cyberspace. Additionally, and importantly, the academic literature also contains substantial amounts of empirical information that can be used to build the narrative of this thesis and to contextualize the described developments.

Secondly, the research makes use of newspaper articles from international and Chinese newspapers (many major Chinese newspapers, like Xinhua or the China News Agency, also publish in English). The main advantage of newspapers is that they were not written in hindsight, but write about ongoing issues. As a result, they are likely to highlight different relationships than texts that were written afterwards, and therefore form a valuable addition to this research. In addition, they are usually focused on a specific event, and as such often contain more specific details than the other source types.

Thirdly, (translations of) policy documents by governments and international organizations (e.g., World Bank, ITU) and reports by think tanks and research institutes (e.g., Merics, Fraunhofer ISI) are used to further complement the data used in this research. Policy documents often form first-hand descriptions of political plans, and as such are valuable for understanding the considerations of the actors issuing these policy documents. On the other hand, reports by third parties tend to dive deeper into a specific subject and to highlight the frictions and nuances regarding this subject. As such, both document types can form a valuable contribution to this research.

Selection of source material

As mentioned before, this thesis follows an iterative process in terms of its methodology. As such, this subsection first discusses how the initial source material for this thesis was selected, followed by how this process went for subsequent cycles.

The goal of the initial analysis was to immerse oneself in the current literature written on Chinese cyberspace and to discover the main elements of and developments in Chinese cyberspace, rather than immediately searching for details and intricacies about these developments. The initial analysis was based on information found in academic literature, as this source type tends to focus most on larger trends and developments. Relevant sources were identified through search queries in the academic database of Scopus. A number of search queries were used, each including either “Chinese” or “China” in combination with a cyberspace-related term, such as “cyberspace”, “Internet” or “digitalization”. A number of steps were taken to further reduce the resulting set of sources. First of all, only articles with a high number of citations were considered, as these articles are likely authoritative in their respective domains, and thus would provide a good starting point for the analysis. The classification ‘high number of citations’ is a relative term in this context. For instance, when selecting sources focusing on censorship in China, which is a popular subject in academic literature, the threshold for inclusion was much higher than literature about, for instance, AI policies in China, about which less academic literature exists. Secondly, attention was paid to the temporal distribution of sources. Instead of only selecting literature about a specific subject when this subject enjoyed strong academic interest, a broad temporal variety of the source material would lead to a wider scope in terms of the discussed developments. Thirdly, despite the broad focus of this thesis, not all sources were equally relevant. Many of the results concerned general trends in digitalization and general aspects of cyberspace. While they may be relevant for understanding the wider context in which developments in

China take place, it was important to reflect per source whether the subject is relevant for Chinese cyberspace, or merely cyberspace in general, to maintain the distinction between Chinese and general cyberspace. Besides the consideration above, any source resulting from the search queries described above was in principle considered relevant for the initial analysis. As explained in section 1.2, the goal of this thesis is to build a comprehensive understanding of the evolution of Chinese cyberspace. This means that no aspects of Chinese cyberspace were excluded from the research in advance, as any subject discussed in the source materials could provide new insights for the case. Furthermore, as explained in section 2.2, this thesis does not focus on a single system builder, but rather conceptualizes the structuration of the system as the result from a multi-actor game. Therefore no prior selection was made to focus on a specific actor. Instead, the source material would be analyzed to identify these relevant actors.

As such, all source material resulting from the aforementioned search queries that fulfilled the requirements above could be analyzed. However, when deciding to analyze a new article, an important aspect to consider was that of saturation (Charmaz, 2006; Creswell & Creswell, 2018). After a given number of articles on a specific subject had been read, the amount of new empirical information that could be found in each of them became negligible. At this stage, one can say that saturation regarding this specific subject had been reached. As such, the initial analysis ended once saturation was reached on the main developments in Chinese cyberspace.

This brings us to the subsequent iterations. For each of the subjects that were identified through the initial analysis as being important developments in Chinese cyberspace, search queries would be used in general Internet search engines (such as Google) to identify relevant newspaper articles and policy documents, as well as queries in academic libraries (such as Scopus and JSTOR) for additional academic literature on the subject. As such, while the initial investigation was mainly based on academic literature, later iterations contained a more diverse mixture of sources. Additionally, forward and backward citations of academic literature were used to identify further relevant source materials. While forward reference searching mostly leads to more academic literature, backward reference searching leads to a wide variety of source materials, as academic literature on Chinese cyberspace typically also cites significant amounts of newspaper articles and policy documents. The subsequent iterations were both useful in cases in which it appeared form the initial analysis that there was a need for further investigation into specific subjects, or certain aspects of these subjects, as this additional information could be found, as well as for subjects of which large amounts of information could already be found, as the subsequent iterations could provide more detailed and specific information about the context of these developments.

As mentioned, source evaluation is highly important, both during the initial and subsequent analyses. Factors that were considered for each source include, among others, its date, authorship (including their geographic origins), its own source materials, its integrity and the credibility of its contents (Creswell & Creswell, 2018; Garraghan, 1946), in order to adequately evaluate and interpret the source material and place it into perspective. Furthermore, where possible, multiple independent sources were consulted to verify whether observations made by one source are also shared by other sources, thereby increasing its credibility.

2.3.2 Data analysis

As mentioned, the approach of this thesis is exploratory. Its aim is to find connections between a range of different elements of Chinese cyberspace using LTS as a lens to find these connections. As such, a mix of predetermined and emergent codes was used while analyzing the sources. Some predetermined codes were

based on the various concepts of the LTS framework, and helped reveal these concepts in the source material. Other predetermined codes were based on the research question and the subquestions. For instance, when answering the subquestion about the collision of the Chinese and US-based cyberspace, codes about the internationalization of Chinese cyberspace were used. Furthermore, while analyzing the contents of the source material, codes describing the most prominent themes and important elements of these contents emerged organically (Creswell & Creswell, 2018). For these emergent codes, the research made use of evolutionary coding (Mayring, 2002), meaning that codes were created, removed, combined and separated during the process, and the texts were coded again once the final set of codes had been established. Using this combination allows for a proper exploration of the topic, as the codes are not driven by prior empirical assumptions and theories. At the same time, codes based on LTS help structuring the contents in the boundaries of the lens.

Regarding the source material, it is important to consider the background of each source. Given that the scope of the research is Chinese cyberspace, there may be significant differences in point of view between Chinese and international sources. As such, it is important to be aware of the background of the authors of a source when analysis the source material. Furthermore, Chinese cyberspace is a highly politicized subject (Y. Hong & Goodnight, 2020). As such, authors may have certain intentions with their writings. A policy document from the US congress clearly has a different goal than an academic paper from a Chinese researcher. Again, while analyzing the source material, it is important to be aware that text itself is not neutral, but conveys a certain framing (Goffman, 1974; Tannen, 1993).

2.3.3 Using the narrative to formulate answers

The data is presented using a structured narrative, which highlights the relationships between the various identified themes (Creswell & Creswell, 2018). This narrative is presented in the form of a thick description (Geertz, 1973), which is characterized by the phenomenon that it does not just describe the events that occurred in a case, but also describes its wider context in detail. This detailed contextualization can give a better understanding to the reader how and why certain events took place, which aligns well with the research objective of this thesis. The narrative discusses the various developments in a chronological structure. This chronological structure serves to better emphasize the co-evolving nature (see section 2.2) of the development of Chinese cyberspace. For the sake of clarity, occasionally a specific subject in the narrative is concluded before continuing to the next subject, even if the next subject overlapped in time with the previous one. Nonetheless, generally, the narrative is chronological.

The structured narrative in this thesis forms a historical reconstruction of the emergence and evolution of Chinese cyberspace, to which all the aforementioned types of source material contribute. As each of them can contain valuable empirical insights for this reconstruction, they are not treated or referred to separately in the structured narrative. Instead, they are used interchangeably and complementarily. Often, a part in the narrative contains references to some general empirical observations found in academic literature, followed by references to several newspaper articles or policy documents that provide more details about the discussed subject or they construct the context of these developments. This reinforcement of the various source types underscores the benefit of using multiple source types.

The narrative does not only contain a reconstruction of the events and developments that took place, however. Throughout the narrative, the presented information is analyzed and evaluated through the LTS lens. By conceptualizing the described developments in terms such as system building, co-evolution and

momentum, the role and meaning of these developments in the larger evolution of Chinese cyberspace can be better understood.

3 Findings

This chapter describes and explains the evolution of Chinese cyberspace using the theoretical concepts described in section 2.2. The information is presented through a structured narrative. The chapter is divided into three sections, corresponding to the three subquestions and timeframes discussed in Section 1.3. Each section is again subdivided into a few subsections that each discuss a different development in Chinese cyberspace. After each subsection, the observations of that subsection are summarized, and a conclusion is given about what the developments described in that subsection meant for the overall development of Chinese cyberspace. Furthermore, at the end of each section, an answer is given to the corresponding subquestion.

3.1 Period 1 – Origins

This section aims to answer the following subquestion: *"Why and how did system builders in China develop an alternative Internet model?"*. It does so by scrutinizing the most important developments in Chinese cyberspace between the introduction of the Internet in China and the completion of the Great Firewall project, paying specific attention to the actions of actors that led to this alternative Internet model and the reasons for these actions. This section is subdivided into three subsections. The first one discusses the early expansion of the Internet in China and the differences in vision between Chinese and international system builders. The second subsection discusses the creation and evolution of the Great Firewall, as well as its wider impacts on Chinese cyberspace. Lastly, the third subsection discusses the earliest expansions of US tech companies into China, focusing on their interactions with Chinese actors and the difficulties that these US companies experienced.

3.1.1 Early visions of the Internet and initial responses

Compared to most other countries, China was a latecomer to the global Internet (X. Dai, 2002). Following the first received email in 1987, the first dedicated Chinese cable connection to the World Wide Web was established in 1994 (FlorCruz & Seu, 2014). The physical cable went from the Institute of High Energy Physics in Beijing to the Stanford Linear Accelerator Center in California, US, and the required routers were provided by the US company Cisco (Cottrell et al., 1994). During its early years, many in China considered the Internet primarily as a tool for researchers to communicate academic findings internationally. The earliest Chinese Internet users were also predominantly academics. As such, Chinese governmental actors initially saw no need for state intervention in the Internet (X. Wu, 2005). However, following the opening of the Internet to the general public in 1995, Internet users became more diverse and their number increased sharply (Economy, 2018; Harwit & Clark, 2001; W. Wu, 1996).

Almost immediately after the introduction of the Internet, four competing Chinese Internet networks were created by four different state ministries and commissions (Shen, 2016). Two of them were intended for educational purposes, and two for commercial ones. These networks were all soon connected to the global Internet (Z. Tan, 1999). However, the Chinese State Council (akin to what is called the cabinet in many other countries) had become concerned about the competition between these various state-supported networks (Harwit, 2008). As a result, in 1994, the National Joint Conference on Economic Informatization was established to reorganize Chinese Internet governance and to end competition between these networks and the ministries that had created them. The conference was followed by the creation of

the State Council's Steering Committee on National Information Infrastructure (NII) in 1996. Internet regulations from any governmental body or agency first had to be approved by the NII, making it the final decision-maker on Internet regulations (Z. Tan, 1999). In the same year, the State Council established stricter state control on the development of the Chinese internet, signing a temporary regulation with provisions that the Chinese state was in control of 'the development of all areas related to the Internet', and that all connections to the Internet had to be 'channeled via international ports established and maintained by the Chinese Ministry of Post and Telecommunication' (Barme & Ye, 1997). The Chinese governmental Internet administration was further centralized in 1998, when all existing governance bodies involved in telecommunications or electronics were merged into the newly established Ministry of Information Industry (MII) (Z. Tan, 1999). From these developments, it becomes apparent that the State Council intended to position itself as a central actor in this newly emerging sociotechnical system in China that we now call cyberspace, granting it the possibility to act as an important system builder. As we will see in the rest of this thesis, the State Council and the Chinese Communist Party (CCP) are indeed one of the most important system builders in Chinese cyberspace.

In general, the responses by the CCP and the Chinese government towards the introduction of the Internet were two-sided. On the one hand, it was recognized at a very early stage that the Internet contained the promise of being a main driver for economic growth (Baum, 1994; Hachigian, 2002; Hao et al., 1996). The Chinese government had already named the year 1996 the 'Year of the Internet', even though China still only had around 150.000 Internet connections (Barme & Ye, 1997) and 1000 registered domain names (Z. Tan, 1999). In practice, however, the number of Chinese Internet users was much larger than the number of connections. In the 1990s, the average income of a Chinese household was still low, whereas owning a private computer was expensive. This led to the rapid rise of Internet cafes, which formed a much cheaper means to access the Internet (Du, 1999; J. Hong & Huang, 2005). Especially in rural areas and smaller cities, internet cafes played an important role in making the Internet more accessible (J. Hong & Huang, 2005). Additionally, governmental supervision (which will further be discussed in section 3.1.2) was weaker in Internet cafes than when using private internet connections, which also contributed to their popularity. This weaker supervision even made wealthier citizens use the Internet cafes, instead of using their own private computers (J. Hong & Huang, 2005; Puel & Fernandez, 2012).

In its Tenth Five-Year Plan published in 2001, the CCP defined informatization as one of its main concerns for economic and social development. The important economic role of the digital sector was reflected in official economic statistics, which showed that in 1999 10.5% of Chinese GDP growth came from the ICT sector, a figure that was predicted to rise to around 40% in 2010, while the number of Internet users grew twentyfold between 1998 and 2001. To facilitate this growth, the Chinese government issued the construction of a large national fiber optic cable grid. (X. Dai, 2002). The Tenth Five-Year Plan also emphasized the importance of rural informatization (Qiang et al., 2009), to make sure that not only the richer cities in the east would benefit from these developments, but the rest of the country as well.

On the other hand, while the Internet was accompanied with large economic promises, the government feared its liberal nature. As exemplified by the famous 'declaration of the independence of cyberspace' (Barlow, 1996), there was a widespread idealism surrounding the early Internet, which defined cyberspace as borderless and beyond the realm of governmental regulation (Goldsmith & Wu, 2006). However, this conception of a free lawless space conflicted fundamentally with the norms and values that the CCP promoted regarding information control in society. Already before the Introduction of the Internet, China had had a long history of information censorship (Lei, 2011; W. Zhang, 1990). Prior to the 1980s, the New China Bookstore held an official monopoly on the distribution of all publications within China,

and the governmental Central Bureau of Publishing supervised all materials before publication. Only state-prescribed books could be sold (Yi Chen, 1992). This system had become less strict during the 1980s with the emergence of private book vendors and an increasing range of tolerated subjects, but a turn to stricter information control was made again after 1989 (Yi Chen, 1992; Griffiths, 2019).

The Chinese government thus sought a way to make this new technology compatible with its norms and values. Government officials started issuing warnings that the Internet would lead to undesired contents. For instance, the Chinese Minister of Post and Telecommunications stated that not all foreign information should simply be allowed to flow in, and that as a sovereign nation, China had to strengthen its information management (Taubman, 1998). In 1996, the Ministry of Post and Telecommunications had officially been given responsibility of monitoring incoming information flows (Barme & Ye, 1997). The first Chinese regulations regarding the Internet were issued in 1997 by the Ministry of Public Security, issuing that it was illegal to use the Internet to 'harm national security; disclose state secrets; or injure the interests of the state or society' (Lum, 2006). However, these very general clauses would soon be followed by a much more comprehensive system, which among western media and scholars came to be known as the 'Great Firewall'. This subject will be further discussed in subsection 3.1.2.

Interestingly, we can identify two large developments intersecting here. On the one hand, through its technological and institutional design, a liberal philosophy was deeply embedded in the global Internet system. Through this embedded philosophy, the global Internet generated momentum towards marginal, or even without, government interference. On the other hand, there was widespread and deeply embedded information censorship in China. In a way, the Chinese information system, including its actor network and its legal, institutional, and organizational configuration, can also be considered a sociotechnical system with strong momentum towards preserving this censorship. However, given that the technological format of the Chinese information supply gradually shifted from being paper based to being digital, these two systems intersected and merged. As the momenta of these systems conflicted with each other, this caused friction, and the way that this system would develop was up for contention. Eventually, this contention would be resolved, as will be discussed in the next subsection.

3.1.2 The Great Firewall

The desire of the Chinese government to align the Internet with Chinese norms and values on content regulation culminated in a comprehensive Internet censorship program. Although the exact process leading to the creation of the Great Firewall is unclear, the project is often ascribed to Fang Binxing, who was the head designer of the project and is also often referred to as the 'father of the Great Firewall' (Global Times, 2011). However, while the Great Firewall is most well-known in the west, it is just one part of a broader censorship program: The Golden Shield project. This project was initiated in 1998 by the Ministry of Public Security as an umbrella project to filter undesired contents from the Internet (J. Wu & Lam, 2017). These contents include politically sensitive information, but also matters like online scams and pornography (Chandel et al., 2019). Managing digital information and communication was (and still is) important to the Chinese government. In its censorship efforts, the Chinese government is mainly concerned with citizens organizing themselves in collective action, protests or strikes (Herold & Marolt, 2011; Zeng et al., 2017). When mobilizing forces are either noticed or expected, these organizing forces should be obstructed, for which censorship is an important tool (So & Westland, 2009). This principle implies that criticism on the government is not that bad per se and often tolerated, as long as it does not lead to collective action or societal unrest (King et al., 2013).

The development of the Great Firewall was a process that unfolded gradually over time and contained several consecutive stages. Within each stage, more sophisticated technologies for content blocking and filtering were created to further increase the effectiveness of the system. The development of the first stage began in 1998, and contained several ways to restrict information access that were gradually expanded and improved upon. It became possible to block specific IP addresses and domain names, making specific websites completely inaccessible (Chandel et al., 2019). An important factor of the effectiveness of the Great Firewall was the way that the optic fiber infrastructure in China was designed. All international Internet traffic towards China had to pass through one of three exchange nodes, which were located near Beijing, Shanghai and Guangzhou (Butcher, 2019; R. Deibert, 2013; Hanson, 2015). Most hardware of the Great Firewall was located at these three exit points, meaning that all incoming and outgoing Internet traffic physically passed through the censorship apparatus (J.-A. Lee, 2018). Additionally, most internal Internet traffic going through China was also routed through these three points. Although routing so much traffic through these three nodes came at the cost of reduced speed and stability for Internet users living far from these nodes, it also increased the effectiveness of internal censorship (Hanson, 2015). This design principle has remained unaltered in the Chinese Internet infrastructure.

These technological applications were accompanied by regulatory adjustments. For instance, information was gathered about which Internet connection belonged to whom, making it much harder to be anonymous on the Internet. Chinese Internet service providers were obliged to verify the identity of anyone wishing to receive an Internet connection, and many popular websites (and later also smartphone apps) required an original identity card to register. Measures were also taken in the popular Internet cafés. Users of these cafés were obliged to show their identity cards before making use of the service. Additionally, all Internet cafés were required to install surveillance software to monitor suspicious behavior of its customers, and immediately provide their ID information to the local police in case of suspicious activities (Chandel et al., 2019). Enforcement of the Great Firewall happened in two ways. On the one hand, there was the governmental censorship apparatus, which was estimated to have around 30,000 police officers employed to monitor the Internet (Watts, 2006). On the other hand, companies themselves were also expected to self-regulate in order to comply with censorship regulations (R. Deibert et al., 2011). Through a new regulation in 2000, companies were made responsible for any contents on their own platforms, regardless of the author (Rongji, 2010). As such, any company offering digital services or content was expected to have a division to handle this responsibility, the process of which was also often partially automated. Smaller companies, unable to employ such a division, often outsourced this responsibility to other organizations specialized in content regulation (Borak, 2020).

In 2006, the first stage of the Golden Shield project was finished, as the project turned into its second phase (Chandel et al., 2019). Besides the blocking of specific domain names and IP addresses, the keyword-filtering system could now also analyze the traffic communicated through an internet connection, even through proxies, and automatically reset the Transmission Control Protocol if the connection contains sensitive words or phrases (Hounsel et al., 2018; J. Wu & Lam, 2017). The principles behind keyword filtering had first been introduced to China by the US company Cisco (Chandel et al., 2019), which had also delivered hardware for the Great Firewall earlier (Johnson & Katz, 2010; Stirland, 2008). Other parts of the system had been provided by Chinese companies such as Huawei (Herman, 2018).

Despite its improvements over time, the Great Firewall was not watertight. Several ways to circumvent the keyword filtering systems existed, such as encrypting connections through a virtual private network (VPN) (Callanan et al., 2010; Hal Roberts et al., 2011). Although the use of firewall circumvention tools decreased significantly between 2000 and 2010 (Griffiths, 2019), many Chinese still made use of

these tools (Mou et al., 2016). However, even though there were ways to circumvent the censorship apparatus, it was inconvenient and expensive enough to prevent the average Internet user from diverting to these tools. Additionally, due to an increasing amount of services inside the Great Firewall that fulfilled the same needs as the inaccessible international services, the need to circumvent the network restrictions was also small (Lobato, 2016). As such, despite these circumvention tools, the Great Firewall served its purpose of censoring information for the general public (M. E. Roberts, 2018).

In subsection 3.1.1, the contention between the liberal nature of the global Internet and the desire of the CCP and the State Council to maintain information censorship was discussed. In the end, the norms and values accompanying the Chinese information system prevailed, mainly due to the system building done by the Chinese central government. The Chinese government decided to design unique technological solutions, such as the Great Firewall, to adjust the Internet to accommodate censorship, and accompany these technological solutions with legal and organizational adjustments, such as requiring ID registration for Internet access, to preserve the Chinese momentum regarding information censorship. As we will see later in this thesis, the decision to opt for strong Internet censorship can be seen as a turning point that contributed significantly to the emergence of a separate cyberspace in China.

3.1.3 US tech companies expand into China

A few years after the introduction of the Internet in China, several multinational tech companies originating from the US started focusing more the Chinese market. These US companies already had a significant market share in the US-based market, as well as several other countries across the globe. Digital markets differ from most conventional markets in the sense that they tend to become "winner-takes-it-all" markets, and companies often acquire monopolistic positions as a consequence of network effects and lock-in effects (Kuchinke & Vidal, 2016; Van der Aalst et al., 2019). Due to these effects, early movers tend to win the race for the market (Shapiro & Varian, 1998). Furthermore, due to high fixed costs but negligible marginal costs, digital services can quickly scale up and expand (Rifkin, 2014). These characteristics helped major US tech companies to easily expand internationally, and they went on to expand their activities into China.

The period around the turn of the century was marked by economic liberalization in China and further integration with the global economic system, in part driven by the accession of China into the World Trade Organization in 2001 (Miao et al., 2018). As such, international companies were starting to get access to the Chinese domestic market, although it was still difficult for them to penetrate. One of the first US tech companies that pioneered into China was search engine Yahoo in 1999 (Decker, 2014), followed by Google in 2000 (Levy, 2011). However, despite venturing early into the Chinese market, these US companies' search engines were not able to dominate the market like they did in many other countries. Several local competitors arose, which were much better adjusted to Chinese local (digital) culture. One such firm was Baidu, which was established in 2001. One successful observation that Baidu made was the Chinese preference for online discussion boards. To fulfil this need, Baidu created a tool that allowed users to easily create a discussion group whenever they entered a search query, which was very popular with users. Another cultural difference that Baidu anticipated well was that in China, pirating music, movies, and software was fully accepted by the general public. Baidu created a user-friendly interface that allowed users to easily search and download pirated content, which is something that would be unthinkable for US-based search engines. While the American search engines generated more accurate search results, the Chinese firms were better adjusted to the local culture (Thompson, 2006). Although Google purchased shares of Baidu in 2004, thereby acquiring a minority stake (The Associated Press, 2004), both services remained

active in China. As such, the Chinese market stayed divided between local and international companies (Thompson, 2006).

However, local cultural preferences were not the only challenge that western companies faced. The Great Firewall project was steadily developing, and both Chinese and international companies providing internet services were expected to comply. However, following the illustrative case of Google, the company initially decided not to filter any search results (Griffiths, 2019). As a result, pages accessed through Google were often intentionally slowed down or made inaccessible by the censors, with page loading times often being seven times as slow as through its competitor Baidu (Donnelly et al., 2009). In 2002, the search engine was blocked completely for two weeks in China. Although spokespersons from the Chinese government denied any involvement in the matter (Knight, 2002), many commentators believed that this blocking was intentional (BBC News, 2002; The Guardian, 2002). In the time that Google's website was inaccessible, any traffic accessing Google was redirected to Baidu, which had good ties with the government (So & Westland, 2009). Many internet users also began using proxy servers outside China to gain access to Google (Knight, 2002). In December 2003, Google was once more blocked in China (Lau, 2010).

Other western companies decided to comply with the wishes of the censors. An example is Yahoo, which entered the Chinese market in 1999. The company initially offered an online directory, and only later created its own search engine. In the US, Yahoo faced fierce competition from newcomer Google, due to which its activities in China became relatively more important for the company. To maintain its position in China, Yahoo decided to adjust to the Chinese censorship norms, for instance by signing the 'Public Pledge on Self-Discipline for the Chinese Internet Industry' issued by the Internet Society of China. This pledge obliged signatories to self-censor information on its platforms, if this for instance harmed state security or social stability, or if it spread superstition or obscenity (Griffiths, 2019). In 2005, Yahoo paid $1 billion to acquire 40% of the shares of Chinese e-commerce company Alibaba (Rao, 2015). At the time, Alibaba owned the popular e-commerce platform Taobao, a consumer to consumer trading platform that dominated the Chinese market and was considered a competitor to the US company eBay (Ou & Davison, 2009). As part of the purchase deal, Yahoo transferred its Chinese activities to Alibaba, and the company would remain to be led by the eccentric Alibaba CEO Jack Ma (Barboza, 2005). Likewise, Google attracted Microsoft employee Kai-Fu Lee, who had also acquired a celebrity status in China, to lead its China division (Thompson, 2006).

As we saw from the examples of Google and Yahoo, US companies had varied approaches towards the censorship regulations in China. For US companies unwilling to commit to censorship practices, operating in China was difficult and put them at a disadvantage compared to local competitors that did comply with the censors. However, the unique preferences of Chinese Internet users also made it harder to dominate the market. These preferences, such as a desire to engage in online discussions or the acceptance (and legality) of pirated contents, led to a different selection environment for companies, in which local Chinese companies could also become successful. As a result, the market was divided between US and Chinese companies, and collaborations between US and Chinese companies were not uncommon.

3.1.4 Conclusion of Period 1

Combining the findings of the previous subchapters, several developments can be observed that make Chinese cyberspace clearly different from the US-based cyberspace. This brings us to the answering of the first subquestion of this thesis: *"Why and how did system builders in China develop an alternative Internet*

model?" Through the analysis in the previous subchapters, the gradual embedding of the Internet in Chinese society has been observed. As we saw in the first subsection, the early Internet, which originated from the US, contained strong momentum towards a free, liberal and deregulated system. This momentum conflicted with the momentum that was already incorporated in the information system in China, as the deep embeddedness of this system led to resistance against systematic change towards less information control. However, despite the fear for this liberal Internet, the Chinese State Council saw the Internet as a very promising means for economic growth. As such, Chinese governmental actors sought to integrate the Internet into the existing structures of Chinese society. Eventually, their system building activities ensured that the pre-existing norms and values present in China prevailed. An important element of this integration was the creation of the Great Firewall and the wider Golden Shield project, which combined technological, regulatory and organizational measures. Meanwhile, Chinese private companies were also shaping Chinese cyberspace in different ways than in other parts of the world. They did so by creating products and services that served local Chinese preferences better, examples being the facilitation of online discussion groups or of searching pirated content. The success of Chinese companies was further aided by the earlier system building efforts of the governmental actors, as some western companies became inaccessible in China due to them not complying with Chinese censorship regulations, resulting in less foreign competition in the Chinese market. As such, the strong censorship model in Chinese cyberspace led to a different selective environment for elements in cyberspace than in other parts of the world, leading to a distinct cyberspace in China. A schematic representation of the most important developments taking place during period 1 can be found in Figure 2.

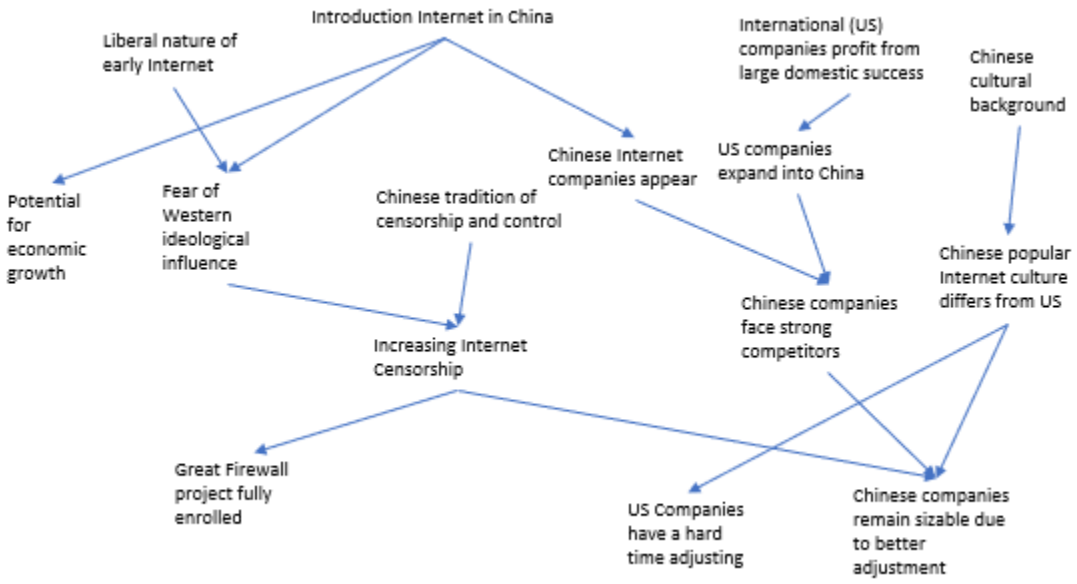


Figure 2: A schematic overview of the most important developments in period 1 and their consequences

This chapter has already shown some problems that US companies operating in China faced. However, as we will see in the next chapter, it would become increasingly difficult for companies to operate in both the US and China, as they increasingly found themselves in a difficult balancing act between pleasing Chinese and domestic actors.

3.2 Period 2 – A distinct Internet

In the last section, we saw why and how system builders in China constructed an alternative Internet model. As this section demonstrates, this Internet model led to an increasing divergence between Chinese cyberspace and the US-based cyberspace. As such, the subquestion that this section intends to answer is: *"Following the emergence of an alternative Internet model in China, how did Chinese cyberspace deviate further from the US-based cyberspace?"*. This section contains two subsection that follow each other. The first subsection discusses the complexities that US companies faced in dealing with Chinese censorship regulations, ultimately culminating in the decision of many US companies to leave the Chinese market. The second subchapter discusses how, due to the absence of US companies, Chinese companies were able to quickly grow and innovate.

3.2.1 US tech companies dealing with censorship

In early 2006, Google launched google.cn, a new version of its search engine specifically aimed at the Chinese market. In this version, politically sensitive or undesired topics could no longer be found (Dann & Haddow, 2008). While the Chinese language version of the uncensored google.com was still available, it was expected that the majority of users would use the censored version instead, given that the Great Firewall caused google.com to be inaccessible for 10% of the time, and slow when it was available (McLaughlin, 2006). With this new search engine, Google hoped to solve the disputes between themselves and the censors, and offer a faster search engine that would always be accessible (Watts, 2006). Google also sold its minority stake of Baidu, which had grown to control 50% of the search market in China (Thompson, 2006), to focus more on expanding its own business (BBC News, 2006).

To Google, it had become clear that the momentum of Chinese cyberspace towards censorship was too strong for them to attempt to offer uncensored services, and given the potential of the Chinese digital market, they made the decision to offer a censored version of its search engine. However, this decision caused a backlash in the US, which was still the most important market for Google. Domestic protests arose, and a Congressional hearing was called to discuss the actions of US tech companies in China (Thompson, 2006). The introduction of google.cn was not the sole reason for discontent in the US. Besides Google, the companies Yahoo, Microsoft and Cisco were also accused of contributing to Chinese censorship and doing business in China at the cost of human rights (Goldenberg, 2006). A few months earlier, several cases had gained negative publicity in which Yahoo aided the prosecution of Chinese dissidents by providing Chinese authorities personal information of Internet users advocating for political reform, which had led to the imprisonment of these dissidents (Auchard, 2007; Kahn, 2005). Alibaba CEO Ma, who had also been made responsible for Yahoo China, had responded by stating that complying with the Chinese censors was simply necessary to do business (Dickie, 2005). The US companies had argued earlier that they regretted contributing to censorship, but that their presence in China ultimately does more good than harm for Chinese citizens (McHugh, 2003), and this argument was repeated in the hearing (Dann & Haddow, 2008; Goldenberg, 2006). However, the congress did not agree with this view, and members of Congress called the collaboration between these companies and the Chinese government "sickening" (Zeller, 2006) and compared them to companies collaborating with Nazi Germany (Thompson, 2006). Yahoo argued that companies simply need to comply with the local laws in countries where they are active, and that lobbying for political prisoners was not the responsibility of companies but of the US government (Auchard, 2007).

The hearing illustrates the tensions between complying with the wishes of the Chinese censors and of the US Congress. While the hearing did not immediately lead to fundamental behavioral changes towards their business operations in China, they led to significant domestic reputation damage for the accused companies. Meanwhile, the increased collaboration with the censors did not result in the desired outcomes in China either. None of the major US tech companies was able to become dominant in the Chinese market, unlike most other places in the world. Despite large financial investments and takeovers of Chinese competitors, US companies like Google, eBay, Yahoo and Amazon remained smaller than their Chinese competitors Baidu, Alibaba, Sina, Sohu, and NetEase. For instance, in the search engine market, Baidu controlled 63% of the market, while Google controlled 19% and Yahoo 7.6% in 2007 (Barboza, 2007). While Google managed to grow a bit over time and was able to become the market leader in digital maps, mobile search and translation technology (Griffiths, 2019), its search engine would remain less popular than Baidu's (Waters et al., 2010). One of the reasons can be ascribed to poor cultural sensitivity. With the introduction of google.cn, Google translated its name to "Gu Ge", a cognate meaning "valley song" or "song of the harvest". Its intention was to choose a name without negative connotations (Levy, 2011). However, many Chinese Internet users perceived the name as being patronizing, as the newly established Chinese middle class did not wish to be associated with a farmer's life. A website called NoGuGe.com had collected thousands of signatures, requesting Google to change its name (Griffiths, 2019).

A second reason for Google's difficulties in becoming more popular was that China's problems with the censors were not solved either, despite the new censored google.cn. Google's search engine kept receiving criticisms by Chinese state media and internet watchdogs, and was slowed down or inaccessible on several occasions. After turning off specific functionalities of their search engines that led to these criticisms, such as associative-word algorithms, or after being more strict in their censorship of undesired content, their engine would become accessible again (Helft, 2009; Watts, 2009; Wong, 2009). Meanwhile, domestic and international criticisms on Google's censorship policy had not diminished (Brenkert, 2009; Donnelly et al., 2009). Furthermore, the popular head of Google China, Kai-Fu Lee, left the company in 2009 to start his own business (Helft, 2009).

In January 2010, Google decided to radically change its strategy in China. In a blogpost, Google's Senior Vice President David Drummond announced that the executive board of Google had reconsidered its approach to China, and would no longer censor search results in China. As reasons, he mentioned the increasing limitation of free speech in China (Drummond, 2010a). However, the trigger had been a highly sophisticated cyberattack originating from China that was discovered a month earlier, which had shocked the company due to its magnitude. The attackers had obtained access to Google's core infrastructure and were able to modify and copy source code (J. Tan & Tan, 2012), and had acquired terabytes of data (Griffiths, 2019). In the process, the Gmail accounts of Chinese human rights activists had been breached and intellectual property from Google had been stolen (Drummond, 2010a). Google Co-founder Sergey Brin later revealed that both the decision to launch the censored search engine in China and the decision to retract it had led to divisions within the executive board (Johnson & Katz, 2010; Vascellaro, 2010). Mentioning his own youth in the Soviet Union, he stated that he had personal objections to the "earmarks of totalitarianism" that he observed in some of China's policies. Brin also commented that the strict censorship policies of China were also emboldening other countries to create their own firewalls, which Google wished to avoid (Vascellaro, 2010).

As expected, the Chinese government replied that self-censorship was a non-negotiable legal requirement for operating in China (Johnson, 2010). Nonetheless, Google decided to terminate its censored search engine in China, while redirecting all traffic from google.cn to google.com.hk, the uncensored Hong

Kong version of its search engine. Google anticipated that this could well mean that access to its services would be blocked entirely in China (Drummond, 2010b). However, after its decision for redirecting all internet traffic, Google remained accessible, although the Great Firewall was still able to filter out most undesired content through its automatic keyword detection systems, similar to other foreign websites (BBC News, 2010). If sensitive search queries were detected, the connection would be reset (Johnson, 2010). Meanwhile, state media responded harshly to Google's decision, calling out Google's "groundless accusations towards the Chinese government of supporting hacker attacks", while also blaming the company for trying to impose its own values on China (Reuters, 2010). A government official from the State Council Information Office's Internet Bureau was disappointed that Google had "violated its written promise it made when entering the Chinese market by stopping filtering its searching service", and mentioned that "foreign companies must abide by Chinese laws and regulations when they operate in China" (Xinhua, 2010). For a few months, it remained unclear whether the redirection of Internet traffic would be accepted by the censors (Drummond, 2010c; K. Li, 2010). In the end, access to google.com.hk was not completely blocked, but many functionalities of Google had been restricted (J. Tan & Tan, 2012). As a result, users stopped using their search engine. By 2014, Google only had a market share of 0.34% (C. Li, 2015). While Google kept some offices open in China for research and development (Yeo, 2016), many senior Google employees in China moved to Chinese tech firms such as Baidu, Sohu, or Tencent instead (J. Tan & Tan, 2012). Only a few products of Google, such as its web browser Chrome, were not perceived as problematic in terms of censorship, and as such remained accessible. Despite the absence of its search engine, Google Chrome would remain the most popular web browser in China (Chiu, 2020).

The example of Google illustrates the difficult balancing that US companies had to face between complying with Chinese censorship rules in order to operate in China, and defending values of free speech to avoid domestic criticisms. Following its initial blockade in China, Google attempted complying with the censors instead. Still, it did not manage to become dominant in the Chinese market. In the end, Google concluded that operating in both the US and China was impossible, and as a result decided to terminate its activities in China. Several other successful US tech platforms, such as Twitter and Facebook, were likewise blocked in China (Branigan, 2009; Gibson, 2009). Although there are examples of Chinese companies simply outcompeting their US competitors due to a more attractive platform focused specifically on the Chinese market, such as Alibaba's Taobao outcompeting eBay (H. H. Wang, 2010), the demands of the censors in China played a large role in shaping the Chinese digital business landscape.

Analyzing the evolution of Chinese cyberspace as a multi-actor game, we can conceptualize the decision of Google to leave the Chinese market as a result of conflicting interests. The Chinese censors and Google's international audience had differing visions of how censorship in China should be treated. Google had both tried censoring and leaving the Internet uncensored in China, but found out that neither side would accept Google's actions unless it would fully opt for its own preferred approach. In the end, Google realized that the demands from both sides were indeed incompatible and decided to comply with the non-Chinese actors. As we will see in the next section, the departure of the US companies shifted the momentum in Chinese cyberspace, and caused Chinese tech companies to become true monopolists in their own market and further develop their own technological platforms.

3.2.2 Space for growth

For many Chinese tech firms, the departure of the US tech companies meant that they had lost wealthy and powerful competitors. As a result, these Chinese tech firms saw their market share further increase. At the

same time, the Chinese digital economy was still growing rapidly. By 2007, there were 162 million Internet users, and this number increased steadily over time (see Figure 3). By 2008, China had the largest number of Internet users in the world, and also in relative terms the number of people in China connected to the Internet had become higher than the world average (Liang & Lu, 2010). As such, the Chinese domestic market, now devoid of international competitors, provided Chinese tech companies with great potential for long-term unhindered growth while enjoying economies of scale (Jia & Winseck, 2018). Of these Chinese tech companies, three stood out in particular: Baidu, Alibaba and Tencent (often summarized as 'BAT'). Within a few years, these companies could be found among the top 10 Internet companies worldwide in terms of user population, Internet traffic, revenue and market capitalization (Jia & Winseck, 2018). Given their large market shares, they could each be considered monopolists in their respective sectors. Additionally, together these three companies acquired 75% of all successful Chinese tech startups (Xia & Fuchs, 2017).

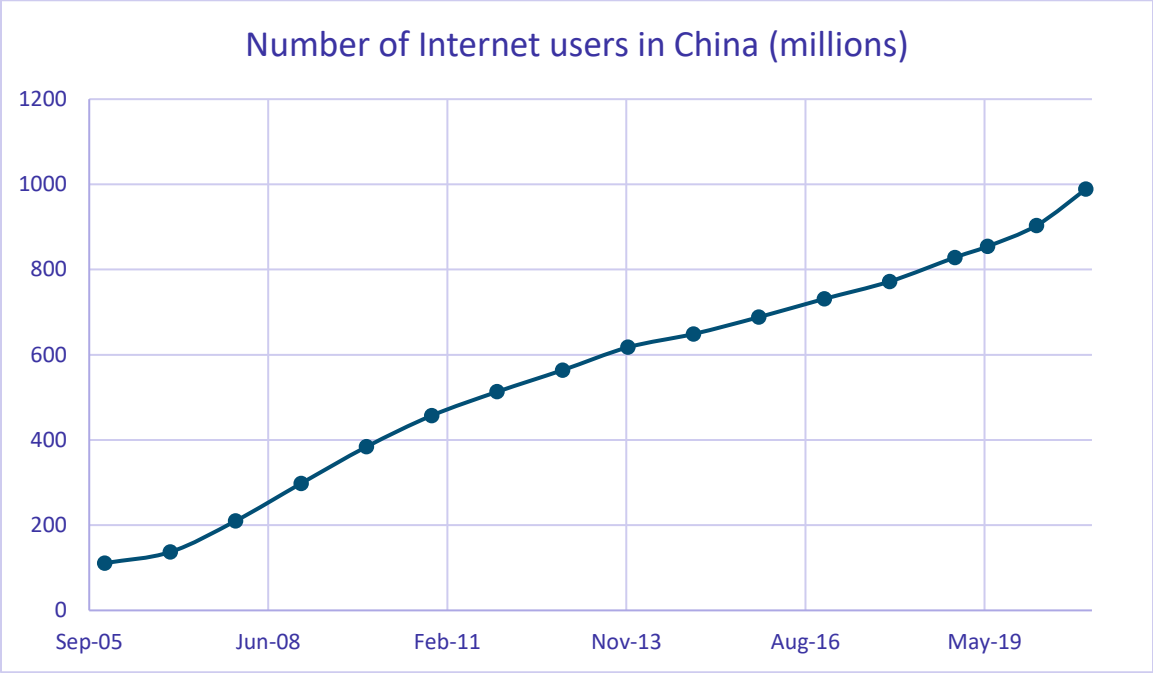


Figure 3: Number of Internet users in China between 2005 and 2020, in millions. Derived from (CNNIC, 2013, 2020)

Up until this point in time, the most prominent differences between the Chinese Internet and the Internet in other countries had been the extensive censorship apparatus and the fact that US tech companies had experienced significant difficulties to get a strong foothold. However, in terms of applications and functionality, the differences had been relatively small. This was about to change, however. The departure of the US tech companies had led to the Chinese tech companies rapidly growing. Once they had become dominant in their markets, however, they did not intend to slow down their growth, as they had acquired momentum towards further growth. As such, these companies began to innovate to achieve this growth through better and more diverse products and services. Although Chinese platforms are often compared to US-based counterparts in popular media (WeChat to WhatsApp, Weibo to Twitter, Baidu to Google, QQ to Facebook Messenger, Taobao to eBay, etc. (BBC News, 2017; Kist, 2015)), innovation by Chinese tech companies led to products and services that could not be found in the US or elsewhere in the world. These

new applications would significantly change the services that Chinese users could enjoy while using the Internet.

For instance, Tencent's platform WeChat is often compared to Facebook's WhatsApp, in the sense that it is a highly popular and widespread direct messaging app (Clover, 2016; Reddy et al., 2015; Wan et al., 2019). However, the functionality of WeChat is much broader than just messaging, and continues to increase. Nowadays, users can use the app to book transportation, pay utility bills, make movie or hotel reservations, check the availability of nearby doctors, read news articles, order food, play games, and make mobile payments, among others (Arnold, 2018; Z. Huang, 2017; Montag et al., 2018; Tu, 2016). It also serves as a platform hosting a wide variety of apps by external partners, and small businesses can offer their products in virtual online shops (Clover, 2016; Y. Yang, 2018). The strong diversification of WeChat was not exceptional, however. Around the same period, other Chinese companies saw a similar broadening of their activities. As Alibaba's CEO Jack Ma stated, he regards the company as a "data company", rather than "merely an e-commerce company" (Liyakasa, 2015).

These innovations were in part driven by the local Chinese context. As part of their system building efforts, Chinese tech companies saw the opportunity to solve problems that they observed in Chinese society. These problem-solving activities resulted in different products and services being available in Chinese cyberspace than in the US-based cyberspace. A good example is the popularity of mobile payment services. Traditionally, it had been very hard for many Chinese to gain access to banking credit due to the less developed Chinese banking sector (Bai et al., 2006; L. Lin et al., 2019). This traditional weakness created an opportunity for Chinese tech companies to innovate and develop a successful product to tackle this issue, and led to the creation of services like WeChat Pay and Alibaba's Alipay. Besides payments on digital platforms, they have also become the most common payment method in physical Chinese stores. By scanning QR codes with a mobile phone, users can easily make a payment. Rather than paying immediately, it is often possible to divide the payment over several months, thereby providing credit to the user (Arnold, 2018). Both companies also obtained banking licenses, meaning that they could start providing small-scale loans to private borrowers and smaller companies (Wildau, 2014, 2015). The phenomenon of providing digital solutions for less developed services can also be observed in other sectors. For instance, the Chinese business environment relies to a large extent on family businesses, together accounting for 85% of all private sector revenue (Ma, 2020). In contrast, in 2017, there was only one shopping mall for every 1.2 million inhabitants in China. This lack of physical shopping malls contributed heavily to the popularity of e-commerce firms, as it provided an easy way to access a large variety of goods (The Economist, 2017), while these smaller family businesses could use these digital platforms to serve a larger customer base.

Like their American competitors earlier, the new technological platforms created tensions with the Chinese censors. In 2009, microblogging site Sina Weibo was launched. Building on the long-standing popularity of discussion boards that had also given Baidu an edge over Google earlier, it quickly became highly popular (S. Chen et al., 2011). Whereas Twitter had been blocked in China in August 2009 by the censors (Branigan, 2009), Weibo, which had an automated rumor-detection service (F. Yang et al., 2012), was allowed to operate. From a statistical experiment, it was found that approximately 16.25% of all Weibo messages were censored after posting (Bamman et al., 2012). Nonetheless, Weibo was a means for users to express themselves freely within legal boundaries (Lixuan Zhang & Pentina, 2012), and due to the possibility for opinion leaders to stimulate societal discussions, the platform began to play a large role in Chinese civil society (Tu, 2016). However, shortly after the accession of the Xi Jinping government in 2013, Chinese government officials stated that popularity of social media led to widespread "irresponsible rumors". These rumors included false information that could lead to protests, unrest, defamation or a

negative image abroad (Kaiman, 2013; Lubman, 2013). New legislation was introduced to combat these rumors. Any message that was marked as a rumor and that was either visited over 5,000 times or reposted over 500 times could lead to a charge with defamation. Such a charge could lead to a sentence of up to three years of imprisonment (BBC News, 2013b). The legislation was met with concerns by Weibo users about the limitation of freedom of speech, who also expressed that the threshold of 5,000 views or 500 reposts was so low that no one would dare expressing their opinion anymore. However, government officials argued that the increase of strange stories online justified the legislation (Blanchard et al., 2013). Additionally, other regulations required users to use their real names when registering to Weibo (Zeng et al., 2017). The increased censorship was one of the reasons why many Chinese users drifted to WeChat, where messages were much harder to censor due to being designed around peer-to-peer communication (K. Lee & Ho, 2014; Tu, 2016). Nonetheless, also on WeChat 2.1 million messages were deleted daily in 2015 (T. Chen, 2015).

The tightening of undesirable information on social media shows that both Chinese and US companies experienced challenges in dealing with Chinese censorship norms while remaining attractive to its users. However, a key difference was that the US companies had to seek a compromise between the Chinese censors and their international audience, whereas Weibo did not face the same repercussions in complying with Chinese law. As such, while the US companies made the decision to leave the Chinese market, Weibo could remain active. Although its popularity declined after the regulatory restrictions described above, it maintained a sizable user base and continued to play an important role in Chinese civil society as a platform for discussion (Tu, 2016). Its societal importance was underscored by the fact that state media and many (local) government agencies also became more active on Weibo (as well as other social media) where they actively engage in discussions (Schlæger & Jiang, 2014). The purpose for this was twofold, as they both attempted to communicate government opinions and monitor the public opinion (G. Yang, 2014). As such, not only was Weibo accepted by the Chinese censors and the government, but it was also embraced as an important part of Chinese cyberspace.

As we saw here, the departure of US companies created space for Chinese companies to grow, innovate and diversify. Profiting from the large domestic market, the departure of the US companies allowed Chinese companies to monopolize the market. As the Chinese companies did not face any repercussions outside China for complying with the censors, they did not face the same hindrances as the US companies did. Profiting from the zero marginal cost characteristic of digital markets (Rifkin, 2014), these companies grew easily, and used their strong position and their acquired momentum to take over promising start-ups and to diversify its services across a wide range of sectors and functions.

3.2.3 Conclusion of Period 2

The second section of the findings was aimed at answering the following question: *"Following the emergence of an alternative Internet model in China, how did Chinese cyberspace deviate further from the US-based cyberspace?"* During this studied period, a clear increase in differences between Chinese cyberspace and the US-based cyberspace could be observed. This divergence started with the departure of most large US-based companies from China. As illustrated through the example of Google, despite their best efforts, many US companies had difficulties combining the Chinese expectations regarding information censorship with domestic expectations to promote liberal values abroad. In the end, these companies found that it was impossible to choose a middle ground between these pressures, and as such decided to leave the Chinese market. However, the different Chinese preferences also played a role, as companies like eBay were simply outcompeted by their Chinese competitors. Nonetheless, the absence of the US tech companies

that defined the Internet across the globe meant that in China, space had been created for a different business environment. Chinese tech companies filled the space in the market that the US companies had occupied earlier, and used the acquired momentum to innovate and diversify their products. In these system building efforts, the Chinese tech companies sought solutions to problems that were specific to China, such as the less developed banking sector and the reliance on small-scale shops, which to a large degree shaped the products and services that these companies provided. As such, the products and services available in Chinese cyberspace differed significantly from those available in the US-based cyberspace. Meanwhile, censorship in Chinese cyberspace was tightened further, as exemplified by the legislation against digital rumors. An schematic overview of the developments of period 2, and how they are related to the developments in period 1, can be found in Figure 4. The red line indicates the beginning of period 2.

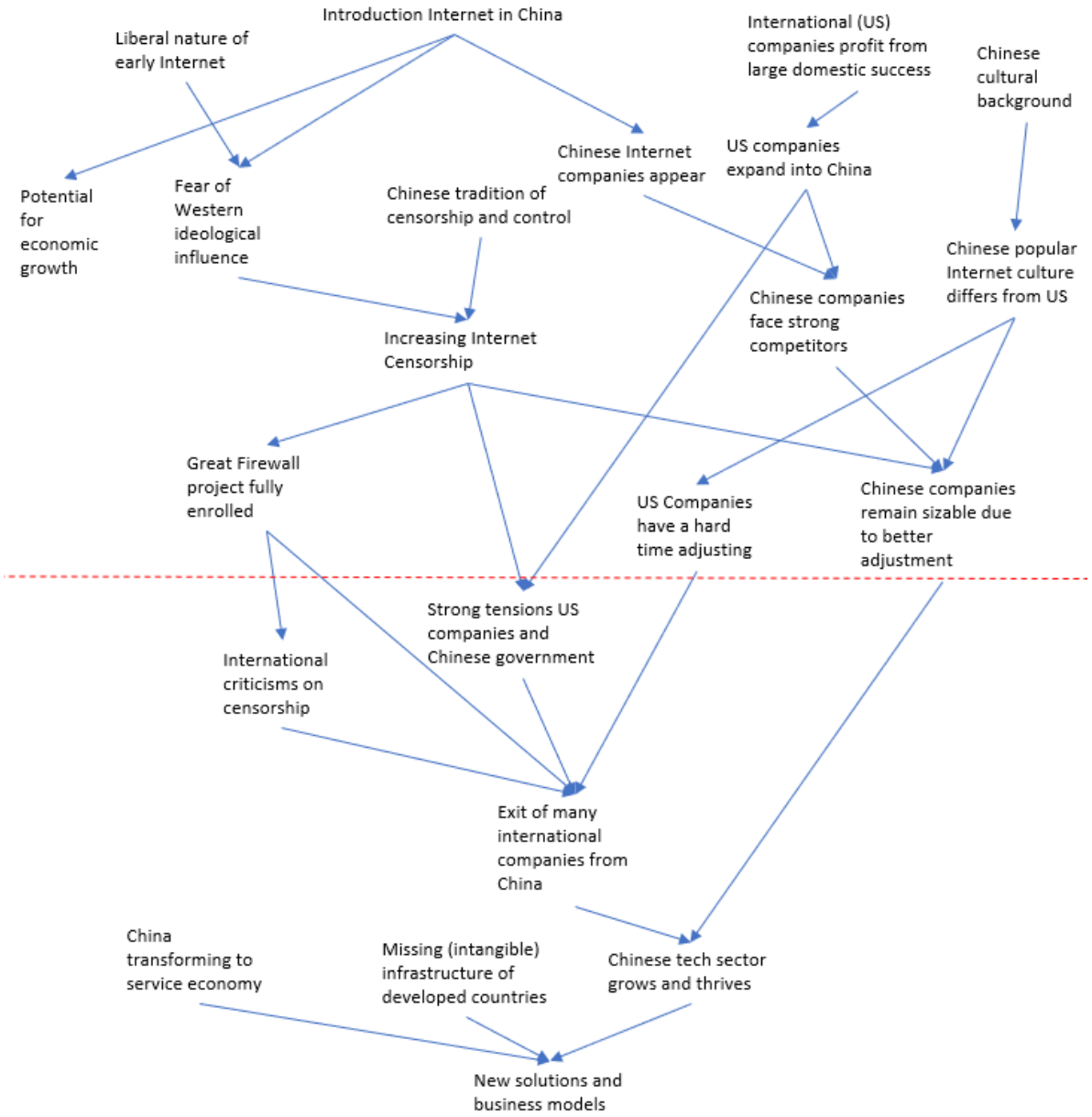


Figure 4: A schematic overview of the most important developments in periods 1 and 2, and their consequences

All in all, these developments show how Chinese cyberspace deviated further from the US-based cyberspace. However, as we will see in the next chapter, actors in Chinese cyberspace began to look outwards and the interaction between the two systems began to increase, having an influence on both systems.

3.3 Period 3 - Outward expansion

In the last section, we saw how the departure of US firms in China lead to the growth of Chinese tech companies, as they established dominance over their domestic market. Due to this large domestic market, the Chinese tech companies enjoyed economies of scale, and as such were able to further improve and develop their products. Due to this domestic success and the acquired momentum, not only did their products over time become advanced enough to be considered of similar quality to the products of the US companies. Due to saturation of the Chinese market and strengthened by the momentum towards growth of the Chinese companies, the Chinese tech companies began looking outward to continue their growth. This section mainly focuses on this outward expansion, and how this was shaped by, and in turn shaped, Chinese cyberspace. The first subsection analyzes why and how Chinese digital companies expanded abroad, while the second subsection focuses on the responses that this expansion provoked abroad. As we will see in the third subsection, the outward expansion of Chinese cyberspace did not only take place through the expansion of Chinese companies, but also in various immaterial ways. As such, the interaction between the Chinese and the US-based cyberspace is the main focus of this section. This section ends with an answer to the third subquestion: *"How did Chinese cyberspace collide with the US-based cyberspace, and how did the resulting interaction and contestation shape both cyberspaces?"*.

3.3.1 Economic expansion abroad

In 2013, Xi Jinping was elected as president of China, after having become general secretary of the Chinese Communist Party in late 2012 (Branigan, 2013; Wong, 2012). As we will see in the following paragraphs, the Xi administration took a much more proactive approach in shaping Chinese cyberspace than previous governments had done. During the 2010s, China was gradually turning from an industrial economy into a service economy (Bajpai, 2020). To maintain the high levels of economic growth achieved during the last decades, the Chinese State Council wished to embrace and foster this economic transition. One of the pillars for this transition would be further digitalization, thereby becoming a global leader in high-tech manufacturing and digital services.

During this period, cyberspace policy was heavily consolidated and centralized, thereby eliminating competition between the various government branches involved with Internet regulation and streamlining decision-making processes. President Xi commented that these overlapping responsibilities were causing "obvious problems" regarding China's Internet governance, which he described as "directly relating to national ideology security and regime security". As such, effective Internet regulation had high priority (Miao & Lei, 2016). Already in 2011, the State Internet Information Office had been established, which was made responsible for all forms of content regulation on the Internet (Shen, 2016; Wines, 2011). The prominence of cyberspace in the policy of the State Council was further amplified by the establishment of the Cyberspace Administration of China (CAC) in February 2014. The CAC was a high-level body, whose main responsibility was to bring order to Chinese cyber regulation (Y. Hong, 2017a), ranging from ensuring cybersecurity to fostering digitalization and economic growth. The central position of the CAC in the

Chinese government was underscored by its composition: it was chaired by President Xi Jinping, Premier Li Keqiang served as its vice-chair, and was further comprised of a large number of members of the State Council whose ministries had a relation to the Internet (Miao & Lei, 2016).

Following the establishment of the CAC, the State Council formulated a series of policy plans that aimed to strengthen the digital ecosystem. In 2015, Premier Li announced the 'Internet Plus' strategy. The plan aimed to "integrate the mobile Internet, cloud computing, big data, and the Internet of Things with modern manufacturing, to encourage the healthy development of e-commerce, industrial networks, and Internet banking, and to guide Internet-based companies to increase their presence in the international market" (State Council, 2015a). In other words, the plan aimed to increase connections between various sectors and different digital technologies throughout the economy. In the same year, the State Council announced the 'Made in China 2025' strategy, setting out how China could become a global leader in high-tech manufacturing (Wübbeke et al., 2016). Likewise, in 2017, the State Council introduced the AI Development Plan, setting out how China could become the global innovation center for AI by 2030 (Department of International Cooperation of the Ministry of Science and Technology, 2017).

In all these plans, the State Council took on a top-down coordinating role. Rather than as detailed policy plans, the plans served to set out the general direction that the Chinese digital ecosystem should develop towards, as is common in Chinese policy plans (see the discussion in section 2.2.3). The detailing and the execution was left to other actors, such as large companies, startups, and local governments, who were explicitly encouraged to take on an active role (Huw Roberts et al., 2021). The coordinating role of the State Council can also be noticed in its decision to establish a team of 'national AI champions' as part of its AI policy. These AI champions were private companies that were designated to each become a global leader within a specific AI domain (see Table 1). While many of these companies already held a leading position in their respective fields prior to this designation (Barrett, 2020), again the State Council provides direction in their development. Furthermore, as Shen (2016) described, while these policy plans were presented by the State Council, they also incorporated ideas from major Chinese businesses, who were consulted before the publication of these plans. As such, Shen argued, rather than solely as state policy, these policy plans should be regarded as the result of complex state-business interactions that took place during the formation of the plans. Nonetheless, scrutinizing the coordinating role of the State Council, which is dividing responsibilities and setting out a direction for development, it becomes clear that the Xi administration should be considered an important system builder in Chinese cyberspace.

Table 1: Chinese national AI champions and their respective domains. Derived from (S. Dai, 2019; S. Dai & Tao, 2019; Jing, 2018; Jing & Dai, 2017; Wernberg-Tougaard, 2021)

Company	**AI Domain**
Baidu	Autonomous Driving
Alibaba Group Holding	Smart Cities
Tencent Holdings	Medical Imaging
iFlyTek	Speech Recognition and Smart Audio
SenseTime	Intelligent Vision
Huawei	Infrastructure and Software
Hikvision	Video Perception
Xiaomi Corp	Smart Home Ware
JD.com	Smart Supply Chain
Qihoo 360 Technology	Cybersecurity

Megvii	Image Perception
Yitu	Image Computing
MiningLamp	Smart Marketing
TAL Education Group	Smart Education
Ping an Good Doctor	Inclusive Finance

Regarding the goals formulated by the State Council in these policy plans, an interesting duality can be observed. On the one hand, the plans were aimed at fostering further growth of the Chinese digital economy, which was becoming an increasingly important component of the Chinese economy (Longmei Zhang & Chen, 2019). On the other hand, each of the plans contained active support for Chinese tech companies expanding their activities abroad. The formulation of the latter reflects the growth that Chinese cyberspace had experienced over the years, with Premier Li stating that in terms of the digital economy, China was now on equal footing with the most advanced countries, or even leading in some aspects (State Council, 2015b). The formulated internal and external goals of the respective policy plans are listed in Table 2.

Table 2: Digital Policy plans by the State Council, and their internal and external goals. Derived from (Huw Roberts et al., 2021; State Council, 2015a; Wübbeke et al., 2016)

Policy	**Internal goals**	**External goals**
Internet Plus	Integrate a wide range of digital technologies across the economy to foster economic growth	Increase international presence of Chinese Internet-based companies
Made in China 2025	Create an innovative Chinese high-tech manufacturing economy to become more self-reliant	Increase exports of Chinese high-tech manufacturing and increase acquisitions abroad
AI Development Plan	Capitalize on the economic and societal promises that AI brings	Define global ethical norms and standards for AI

This focus on outward expansion of the Chinese cybersphere took place during a period in which economic ties between China and the rest of the world were growing in general. In 2013, President Xi had announced the Belt and Road Initiative (BRI), which through extensive infrastructure investments aimed to established firmer and more durable trade connections between China and other countries in Asia, Africa and Europe, akin to the ancient silk roads (Ferdinand, 2016; Y. Huang, 2016). Besides physical infrastructure, the plans also involve digital infrastructure and smart city development, and a digital ecosystem is being built in which Chinese telecom equipment, smart city sensors and data platforms are being exported (Kozłowski, 2018; Wheeler, 2020). The construction of a digital silk road was also discussed in China's 13th Five-Year Plan (2016-2020) (Y. Hong, 2017b). Although the Belt and Road Initiative is sometimes perceived as an umbrella concept, meaning that it is often unclear whether plans are a direct result of the BRI or whether they would have taken place anyway and are simply added to the broad BRI umbrella (Schlenzig, 2020), its inclusion in the Five-Year Plan indicates the importance of digital expansion abroad for the government. This digital expansion serves a wide range of economic and political goals, including the mitigation of domestic economic overcapacity by exporting products and services, the growth of Chinese firms through global expansion, the strengthening of the position of the renminbi as an international currency, the

construction of transnational network infrastructure centered around China, and the promotion of inclusive globalization (Shen, 2018).

During the 15th Forum on Internet Media of China in 2015, an annual event in which representatives of ICT companies, media, government departments, Internet investment institutions and city officials gather to exchange knowledge and discuss topics regarding cyberspace, the deputy chief of the CAC urged digital businesses to take on a leading role in building the digital dimension of the BRI by expanding their e-commerce, industrial and digital banking activities abroad (He, 2015; H. Zhao, 2015). Again, we see the same pattern as with the policy plans discussed earlier, where the Chinese central government encourages foreign expansion of private companies. Chinese companies responded positively to the plan and actively participated in the BRI. Already before the launch of the BRI, companies like Huawei and ZTE were building physical telecommunications infrastructure, connecting China to other parts of Eurasia (Rolland, 2015). They would also become important actors in the digital BRI. ZTE's Chief Innovation and Chief Strategy Officer Chen Jie said that ZTE was ready to play a leading role in building an "information superhighway" and added that the company was already active in 50 of the 64 countries then participating in the BRI. Its focus would especially be on 5G and smart city technologies (Soo, 2016). In terms of e-commerce, Chinese companies were also successfully expanding abroad. Online retailer JD.com planned to open over 20 new warehouses outside of China, thereby profiting from new railway networks constructed through the BRI, and enabling smaller Chinese companies to sell their products abroad more effectively (Yongrong Chen & Liu, 2017). Likewise, Alibaba's Jack Ma stated that the most important regions for expansion for his company were those included in the BRI, which generally were heavily populated but contained poor infrastructure, and as such provided ample space for growth (TASS, 2016). Ma also endorsed the view that the new silk road should also become an e-road (Jaipragas, 2017). At a G20 summit, Ma advocated for the creation of a global digital network that would for an "electronic world trade platform" (T. Zhang, 2016), the intention of which was to facilitate cross-border electronic trade by harmonizing global regulations, standards and taxation (eWTP, n.d.). The plan was endorsed by the G20 (The Economist, 2017).

Not all plans of Chinese companies for expansion abroad succeeded. Tencent had attempted to introduce WeChat in Europe, hiring Football World Player of the Year Lionel Messi for television advertisements (Lukman, 2013). However, it did not manage to successfully compete with Facebook and WhatsApp, who had already established large user networks in Europe (The Economist, 2017). Nevertheless, overall, the presence of Chinese tech companies in global markets had grown significantly. In terms of telecom equipment, Huawei had by far become the largest manufacturer in the world, with ZTE also being among the largest ones (TelecomLead, 2018). By the end of 2020, 7 of the 10 largest smartphone brands worldwide were Chinese (Gadgets Now, 2020). Especially in markets of developing countries, such as Brazil, Indonesia, India, and many countries in Africa, Chinese tech companies are involved in fierce competitions with their US counterparts (O'Hara & Hall, 2018).

In this subsection, we analyzed how Chinese companies went from being active in China alone to becoming transnationally active. As we saw earlier, the departure of US tech companies created the conditions for Chinese tech companies to grow and innovate. This rapid growth of these companies changed the mindset of actors in China. They began to see their tech products as being of at least equal quality as western products, as can be derived from the statements by Premier Li, but also from the ambitions of becoming a global digital leader, which can be identified in the State Council's policy plans. The rapid domestic growth of tech companies also provided these companies the scale required to become competitive in US-dominated markets (as discussed earlier, economies of scale are very important for success in digital

markets). Hence, we can argue that the change in mindset among Chinese actors and the rapid growth of the previous years generated momentum towards further expansion, which had to be sought abroad. Several actors can be identified that through their system building efforts considerably propelled and shaped this international expansion. Since taking office, President Xi Jinping and his administration have actively pushed for a stronger and more coordinated digital sector. In this effort, the Xi administration became an important system builder, bringing together other actors and incentivizing them to fulfill specific tasks and functions within Chinese cyberspace. The policy plans of the Xi administration also promoted a clear vision for Chinese cyberspace, harnessing its momentum and providing direction for its future development. At the same time, the role of private tech companies as system builders should not be underestimated. Through the exploration of proposals such as the electronic world trade platform and by proactively taking part in the BRI, these companies pioneered the possibilities of foreign expansion and actively sought to shape ecosystems abroad. As we will see in the next subsection, the expansion of Chinese cyberspace would eventually lead to strong contention abroad, breaking the system momentum and forcing actors in Chinese cyberspace to reconsider their plans.

3.3.2 International security concerns

After a long period of rapid growth of Chinese tech companies, resulting in their expansion abroad, their growth was halted towards the end of the 2010s. Around this time, China was engaged in a trade war with the United States. The US government believed this trade war was justified due to three major concerns it had. First, due to a negative trade balance with China, the US was losing jobs and employment opportunities. Second, the US government was concerned that Chinese companies were illegally acquiring technology and intellectual property, and sought to stop this. Third, there were fears that China posed a threat to the national security of the US, and as such technological cooperation needed to be decreased (Liu & Woo, 2018). Especially the second and the third concerns had strong connections to Chinese cyberspace. For years, Huawei had on multiple occasions been accused of reverse engineering, theft and espionage by US companies such as Cisco and network operator T-Mobile (Mascitelli & Chung, 2019; Yep et al., 2019), while security concerns about telecommunication hardware from Huawei had also been present for a longer time already (Inkster, 2019). Although Huawei repeatedly denied all accusations (BBC News, 2013a; Kharpal, 2019; Pinchuk, 2012), the US government remained highly skeptical, arguing that the close ties of Huawei to the Chinese government and the important position that it had acquired in telecommunications hardware created a threat in itself (Volz & Chin, 2019), given that Chinese companies are required by law to store private data and share it with Chinese governmental actors if asked (Y. Yang & Liu, 2018).

In February 2018, the directors of the CIA, FBI and NSA advised the US Senate against using phones and telecom equipment from Huawei and ZTE, due to cybersecurity concerns. The directors stated that they feared espionage or theft from their networks (Salinas, 2018; Van Boom, 2018). In June, the US Congress raised concerns about ties of US tech companies with Chinese companies, and requested Facebook and Google to stop sharing data with Huawei and mobile phone developer Xiaomi (Musil, 2018; Nieva, 2018). The US State Department adopted all aforementioned advices. However, while these decisions made it harder for these Chinese tech companies to expand into the US, their problems did not end there. Besides domestic restrictions, the US State Department also began to try to convince and persuade other countries not to include technology of Huawei and ZTE in their future 5G networks. If other countries allowed Chinese equipment into their networks, the State Department warned, then that would result in reduced intelligence cooperation with the US in the future (Emmott, 2019; Pancevski & Germano,

2019; Petty et al., 2019). Meanwhile, the Chinese ambassador to Canada announced that banning Huawei from contributing to its 5G network would lead to unspecified repercussions (T. Smith, 2019), while the Chinese ambassador to the United Kingdom said that it would send a bad message and affect trade and investment (Keane, 2019). While some countries, like Germany (which was threatened earlier by the US that allowing Huawei to contribute to its network would lead to less security collaboration), did not forbid individual vendors from contributing to its 5G network outright, it did raise additional security standards (Nicola, 2019), which was sufficient for the US government (Schuller, 2019). In May 2019, US President Donald Trump issued a formal ban against installing telecom equipment from abroad that "posed an unacceptable risk", a very general clause that effectively banned Huawei and ZTE from implementing their technology in the US 5G network (Kang & Sanger, 2019). A few days later, Google announced that it had decided that Huawei's smartphones were no longer allowed to use Google's Android operating system, its app store, or its apps (Moon, 2019), forcing Huawei to develop its own operating system instead (BBC News, 2019a). Later, US suppliers were also banned from delivering supplies to Huawei (Freifeld & Alper, 2021).

The US was not the first country to ban Huawei and ZTE over cybersecurity concerns. Australia, New Zealand and Japan had already excluded the companies from their telecommunication networks (BBC News, 2018; Jolly, 2018; Shida & Takemoto, 2018). Following the US ban, the UK also decided not to allow any new Huawei equipment in its 5G network anymore, while phasing out existing equipment by 2027 (PA Media, 2020; Sabbagh & Kuo, 2020). Likewise, the European Commission announced that it would not allow equipment of "high risk vendors" in the core parts of its 5G networks (European Commission, 2020). Canada effectively blocked Huawei by postponing the decision whether their equipment could be implemented, thereby offering other 5G suppliers the chance to implement the network instead (Ljunggren, 2020). According to Indian government officials, the country is also likely to ban Huawei equipment in the near future (Ahmed & Phartiyal, 2021). These examples show that the international resistance against these Chinese telecom providers was widespread. On the other hand, multiple other large countries, such as Russia and Brazil, still allowed Huawei to build their 5G networks (BBC News, 2019b; Reuters, 2021). Despite the international setbacks, Huawei and ZTE remain very important actors globally, together controlling 48.9% of the global 5G telecom equipment market in July 2020 (P. Zhang, 2020).

Following the prohibition of Chinese telecom equipment, the international resistance against elements of Chinese cyberspace increased further. In April 2020, US Secretary of State Mike Pompeo launched the Clean Path Initiative, followed by the Clean Network in August (Pompeo, 2020a, 2020b). This initiative was presented as a means to provide a secure digital environment for US citizens and companies, explicitly referring to "aggressive intrusions by malign actors, such as the Chinese Communist Party". In addition, the plan also explicitly referred to multiple large Chinese companies, such as Huawei, ZTE, Alibaba, Baidu, China Mobile, China Telecom, and Tencent as companies that should not be collaborated with (US Department of State, n.d.). The program aimed to provide a network completely devoid of components or software provided by Chinese companies. This included apps in app stores or pre-installed on smartphones, international telecommunications services, cloud storage, undersea cables, and transmission, control, computing, or storage equipment. In other words, the plans covered almost the entirety of cyberspace, intending to keep Chinese influences out. While Chinese companies were categorically excluded, non-Chinese companies providing these network elements were required to adhere to a set of internationally established standards (Pompeo, 2020b; US Department of State, n.d.). Pompeo

sent out an open invitation to other countries and companies to join the initiative (Layton, 2020). By the end of 2020, the initiative contained 53 countries and 180 telecommunications companies (Hartman, 2020).

In August 2020, President Trump signed two executive orders that demanded that the Chinese social media platforms TikTok and WeChat would be sold to non-Chinese owners, or else US companies and citizens would be "prohibited of carrying out transactions" with these companies (Carvajal & Kelly, 2020) While the vague wording of the executive orders made it unclear what exactly the consequences for the companies would be, its message was clear in that these Chinese companies would face significant difficulties in their future operations (Swanson, 2020). Although both executive orders were ultimately rejected in court cases (Allyn, 2020; Shepardson, 2020) and the succeeding administration of US President Joe Biden distanced itself from the bans of WeChat and Tiktok (Arbel, 2021), the political tensions involving Chinese companies are at the time of writing this thesis far from being solved, as illustrated by the continuation of excluding Huawei and ZTE from telecom networks (Shepardson, 2021). However, despite the Clean Network initiative, the international position of Huawei and ZTE remained strong on a global scale, with for instance Huawei equipment being used in two-thirds of all 5G networks worldwide (Segal, 2020).

In this subsection, we studied the backlash that Chinese companies faced during their international expansion. An interesting observation is that the US State Department not only excluded Chinese technology from its own country, but also urged other countries to do the same. An explanation for this can be found in the nature of the US-based cyberspace. Unlike Chinese cyberspace, it is not geographically limited to the US alone, but forms a sociotechnical system spanning most of the globe. As such, to keep its cybersphere completely free of Chinese technology, it did not suffice to only exclude it from the US, but it would need to be excluded from other countries as well. The US State Department here acted as an important system builder in the US-based cyberspace by attempting to exclude Chinese companies from the entire system. As in any sociotechnical system, both the reasons and the consequences of specific developments are often complex and multi-faceted. Although officially cybersecurity and the loss of intellectual property were cited as the main reasons for exclusion of Chinese technology, the exclusion of Chinese companies also resulted in US companies enjoying decreased competition from Chinese competitors (J. Wang, 2020). As such, the exclusion of Chinese tech companies was beneficial to US tech companies (Mascitelli & Chung, 2019), similarly to how the departure of US companies following disagreements with the Chinese government benefited Chinese tech companies a decade earlier. As such, we can observe an interesting parallel, where both in Chinese cyberspace and in the US-based cyberspace elements of each other's system that were deemed undesirable by important actors were excluded. However, as we will see in the next and final subsection, the growing international presence of Chinese cyberspace did not only occur through foreign expansion of Chinese companies. Chinese actors were also becoming much more important in international Internet governance and digital standardization, which both served to increase the International outreach of the Chinese ideal of 'cyber sovereignty'.

3.3.3 Cyber sovereignty

Besides through economic expansion, the growing importance of China in the global Internet system could also be noticed in the governance of the global Internet (Arsène, 2012; Negro, 2020; Shen, 2016). Global Internet governance has traditionally been heavily influenced by the western conceptualization of openness and liberalism that accompanied the early Internet (as discussed in subsection 3.1.1). This western conceptualization is for example reflected in the multi-stakeholder model that is prevalent in Internet

governance, in which non-profit organizations, private companies and technological experts all hold considerable influence. Due to the dominance of the US in global cyberspace, these western values have spread without much resistance and become nearly universal in global cyberspace (Demchak, 2016; Dutton & Peltu, 2008). However, the Chinese government promotes a different vision on the ideal way cyberspace should be governed. This Chinese vision is centered around the notion of 'cyber sovereignty'. President Xi Jinping summarized the core principle during his address at the 2015 World Internet Conference (WIC) (Ministry of Foreign Affairs of the People's Republic of China, 2015):

> *"We should respect the right of individual countries to independently choose their own path of cyber development, model of cyber regulation and Internet public policies, and participate in international cyberspace governance on an equal footing. No country should pursue cyber hegemony, interfere in other countries' internal affairs or engage in, connive at or support cyber activities that undermine other countries' national security."*

Although the idea behind cyber sovereignty has a long history in the Chinese conception of the Internet, the concept was increasingly promoted under the leadership of President Xi Jinping (Zeng et al., 2017) and during this period became a regular topic in policy documents involving cyberspace (Creemers, 2020b). In addition, the technological tensions with the US (as discussed in the previous subchapter) further increased the perceived need for a more autonomous cyberspace (Creemers, 2020a). The concept 'cyber sovereignty' is not strictly defined, however, and even within China there is still debate about what the term exactly entails (Creemers, 2020b; Zeng et al., 2017). This again reflects the evolving nature of policy plans that can be identified more often in China (Creemers, 2020b). However, despite the unclarity of the term, it is clear that the notion of cyber sovereignty embodies an alternative view on the role that individual states play regarding the regulation and governance of cyberspace. A core belief encompassed in the notion of cyber sovereignty is that a nation's cyberspace falls directly under the authority of its national government. Governments should be sovereign in their decisions, meaning that no other country, nor a non-state actor, has the authority to overrule decisions of national governments.

The advocation of cyber sovereignty implies a change from the status quo. By technological and institutional design, the Internet is heavily US-centric. An example is the geographical distribution of the thirteen DNS root servers. Together, these root servers administer the Domain Name System (DNS), meaning that they are responsible for the administration and allocation of all top-level domain names, such as the ones ending with *.com, .org* or *.net*. Due to a technical limitation of the Internet protocols that were used during the early years of the World Wide Web, only thirteen of such root servers could be assigned. Out of these thirteen, ten were administered by organizations from the US, while the remaining three were administered by organizations from Europe or Japan. (IANA, n.d.; ITU, n.d.). Moreover, the American non-profit organization ICANN, which also administered a root server, was responsible for the governance and management of the DNS (Palladino & Santaniello, 2021; Weitzenboeck, 2014). However, ICANN was formally accountable to the US Department of Commerce (Shen, 2016; Traynor, 2014), meaning that the US government ultimately held significant control over this core element of global Internet infrastructure.

This unequal geographic distribution had concerned other countries for a long time. Already throughout the 00s, China and several other countries from the Global South had consistently pushed for a more internationalized global Internet governance (Bhuijan, 2010; Mueller, 2012; Shen, 2016). The reason

for this internationalization was not only due to political concerns. Following an earthquake in Taiwan in December 2006, eleven submarine Internet cables were damaged (Global Times, 2009). As a result, over 90% of all international Internet traffic to China was disrupted (W. Qiu, 2011), and it took a month before Internet access in China had been fully restored (Global Times, 2009). The main problem with this outage was that since all DNS root servers were located outside of China, China was heavily dependent on these international cable connections, making it vulnerable to outside disturbances (Sahari, 2017). Around this time, more than half of all Chinese websites had a *.com*, *.org* or *.net* registration, which all fell under the DNS system (Ning, 2007). An alternative was already available, however. Websites with *.cn* domain names effectively fell under the control of the state-owned non-profit China Internet Network Information Center (CNNIC) (C. R. Hughes & Ermert, 2003). Partially due to ICANN's slow implementation of domain name support for Chinese characters, but also partially because of concerns about the powerful position of ICANN, the CNNIC had essentially created its own DNS root for Chinese-character domain names. To keep this system compatible with the global DNS system, the ICANN domain name for China, *.cn*, would automatically be added to queries from outside China (Mueller, 2011). To further reduce Chinese reliance on the DNS system, the CNNIC decided to drastically reduce the price of *.cn* domain names from 300 yuan to 1 yuan per year. The Ministry of Information Industry supported the CNNIC in this effort (Ning, 2007). The plan had paid off, as within a year the number of *.cn* domain names had increased from 1.8 million to 8.45 million registrations (Shen, 2016).

ICANN continued to play an important role in global Internet governance. Concerns about the dominant position of the US in the global Internet governance structure were later amplified by the revelations by Edward Snowden about the PRISM surveillance program, in which the US National Security Agency used their dominant position to gather information stored on servers located in the US for surveillance purposes (Greenwald & MacAskill, 2013; Zeng et al., 2017). As a result of these continuous concerns, reforming the ICANN had become an explicit goal of Chinese representatives in global Internet governance discussions (Zeng et al., 2017). While an initial effort from China and Russia to place the DNS under the authority of the International Telecommunications Union (ITU) in 2012 had failed (D. Lee, 2016), their efforts paid off eventually. During an ICANN meeting in 2014, it was decided that the organization would undergo a procedure of reform. By 2016, ICANN was no longer accountable to the US Department of Commerce (ICANN, 2016). Instead, it was now an independent non-profit organization that would consider opinions from companies, experts, academics and national governments (D. Lee, 2016). Meanwhile, the reform of ICANN led to concerns in the US that losing control over the ICANN meant losing control over the Internet to authoritarian regimes (Kessler, 2016).

It is important to note that China was not alone in promoting a more sovereign position for national governments in Internet governance. Many countries, including Russia, Brazil, South Africa, and Iran, held similar views (Stevens, 2015). However, what made China unique is that, due to the strength of its domestic digital ecosystem, it was able to push these ideas forward on a global stage. For instance, since 2014, the CAC organized the annual World Internet Conference (WIC), in which Chinese and foreign politicians, industry leaders and government officials convened to discuss current issues regarding cyberspace, innovation and society. Besides these debates, the WIC also served as a platform in which the Chinese cyber-governance model could be promoted (Makinen et al., 2015). The WIC fell into a longer list of occasions in which cyber sovereignty was promoted internationally, including at other Internet governance meetings and at the United Nations General Assembly (Creemers, 2020b). Naturally, the promotion of cyber sovereignty served the goal of finding fellow supporters to reform global Internet governance. However, the promotion of cyber sovereignty also served as a legitimization of China's domestic policies.

The strong role of the Chinese state in censorship and social management was still exceptional on a global scale. Defending the right of the Chinese state as a sovereign nation to determine its own cybersphere policies could help legitimize its actions against domestic opposition and international criticisms (Makinen et al., 2015; Zeng et al., 2017).

Like we saw earlier with the Belt and Road Initiative, in global Internet governance the Chinese government was an important system builder attempting to change the status quo, but not the only Chinese actor that fulfilled this role. Following their domestic growth, Chinese private companies also became more involved with cyberspace governance themselves (Shen, 2016). For instance, Alibaba's CEO Jack Ma was elected as a co-chair of NETmundial, an international multi-stakeholder Internet governance platform related to ICANN that aimed to provide a roadmap for the future development of the Internet (Hou, 2015; NETmundial, n.d.). As Shen (2016) described, Chinese governmental representatives also promoted the interests of Chinese tech companies in Internet governance negotiations. This led to a slightly ambiguous message, as on the one hand, China promoted a multilateral governance structure in which every nation had sovereign control over its cybersphere, but on the other hand it stressed the shared responsibility of government and private companies in the governance of cyberspace (Shen, 2016; Y. Zhao & Cao, 2014).

While Internet governance was one means through which Chinese norms and values regarding cyberspace became more prominent globally, it was not the only one. Following the Made in China 2025 policy, in which China strived to become a producer of advanced technological components, China was now moving towards a stronger focus on technological standardization, which was seen as the next step in its economic development (Koty, 2020). As we saw in subsection 3.3.1, the Chinese AI development plan contained the explicit ambition to determine global norms and standards in AI (Huw Roberts et al., 2021). Also in other digital domains, technological standardization was increasingly defined as a focus area for China. During the 19th National Congress of the CCP in October 2017, the ministerial General Administration of Quality Supervision, Inspection and Quarantine and the Standardization Administration of China (SAC), which is a body authorized by the State Council to manage, supervise and coordinate technological standardization in China (ISO, n.d.), proposed the 'China Standards 2035' project (SESEC, 2018). The goal of this project was to formulate an advice to the CCP Central Committee and the State Council for a long-term strategic policy to strengthen the Chinese role in global technological standardization (Seaman, 2020; SESEC, 2018). A working group led by the Chinese Academy of Engineering and the SAC was set up, and in March 2020, the China Standards 2035 plan was presented (Standartisation Administration of China, 2020). The plan focused on how China could move towards a globally dominant standard setting position, in areas such as AI, cloud computing, Internet of Things, or big data, as well as a broader range of fields such as agriculture and biotechnology. On the one hand, the plan was seen as necessary for China's internal economic development. A weakness in the Chinese economy was the large amount of local and regional technological standards that were in place in China, which often even contradicted one another (Seaman, 2020). A result of this phenomenon was that technological design requirements tended to differ heavily between cities and changed frequently over time (Kharpal, 2020). As such, the China Standards 2035 plan allowed for better harmonization of technological systems in China, while also creating economies of scale. However, as with several other policy plans discussed earlier, the plan also contained an external goal, namely that Chinese companies and experts should become more important in global standard setting (Kharpal, 2020). Such a development would mean that Chinese-influenced standards, along with the norms and values encompassed in these standards, would also significantly shape cyberspace outside of China. The plan had a symbiotic relationship with the Belt and Road Initiative, which not only aided Chinese companies in expanding abroad, but also allowed for the

exportation of Chinese standards (Cai, 2017). In the BRI, the implementation of Chinese standards was often included in memoranda of understanding with foreign governments (Kharpal, 2020). This approach of implementing standards through bilateral agreements weakened the position of traditional standardization bodies (Rühlig, 2020), while increasing the outreach of Chinese standards.

Although some experts described the China Standards 2035 plan as a hype (Wilson, 2020) and at the time of writing this report it is yet too early to see concrete consequences of the plan, the growing Chinese influence in technological standardization is already leading to contention. An example in which this becomes apparent is the Chinese proposal to renew the TCP/IP protocols, which together define the way that computers communicate with each other over the Internet (Encyclopaedia Britannica, n.d.). In March 2020, Huawei, China Unicom, China Telecom, and the Ministry of Industry and Information Technology (the successor of the MII) handed in a proposal at the ITU for a 'New IP' (Gross & Murgia, 2020). Its proponents argued that a successor for the IP was required to overcome technological limitations of the current TCP/IP, such as enabling variable address lengths, which is expected to avoid problems with many innovative applications in the domain of Internet of Things (Durand, 2020). Furthermore, the proponents argued that the proposal would not have any implications for Internet governance (Huawei, n.d.). However, critics were wary of the wider implementations of the protocol. Due to its top-down design, Internet service providers would be able to monitor all connected devices and traffic over the network. This would give these service providers considerable power, and would for instance make it possible to automate many censorship processes or to remotely disconnect devices from the Internet, thereby significantly increasing the effectiveness of Internet censorship (Murgia & Gross, 2020; Sharp & Kolkman, 2020). The possibility for service providers to centrally implement rules corresponds to the Chinese notion of cyber sovereignty, as every country would be autonomous in implementing such centrally enforced rules through its service providers. This autonomy would be further enforced by the support that the New IP provides for 'ManyNets', which entails a "federated set of networks" that behave independently and are also controlled independently (Durand, 2020). In other words, each subnetwork could have its own set of rules while remaining compatible. Such a decentralized design could contribute to the emergence of a Splinternet (which was discussed in subsection 3.3.2) (Hoffmann et al., 2020).

A fundamental principle of Science and Technology Studies is that technologies themselves are not neutral. Instead, through the way in which they are designed, they shape the societal systems in which they are embedded (Winner, 1980). The New IP proposal is an example of how certain norms and values are reflected in technological design questions. Likewise, the technological design of the New IP can influence the arrangement of cyberspace, not just in China, where the norms of the New IP originated, but across the world. Although the ITU has not yet taken a final decision on the New IP plan and the discussion is still ongoing at the time of writing this thesis, the example of New IP illustrates how a strong Chinese influence in standard setting can shape cyberspace both in China and across the globe.

In this subsection, we saw how Chinese norms and values regarding cyberspace are becoming increasingly influential worldwide. Aided by the increasingly advanced capabilities of Chinese tech companies, the Chinese State Council began to advocate a move towards a global technological standard setting position in digital technologies. At the same time, Chinese diplomatic efforts to change the norms in global Internet governance towards the ideal of cyber sovereignty were also increasing. This subsection shows that besides the economic expansion of Chinese tech companies abroad, the success of Chinese cyberspace also began to impact cyberspace abroad through different means. Paradoxically, the approach of the Xi administration towards a more sovereign and autonomous cyberspace contributed to an increased

Chinese international presence, as reforms in global Internet reforms and an influential position in global standard setting would allow China to become less dependent on others.

3.3.4 Conclusion of Period 3

This section focused on the outward expansion of Chinese cyberspace, in an effort to answer the following subquestion: *"How did Chinese cyberspace collide with the US-based cyberspace, and how did the resulting interaction and contestation shape both cyberspaces?"*. As we saw in the previous subsections, several important actors drove the international expansion of Chinese cyberspace. First of all, since the accession of president Xi, the Chinese State Council began to take a proactive role as a central system builder in Chinese cyberspace. It developed a set of ambitious policy plans, which besides internal goals each also contained goals aimed at international expansion. The State Council also actively encouraged and supported other actors to join them in these efforts, for instance through the Belt and Road Initiative (BRI). On the other hand, there were the successful Chinese tech companies, who, following their momentum towards further growth, wished to maintain this growth. As a result, these companies began to look at opportunities for expansion abroad. However, the international expansion of Chinese companies led to contestation with the US-based cyberspace. Many foreign governments, with the US government as its major proponent, voiced security concerns regarding the products and services of Chinese tech companies, which led to contestation. Many countries began to exclude Chinese companies from providing essential components to their digital infrastructure. In turn, this prohibition of Chinese products and technology had its influence on Chinese cyberspace. The State Council had already begun to promote a strategy towards a larger Chinese role in technological standardization, partially to promote the creation of more advanced technology in China, and partially to become more autonomous in terms of technological capabilities. However, the exclusion of Chinese companies strengthened the shift towards this standard-setting position. Furthermore, the influence of Chinese cyberspace on the US-based cyberspace could also be experienced in terms of global Internet governance. Driven by the Chinese notion of cyber sovereignty, Chinese governmental representatives and company executives sought to reform the global governance structure of the Internet, making it less US-centric and strengthening the role of national governments in regulation cyberspace, as opposed to the multi-actor governance model that was followed thus far. Furthermore, the advocation of cyber sovereignty and the decision of foreign governments to exclude Chinese technology increases speculation of a so-called splinternet, which would result in two parallel cyberspaces that become detached from each other. Interestingly, Chinese proposals, such as the New IP, seem to support such system decoupling by design. Overall, interestingly, two contradictory trends can be observed. On the one hand, there is a strong increase of the influence of Chinese cyberspace in the US-based cyberspace, through the BRI, the active role in Internet governance bodies and the move towards a larger role in standardization. On the other hand, there is a movement driven by actors from both cyberspaces towards further decoupling of the two digital realms. An overview of the most important developments during period 3 is shown in Figure 5, as well as the relations of these developments with earlier developments in Chinese cyberspace. Again, the red lines depict the separations between the periods.

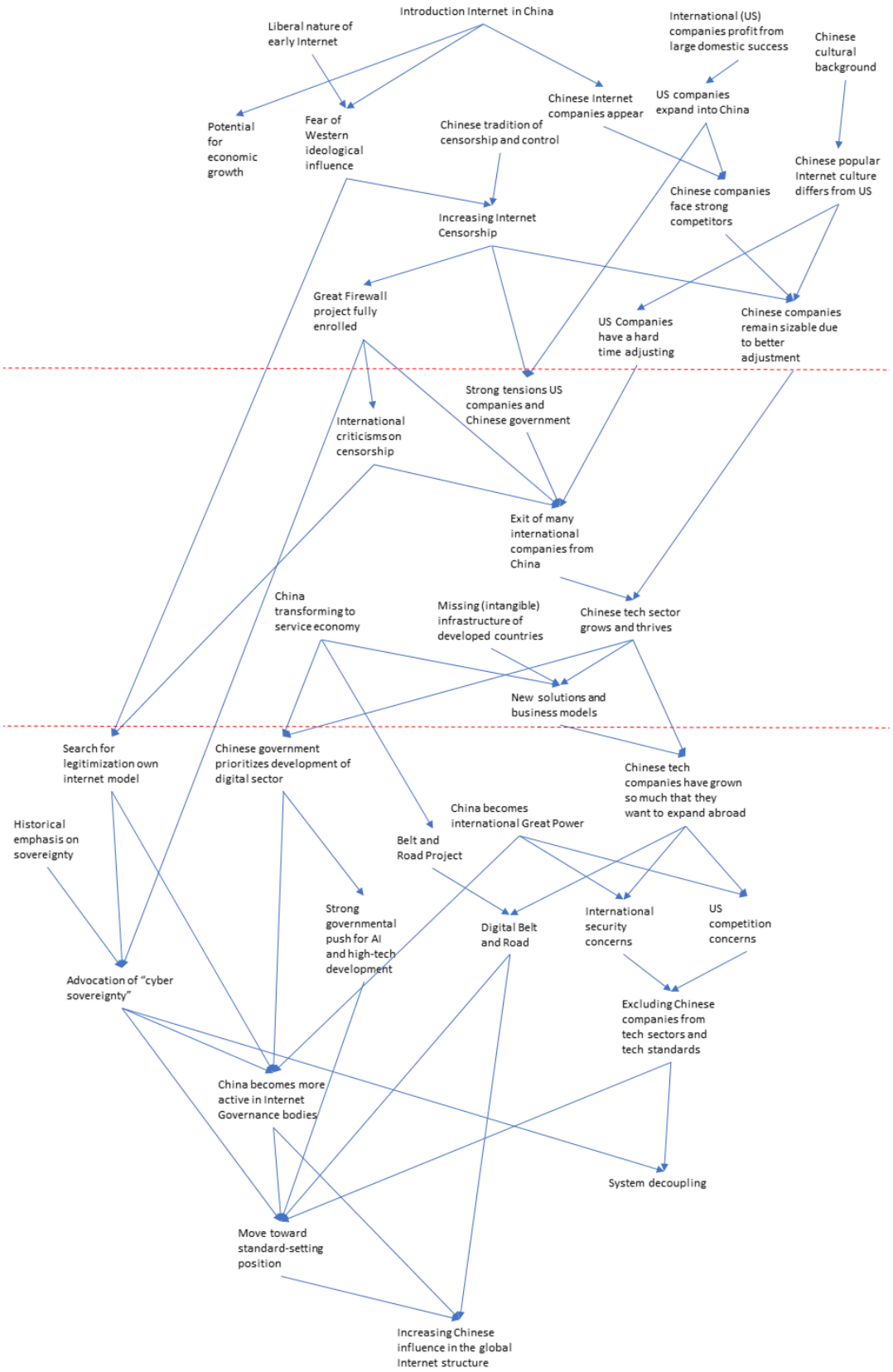


Figure 5: A schematic overview of the most important developments in periods 1, 2 and 3, and their consequences

4 Conclusion & discussion

This chapter will serve as the concluding chapter of this thesis. In the 'Conclusion' section, the findings from the previous chapter are analyzed and combined to answer the research question of this thesis. The final section will be the 'Discussion' section, in which the findings of this thesis are evaluated. The wider implications of the results of this thesis are discussed, as well as observed limitations of this study and recommendations for future research.

4.1 Conclusion

This thesis has focused on answering the following question: *"How can the emergence and evolution of an alternative cyberspace in China be explained from a Large Technical Systems perspective?"*. Through the Large Technical Systems (LTS) perspective, the long-term evolutionary and sociotechnical nature of Chinese cyberspace has been made visible. This thesis has shown that the current state of Chinese cyberspace is the result of a long history of consecutive events and developments, in which actors confronted with certain situations made decisions based on the situation they found themselves in. By changing technological, social, economic, and legal elements in Chinese cyberspace, these actors changed the momentum of the system and thereby indirectly shaped future developments.

The evolutionary nature of Chinese cyberspace becomes most apparent when listing the consecutive developments that had the largest impact on the momentum of Chinese cyberspace. The liberal nature of the early Internet conflicted with pre-existing norms and practices as propagated by the CCP regarding information censorship. To bring the Internet in accordance with these norms and practices, the State Council initiated the creation of the Great Firewall. The Great Firewall served to shield Chinese society from undesired foreign influences, as well as undesired domestic contents on the Internet. A side effect of this Great Firewall was that local Chinese companies became more attractive for Chinese users, as many services from US companies were often unavailable or slow. Efforts of US companies to comply with the Chinese censors to combat these problems resulted in criticisms in the US for contributing to censorship and repression of freedom. The US tech companies felt that they had to decide between either being active in China or strengthening their position outside of China, and chose for the latter. The departure of Chinese tech companies meant that companies like Baidu, Alibaba and Tencent had lost powerful competitors, and as a result were able to monopolize the market and undergo strong growth. In this process, the Chinese tech companies diversified their activities and were able to innovate so much that they became technologically competitive to the US companies. After the Chinese market was saturated, the Chinese tech companies actively sought to expand their activities abroad, and in this process, they were aided through comprehensive programs as initiated by the State Council. However, without the strong domestic growth of Chinese tech companies, both the need to expand abroad and the capability to offer technologically advanced products would not have existed. This capability led to Chinese tech companies being able to strengthen their position in global technological standardization and in exporting technology to other countries, even though these efforts resulted in resistance in some countries. Likewise, an important reason why Chinese representatives were able to significantly influence global Internet governance discussions was the grown importance of the Chinese tech sector. In the analysis of this thesis, no hints could be found that the creation of the Great Firewall or the blocking of US companies not complying with Chinese censorship norms had been intended to increase the Chinese influence in global cyberspace. However, due

to the shifts in momentum resulting from these events, the conditions were created for these future events to occur. An overview of the most important developments in Chinese cyberspace and their consequences can be found in Figure 5.

Conceptualizing the development of Chinese cyberspace as a multi-actor system building process, several actors come forward from the analysis as having had a significant influence on the emergence and evolution of the system. Two of the most influential actors (or perhaps it would even be more accurate to describe them as a single actor, given the overlap in people involved) in the development of Chinese cyberspace have been the CCP leadership and the Chinese State Council. The underlying philosophy of a liberal, open, and deregulated cyberspace that accompanied the early Internet led to strong friction with the philosophy of the CCP regarding how society should be organized. Due to its central position in Chinese society, the State Council was able to adjust the dominant norms underlying the technological design of the Internet in China through the implementation of the Great Firewall and the institutionalization of Internet censorship. In fact, due to the far-reaching importance of the Great Firewall on Chinese cyberspace it appears that had it not been for the norms and values of the CCP, Chinese cyberspace would not have had such a distinct character as it does today. While the State Council had already been actively involved with the Internet since its introduction, a notable increase in involvement can be observed after the accession of the Xi Jinping government. Through the formation of the Cyberspace Administration of China, the increased emphasis of cyber sovereignty, the hosting of the World Internet Forum and the ambitious digital policy plans, the State Council positioned itself even firmer as an important system builder in Chinese cyberspace. Furthermore, it is noteworthy that despite the changing nature of Chinese cyberspace, the guiding principles of the CCP have remained remarkably consistent. Already in the early years of Chinese cyberspace, there was a strong emphasis on the Chinese central government having a final say in the design and policies of cyberspace, and their interests prevailing over interests of other actors. This vision was again reflected in the formulation of the ideas behind cyber sovereignty fifteen to twenty years later. As a result, while the particularities of Chinese cyberspace differed significantly over time, the norms of the CCP towards this system did not. The consistency of the message of the CCP in combination with the central position of the State Council in Chinese cyberspace resulted in other actors having to adjust their behavior to these norms, thereby gradually conforming more and more to the vision of cyberspace as advocated by the CCP. The norms and values of the CCP thereby served as a selective force regarding which elements could or could not be part of Chinese cyberspace, leading not only to the absence of US companies, but also for instance to WeChat becoming more popular than Sina Weibo.

On the other hand, while the steering influence of the CCP and the State Council becomes apparent from the analysis, their influence should also not be overestimated. Many important developments, from the innovative products of Tencent and Alibaba providing solutions to existing problems within Chinese society to telecommunications equipment from Huawei and ZTE becoming leading in the world happened without direct influence from the Chinese central government. Instead, these actors have significantly shaped Chinese cyberspace themselves. While the Chinese State Council formulated many ambitious policy plans such as the Belt and Road Initiative, Made in China 2025 or China Standards 2035, these visions and policy plans were oftentimes responses to developments that were already ongoing in Chinese cyberspace. As such, it becomes questionable whether these focuses should really be partially attributed to the State Council, or whether they are merely endorsements and encouragements of developments that would also have taken place without these policy plans issued by the government. As such, despite the importance the CCP and the State Council as system builders, the importance of these Chinese private companies in the evolution of Chinese cyberspace endorses the approach that conceptualizing the system building of Chinese

cyberspace as a multi-actor game provides a more accurate depiction of why certain developments in Chinese cyberspace took place.

Furthermore, this thesis shows that studying the various elements of Chinese cyberspace as elements of a sociotechnical system reveals important interrelations between these elements. The rapid growth and the innovative capabilities are usually studied from a business and ecosystems lens. However, as this thesis shows, they were indirectly the result of the Chinese censorship regulations, which are usually studied from the privacy lens. Likewise, the tensions between actors from Chinese cyberspace and the US-based cyberspace, which are usually approached through a geopolitical lens, find their origins in this rapid growth of Chinese tech companies. While these relationships are occasionally touched upon in studies using these other lenses, these interrelationships are usually black-boxed or simply 'assumed to be there'. Hence, this thesis shows how a sociotechnical approach can reveal these types of interactions between the various elements of a system.

All in all, this thesis has shown that the current state of Chinese cyberspace can be considered the result of a long evolutionary and sociotechnical process, which ultimately began by the incompatibility of the US-based Internet system and existing dominant norms and practices in Chinese society. The gradual system building efforts of the Chinese Communist Party, the State Council and large Chinese tech companies ultimately culminated in Chinese cyberspace building the technological capabilities to become an important international stakeholder in terms of high-tech equipment and standardization, while the system momentum also incentivized Chinese actors to increasingly look abroad to achieve their goals, such as sustained growth but also increased digital sovereignty. Due to the deeply embedded normative differences that exist between the US-based and Chinese cyberspace, resistance in the west against elements from Chinese cyberspace has arisen, just like how several decades earlier there was Chinese resistance against elements from the US-based cyberspace. Many developments described in this thesis are still ongoing, and it remains to be seen whether the international influence of Chinese cyberspace will continue to increase, whether the Internet will undergo further decoupling, or whether it will be possible to bring the various elements from Chinese and the US-based cyberspace in accordance with each other. However, in any case, a deeper understanding of the origins and the motives behind the expansion of Chinese cyberspace can serve to mitigate disagreements and contribute to more informed actions.

4.2 Discussion

In this section, the findings of this research are evaluated and placed in a wider context. In particular, the feasibility of another distinct cyberspace emerging like in China is discussed, as well as some lessons about the application of theories of sociotechnical change in China. Additionally, the limitations of this study are discussed, and recommendations for future research are provided.

4.2.1 Feasibility of another distinct cyberspace

This thesis has described and explained how a separate cyberspace could emerge and become successful in China. Given the global uniformity of the Internet, the emergence of this separate cyberspace is remarkable, and thus far it is unique in its distinctiveness. However, the success of Chinese cyberspace raises the question if a similar development could also occur in other countries willing to shape cyberspace in accordance with the dominant preferences in that country. Based on the findings of this thesis, several considerations about the feasibility of a separate cyberspace emerging elsewhere can be made.

First of all, one element that led to the uniqueness of Chinese cyberspace was how it was adjusted to Chinese societal challenges. Besides the incompatibility of the liberal US Internet and Chinese norms and practice regarding information censorship, many more examples can be found. For instance, the lack of a well-functioning banking system gave rise to the enormous popularity of digital payment systems, for which the need was far smaller in countries that did already have the infrastructure to easily access affordable loans. The relatively large amount of family businesses in China contributed significantly to the emergence of platforms such as Alibaba's Taobao, which served as a platform to vastly increase the outreach of small businesses, but also to many of the functionalities of WeChat, which served as a platform through which smaller companies could easily offer their services. Furthermore, the entire conceptualization of cyber sovereignty also reflects Chinese characteristics, as the notion supports the more central position that the Chinese national government holds compared to the government in many other countries, where a multi-stakeholder model is more common. All these examples serve to illustrate that Chinese cyberspace did not develop 'in a vacuum', but instead was deeply shaped by the wider context of Chinese society. Of course, China is not the only country in which local circumstances differ from the US. However, due to the more protective environment created by the Great Firewall, among others, these selective pressures in Chinese society could come to expression more, thereby shaping Chinese cyberspace more in response to its own characteristics and challenges than would have happened if the US-based system configuration of cyberspace had simply been transposed to China.

Secondly, an important element in the emergence of Chinese cyberspace was the rejection of the values embedded in the US-based cyberspace, which supported the ideals of a liberal and free space devoid of governmental intervention. The Chinese government was certainly not the only national government that rejected these principles. Many countries, including Russia, Iran, Turkey, and Egypt, are also in favor of more stricter content regulations on the Internet (Zittrain et al., 2017). Meanwhile, regions like the European Union also advocate a slightly different set of norms and values in cyberspace, with a much stronger focus on privacy and ethics than the United States, where the focus rests more on liberty (O'Hara & Hall, 2018). Of the countries mentioned here, Russia forms a particularly interesting case. While Facebook and Google are both accessible in Russia, Russia is together with China one of the only countries in the world where these US platforms are not dominant, as respectively VKontakte and Yandex are the most popular platforms (although Google still controls 44% of the Russian search engine market) (Serpstat, n.d.; Wallach, 2020). Unlike in China, these platforms did not enjoy any particular advantages as a result of governmental interference. Instead, looking at VKontakte, the company managed to become the most popular Russian social media platform by simply imitating Facebook, while also providing easy access to pirated movies and music, much like Baidu did in China (Griffiths, 2019). Still, these Russian tech companies did not nearly become as innovative as the US or Chinese tech giants. Although it is always arbitrary to pinpoint a single cause given the complexity of the matter, a key difference between Russia and China is the enormous domestic market that China has, which provided ample space for Chinese tech companies to grow in and allowed these companies to enjoy economies of scale. Only India and, to a lesser extent, the European Union have an internal market that could be considered comparable in size.

Lastly, the increasing importance of Chinese cyberspace has resulted in the Chinese vision of cyber sovereignty being propagated more on the international stage. This vision contains the message that national governments should be autonomous in shaping cyberspace within their national boundaries in accordance with their own preference. As such, this vision contains the premise that, if desired, other countries should also be able to create a fundamentally different cyberspace. If the ideals of cyber sovereignty are translated into tangible Internet governance reforms in the future, for instance through technological changes such as

the New IP proposal or through international organizations such as the ITU ascribing to these principles, then that could provide both the opportunity and the legitimization for other countries to also make more drastic changes to their cyberspace.

However, given the considerations mentioned earlier, even if the idea of cyber sovereignty would become more accepted globally, it would still be a challenge to make significant changes to cyberspace. The large Chinese domestic market, the rejection of the norms and values incorporated in the US-based cyberspace, and the different set of domestic problems that the Internet in China could solve together formed a unique set of conditions for Chinese cyberspace to develop the way it did. As such, while the possibility of another distinct cyberspace emerging should certainly not be ruled out, it does not seem likely to happen anytime soon.

4.2.2 Limitations

Due to the scope and the methodology of this thesis, this thesis contains several limitations. These limitations will be discussed in this subsection.

The first limitation of this thesis results from the choice to base the research on written sources about Chinese cyberspace. Due to the scope of this thesis, the research focuses on the actions, ideas, and decisions of very important actors within Chinese cyberspace, including CEOs of large tech companies, politicians and highly ranked government officials. Since these people would not be available for an interview, nor be approachable in any other way, this thesis had to focus on available literature. However, only a limited amount of these sources was written or contains interviews with the stakeholders involved. Instead, a significant amount of the source material consisted of secondary sources, which were often based on information from Chinese sources, as well as interpretations and observations resulting from substantial academic research. Although these sources are of high quality, the use of secondary sources can lead to difficulties when using a constructivist approach, which was used in this thesis. The reason for these difficulties is that the constructivist approach not only pays attention to factual developments, but also to the motives and beliefs of actors and the wider context in which they found themselves. Secondary sources can provide in-depth information about factual events and the broader context of these events, but motives and beliefs cannot be known with certainty unless these actors provide information about them themselves or unless they can be synthesized from written texts by these actors. However, given that the relevant actors for this thesis are of such stature that they would not be available for such discussions, this limitation is inherent to the nature of this thesis. Nonetheless, it is a limitation that should be acknowledged.

A second limitation is due to the closed nature of decision-making processes in China. Typically, in western contexts, processes of policy formulation happen in sight of civil society, or often even in collaboration with stakeholders. As a result, a significant amount of information already becomes public during the process itself, including the positions of individual actors in these decision-making processes or proposals that were not turned into actual policy. This is especially true for governmental actors. However, in China these decision-making processes usually occur behind closed doors, and only the end results of the discussions are announced. This makes it difficult to find out how certain decisions were drawn from these discussions, or even who were involved in these discussions. Moreover, due to this closed nature, some information even remains unknown in general. For instance, while the implementation of the Golden Shield project is ascribed to the Ministry of Public Security (J. Wu & Lam, 2017) and the lead engineer of the Great Firewall is known (Global Times, 2011), the exact origins of and the buildup to the Great Firewall itself remain unknown. While the narrative of this thesis can still be constructed without these pieces of

information, it would have been preferable to have knowledge of these processes, so that an even deeper analysis could have been made.

A third limitation is that, as discussed in section 2.2, due to the focus of the Large Technical Systems framework on the larger and more structural elements of a sociotechnical system, there is a risk of neglecting the importance of smaller actors, such as users. In the analysis of this thesis, the role of users in the shaping of Chinese cyberspace indeed appeared to be limited. It might be the case that the limited importance given to users in the findings of this thesis is a misrepresentation caused by this limitation of the framework.

A fourth limitation is that the importance of certain developments often only becomes apparent in hindsight. As exemplified by the causal relations investigated in this thesis, earlier developments can contribute to future developments in ways that were often not expected in advance, for instance because they influence the momentum of the system. Because of this uncertainty, it could be the case that the importance of developments during the period analyzed in this thesis only becomes clear once future developments have taken place. Therefore, it is important to acknowledge that this thesis can by no means provide an exhaustive overview of the important developments in Chinese cyberspace, and that additions can always be made in the future.

4.2.3 Recommendations for future research

The results of this research show that studying Chinese cyberspace, or cyberspace in general, from a sociotechnical perspective can lead to interesting insights. As such, this thesis serves as inspiration for various other valuable research subjects, in which this sociotechnical lens could also be applied to generate new insights.

First of all, this research has focused on how the frictions between Chinese society and the US-based cyberspace resulted in the emergence of a distinct cyberspace. However, China was not the only country where the US-based cyberspace led to frictions. As such, it would be interesting to extend this research by investigating why other countries did not develop a distinct cyberspace, despite frictions with the US-based Internet, and what ways system builders in that country found instead to bring the Internet in accordance with the practices in that country.

Secondly, in an attempt to provide an overview of the most impactful developments that shaped Chinese cyberspace, this thesis has primarily focused on a macro-scale. However, looking at this sociotechnical system from a different perspective can reveal new dynamics. An example of such a different perspective could be a focus on users: how they interacted with the Internet, how these interactions changed over time, and how the Internet gradually changed their lives. Such a focus might especially be relevant due to the acknowledgement made earlier that LTS tends to attribute less importance to these smaller actors. Another interesting, but very different, perspective could be to focus on the impacts of the expansion of Chinese cyberspace on a specific site outside China, such as in a city that participates in the Belt and Road Initiative.

Thirdly, given the rapid developments occurring both within and outside Chinese cyberspace, it would be useful to investigate these new developments again within a few years. Not only would such renewed research extend the information of this research with a new period, but it would also shed new light on the observations of this thesis, as due to the evolutionary nature of Chinese cyberspace some development that initially appeared to be rather minor occurrences may unexpectedly lead to significant changes in the future.

Lastly, it would be interesting to contrast the evolution of Chinese cyberspace with that of the US-based cyberspace. While the development of ARPANET, an early predecessor to the current Internet developed in the US, has already been studied from a Large Technical Systems perspective (T. P. Hughes, 1998), a comprehensive study of the US-based cyberspace comparable to this study about Chinese cyberspace does not yet exist. Such as study could reveal parallels and differences between the two systems, which could lead to interesting comparisons.

5 Bibliography

Ahmed, A., & Phartiyal, S. (2021, March 11). India likely to block China's Huawei over security fears: officials. *Reuters*. https://www.reuters.com/article/us-india-china-huawei-idUSKBN2B31PU

Allyn, B. (2020, September 27). U.S. Judge Halts Trump's TikTok Ban, Hours Before It's Set To Start. *NPR*. https://www.npr.org/2020/09/27/917452668/u-s-judge-halts-trumps-tiktok-ban-hours-before-it-was-set-to-start?t=1620133968674

Arbel, T. (2021, February 11). US distances itself from Trump attempts to ban WeChat. *ABC News*. https://abcnews.go.com/Business/wireStory/us-distances-trump-attempts-ban-wechat-75829270

Arenal, A., Armuña, C., Feijoo, C., Ramos, S., Xu, Z., & Moreno, A. (2020). Innovation ecosystems theory revisited: The case of artificial intelligence in China. *Telecommunications Policy*, *44*(6). https://doi.org/10.1016/j.telpol.2020.101960

Arnold, M. (2018, May 29). Blurring the lines of banking in China. *Financial Times*. https://www.ft.com/content/ef39e678-632f-11e8-90c2-9563a0613e56

Arsène, S. (2012, May 21). The impact of China on global Internet governance in an era of privatized control. *Chinese Internet Research Conference*.

Arthur, W. B. (1989). Competing Technologies, Increasing Returns, and Lock-In by Historical Events. *The Economic Journal*, *99*(394), 116–131.

Auchard, E. (2007, November 13). Yahoo settles case over Chinese dissident e-mails. *Reuters*. https://www.reuters.com/article/us-yahoo-china-idUSN1360603420071113

Bai, C.-E., Lu, J., & Tao, Z. (2006). Property rights protection and access to bank loans. *The Economics of Transition*, *14*(4), 611–628. https://doi.org/10.1111/j.1468-0351.2006.00269.x

Bajpai, P. (2020, April 22). *China's GDP Examined: A Service-Sector Surge*. Investopedia. https://www.investopedia.com/articles/investing/103114/chinas-gdp-examined-servicesector-surge.asp

Bamman, D., O'Connor, B., & Smith, N. A. (2012). *View of Censorship and deletion practices in Chinese social media*. First Monday. https://firstmonday.org/article/view/3943/3169

Barboza, D. (2005, August 11). Yahoo Is Paying $1 Billion for 40% Stake in Alibaba. *The New York Times*. https://www.nytimes.com/2005/08/11/technology/yahoo-is-paying-1-billion-for-40-stake-in-alibaba.html

Barboza, D. (2007, January 6). Google Makes Another Investment in the Internet in China. *The New York Times*. https://www.nytimes.com/2007/01/06/technology/06google.html?scp=5&sq=google+china&st=nyt

Barlow, J. P. (1996, February 8). *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence

Barme, G. R., & Ye, S. (1997, June 1). *The Great Firewall of China*. WIRED. https://www.wired.com/1997/06/china-3/

Barrett, E. (2020, January 20). *A.I. in China: TikTok is just the beginning*. Fortune. https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/

Baum, R. (1994). *Burying Mao: Chinese Politics in the Age of Deng Xiaoping*. Princeton University Press.

Baxter, P., & Jack, S. (2008). Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. *The Qualitative Report*, *13*(4), 544–559.

Bazeley, P. (2013). *Qualitative Data Analysis: Practical Strategies*. Sage.

BBC News. (2002, September 2). China blocking Google. *BBC News*. http://news.bbc.co.uk/2/hi/technology/2231101.stm
BBC News. (2006, June 23). Google offloads Baidu investment. *BBC News*. http://news.bbc.co.uk/2/hi/business/5108778.stm
BBC News. (2010, March 23). China condemns decision by Google to lift censorship. *BBC News*. http://news.bbc.co.uk/2/hi/asia-pacific/8582233.stm
BBC News. (2013a, July 19). Huawei denies spying allegations by former CIA chief. *BBC News*. https://www.bbc.com/news/business-23373178
BBC News. (2013b, September 9). China issues new internet rules that include jail time. *BBC News*. https://www.bbc.com/news/world-asia-china-23990674
BBC News. (2017, September 26). Social media and censorship in China: how is it different to the West? *BBC News*. https://www.bbc.com/news/newsbeat-41398423
BBC News. (2018, August 23). Huawei and ZTE handed 5G network ban in Australia. *BBC News*. https://www.bbc.com/news/technology-45281495
BBC News. (2019a, May 20). Huawei's Android loss: How it affects you. *BBC News*. https://www.bbc.com/news/technology-48334739
BBC News. (2019b, June 2). Huawei signs deal with Russian telecoms firm to develop 5G. *BBC News*. https://www.bbc.com/news/business-48537643
Bennhold, K., & Ewing, J. (2020, January 16). In Huawei Battle, China Threatens Germany "Where It Hurts": Automakers. *The New York Times*. https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html
Bentley, J. H. (1996). Cross-Cultural Interaction and Periodization in World History. *The American Historical Review*, *101*(3), 749–770. https://doi.org/10.2307/2169422
Bhuijan, A. J. M. S. A. (2010). *Postcolonial states and internet governance: possibilities of a counter-hegemonic bloc?* Simon Fraser University.
Blanchard, B., Li, H., & Carsten, P. (2013, September 9). China threatens tough punishment for online rumor spreading. *Reuters*. https://www.reuters.com/article/us-china-internet-idUSBRE9880CQ20130909
Borak, M. (2020, October 16). Beyond the Great Firewall: China's vast censorship apparatus ropes in companies to do the work themselves. *South China Morning Post*. https://www.scmp.com/abacus/tech/article/3105522/beyond-great-firewall-chinas-vast-censorship-apparatus-ropes-companies
Branigan, T. (2009, June 2). China blocks Twitter, Flickr and Hotmail ahead of Tiananmen anniversary. *The Guardian*. https://www.theguardian.com/technology/2009/jun/02/twitter-china
Branigan, T. (2013, March 14). Xi Jinping becomes China's president. *The Guardian*. https://www.theguardian.com/world/2013/mar/14/xi-jinping-installed-china-president
Brenkert, G. G. (2009). Google, human rights, and moral compromise. *Journal of Business Ethics*, *85*(4), 453–478. https://doi.org/10.1007/s10551-008-9783-3
Brown, R. (1963). *Explanation in Social Science*. Routledge.
Butcher, H. (2019, March 12). *Navigating the Internet in China: Top Concerns for Foreign Businesses*. China Briefing. https://www.china-briefing.com/news/internet-china-top-concerns-foreign-businesses/
Cai, P. (2017). Understanding China's Belt and Road Initiative. *Lowy Institute*, *March*, 1–26. https://www.lowyinstitute.org/sites/default/files/documents/Understanding China's Belt and Road

Initiative_WEB_1.pdf
Callanan, C., Dries-Ziekenheiner, H., Escudero-Pascual, A., & Guerra, R. (2010). *Leaping Over the Firewall: A Review of Censorship Circumvention Tools*.
Capri, A. (2020). *Strategic US-China decoupling in the tech sector: Why and how it's happening* (Issue June).
Cartwright, M. (2020). Internationalising state power through the internet: Google, Huawei and geopolitical struggle. *Internet Policy Review*, *9*(3), 1–18. https://doi.org/10.14763/2020.3.1494
Carvajal, N., & Kelly, C. (2020, August 7). Trump issues orders banning TikTok and WeChat from operating in 45 days if they are not sold by Chinese parent companies. *CNN*. https://edition.cnn.com/2020/08/06/politics/trump-executive-order-tiktok/index.html
Chandel, S., Zang, J., Yu, Y., Sun, J., & Zhang, Z. (2019). The Golden Shield Project of China: A Decade Later - An in-Depth Study of the Great Firewall. *2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2019*, 111–119. https://doi.org/10.1109/CyberC.2019.00027
Charmaz, K. (2006). *Constructing Grounded Theory: A Practical Guide through Qualitative Analysis*. SAGE Publications Ltd.
Chen, S., Zhang, H., Lin, M., & Lv, S. (2011). Comparision of microblogging service between Sina Weibo and Twitter. *Proceedings of 2011 International Conference on Computer Science and Network Technology, ICCSNT 2011*, *4*, 2259–2263. https://doi.org/10.1109/ICCSNT.2011.6182424
Chen, T. (2015, July 19). *2.1 million WeChat "false rumors" deleted daily*. WalktheChat. https://walkthechat.com/centership-of-wechat-rumors-on-wechat-2-1million-rumors-deleated-daily/
Chen, Yi. (1992). Publishing in China in the Post-Mao Era: The Case of Lady Chatterley's Lover. *Asian Survey*, *32*(6), 568–582. https://doi.org/10.2307/2645161
Chen, Yongrong, & Liu, X. (2017, April 29). Xinhua Insight: Belt and Road Initiative boosts China's e-commerce. *Xinhua*. http://www.xinhuanet.com//english/2017-04/29/c_136245718.htm
Cheung, T. M. (2018). The rise of China as a cybersecurity industrial power: balancing national security, geopolitical, and development priorities. *Comparative Industrial Policy and Cybersecurity*, *3*(3), 306–326. https://doi.org/10.1080/23738871.2018.1556720
Chiu, K. (2020, October 5). Google Chrome remains China's most popular web browser, even with Google search and other apps blocked. *South China Morning Post*. https://www.scmp.com/abacus/tech/article/3103747/google-chrome-remains-chinas-most-popular-web-browser-even-google
Ciuriak, D. (2019). The US-China Trade War : Technological Roots and WTO Responses The US-China Trade War : Technological Roots and WTO Responses. *Global Solutions Journal*, *4*(March), 130–135.
Clover, C. (2016, March 18). Tencent's WeChat dominates China's lucrative messaging app market. *Financial Times*. https://www.ft.com/content/aadd256e-d0ef-11e5-831d-09f7778e7377
CNNIC. (2013). *Statistical Report on Internet Development in China*.
CNNIC. (2020). *The 45th China Statistical Report on Internet Development*.
Cottrell, R. L. A., Granieri, C., Fan, L., Xu, R., & Karita, Y. (1994). Networking With China. *Conference on Computing in High Energy Physics*.
Creemers, R. (2020a). *China's Approach to Cyber Sovereignty*.
Creemers, R. (2020b). China's Conception of Cyber Sovereignty: Rhetoric and Realization. In D. Broeders & B. van den Berg (Eds.), *Governing Cyberspace: Behavior, Power, and Dipolmacy* (pp.

107–142). Rowman & Littlefield.
Creswell, J. W., & Creswell, J. D. (2018). *Research Design* (5th ed.). SAGE Publications Ltd.
Dai, S. (2019, August 30). China adds Huawei, Hikvision to expanded 'national team' spearheading country's AI efforts. *South China Morning Post*. https://www.scmp.com/tech/big-tech/article/3024966/china-adds-huawei-hikvision-expanded-national-team-spearheading
Dai, S., & Tao, L. (2019, November 26). Chinese data mining firm MiningLamp, now a national AI champion, began by helping police solve crimes. *South China Morning Post*. https://www.scmp.com/tech/start-ups/article/3039252/chinese-data-mining-firm-now-national-ai-champion-started-out
Dai, X. (2002). Towards a digital economy with Chinese characteristics? *New Media and Society*, *4*(2), 141–162. https://doi.org/10.1177/14614440222226316
Dann, G. E., & Haddow, N. (2008). Just doing business or doing just business: Google, Microsoft, Yahoo! and the business of censoring China's Internet. *Journal of Business Ethics*, *79*(3), 219–234. https://doi.org/10.1007/s10551-007-9373-9
David, P. A. (1985). Clio and the Economy of QWERTY. *The American Economic Review*, *75*(2), 332–337. https://doi.org/10.2104/ha080079
de Kloet, J., Poell, T., Guohua, Z., & Yiu Fai, C. (2019). The plaformization of Chinese Society: infrastructure, governance, and practice. *Chinese Journal of Communication*, *12*(3), 249–256. https://doi.org/10.1080/17544750.2019.1644008
Decker, S. (2014, August 6). An Insider's Account of the Yahoo-Alibaba Deal. *Harvard Business Review*. https://hbr.org/2014/08/an-insiders-account-of-the-yahoo-alibaba-deal
Deibert, R. (2013). Trouble at the border: China's internet. *Index on Censorship*, *42*(2), 132–135. https://doi.org/10.1177/0306422013495334
Deibert, R. J. (2002). Dark guests and great firewalls: The internet and Chinese security policy. *Journal of Social Issues*, *58*(1), 143–159. https://doi.org/10.1111/1540-4560.00253
Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (2011). Access Contested: Toward the Fourth Phase of Cyberspace Controls. In R. Deibert, J. Palfrey, R. Rohozinski, & J. Zittrain (Eds.), *Access Contested: Security, Identity and Resistance in Asian Cyberspace* (pp. 3–20). MIT Press.
Dekker, B., Okano-Heijmans, M., & Zhang, E. S. (2020). *Unpacking China's Digital Silk Road*.
Demchak, C. C. (2016). Uncivil and Post-Western Cyber Westphalia: Changing interstate power relations on of the cybered age. *The Cyber Defense Review*, *1*(1), 49–74.
Department of International Cooperation of the Ministry of Science and Technology. (2017). *Next Generation Artificial Intelligence Development Plan*. http://fi.china-embassy.org/eng/kxjs/P020171025789108009001.pdf
Dickie, M. (2005, November 10). Yahoo backed on helping China trace writer. *Financial Times*. https://www.ft.com/content/7ed7a41e-515f-11da-ac3b-0000779e2340
Donnelly, L., Foster, P., & Andrews, A. (2009, September 5). China Google boss departure reignites debate over censorship. *The Telegraph*. https://www.telegraph.co.uk/news/worldnews/asia/china/6143553/China-Google-boss-departure-reignites-debate-over-censorship.html
Drummond, D. (2010a, January 12). *A new approach to China*. Official Google Blog. https://googleblog.blogspot.com/2010/01/new-approach-to-china.html
Drummond, D. (2010b, March 22). *A new approach to China: an update*. Official Google Blog. https://googleblog.blogspot.com/2010/03/new-approach-to-china-update.html

Drummond, D. (2010c, June 28). *An update on China*. Official Google Blog. https://googleblog.blogspot.com/2010/06/update-on-china.html

Du, X. (1999). Internet diffusion and usage in China. *Prometheus: Critical Studies in Innovation*, *17*(4), 405–420. https://doi.org/10.1080/08109029908632119

Durand, A. (2020). *New IP*. https://www.icann.org/en/system/files/files/octo-017-27oct20-en.pdf

Dutton, W. H., & Peltu, M. (2008). The New Politics of the Internet. Multi-stakeholder Policy-making and the Internet Technocracy. In A. Chadwick & P. Howard (Eds.), *Routledge Handbook of Internet Politics* (pp. 384–400). Routledge.

Economy, E. C. (2018, June 29). The great firewall of China: Xi Jinping's internet shutdown. *The Guardian*. https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown

Emmott, R. (2019, February 5). U.S. warns European allies not to use Chinese gear for 5G networks. *Reuters*. https://www.reuters.com/article/us-usa-china-huawei-tech-eu/u-s-warns-european-allies-not-to-use-chinese-gear-for-5g-networks-idUSKCN1PU1TG

Encyclopaedia Britannica. (n.d.). *TCP/IP*. Encyclopaedia Britannica. Retrieved May 9, 2021, from https://www.britannica.com/technology/TCP-IP

European Commission. (2020, January 29). *Commission endorses EU toolbox to secure 5G networks*. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/ip_20_123

eWTP. (n.d.). *About us - eWTP*. EWTP. Retrieved May 24, 2021, from https://www.ewtp.org/about/introduction.html

Feijóo, C., Kwon, Y., Bauer, J. M., Bohlin, E., Howell, B., Jain, R., Potgieter, P., Vu, K., Whalley, J., & Xia, J. (2020). Harnessing artificial intelligence (AI) to increase wellbeing for all: The case for a new technology diplomacy. *Telecommunications Policy*, *44*(6). https://doi.org/10.1016/j.telpol.2020.101988

Ferdinand, P. (2016). Westward ho—the China dream and 'one belt, one road': Chinese foreign policy under Xi Jinping. *International Affairs*, *92*(4), 941–957. https://doi.org/10.1111/1468-2346.12660

FlorCruz, J. A., & Seu, L. (2014, April 24). From snail mail to 4G, China celebrates 20 years of Internet connectivity. *CNN*. https://edition.cnn.com/2014/04/23/world/asia/china-internet-20th-anniversary/index.html

Freifeld, K., & Alper, A. (2021, January 17). Exclusive: Trump admin slams China's Huawei, halting shipments from Intel, others - sources. *Reuters*. https://www.reuters.com/article/us-usa-huawei-tech-exclusive-idUSKBN29M0KD

Gadgets Now. (2020, November 10). *10 'biggest' smartphone companies in the world right now*. Gadgets Now. https://www.gadgetsnow.com/slideshows/10-biggest-smartphone-companies-in-the-world-right-now/photolist/79138464.cms

Garraghan, G. J. (1946). *A Guide to Historical Method* (J. Delanglez (Ed.); 1st ed.). Fordham University Press.

Geels, F. W. (2002). Technological transitions as evolutionary reconfiguration processes: A multi-level perspective and a case-study. *Research Policy*, *31*(8–9), 1257–1274. https://doi.org/10.1016/S0048-7333(02)00062-8

Geels, F. W. (2007). Transformations of Large Technical Systems. *Science, Technology, & Human Values*, *32*(2), 123–149. https://doi.org/10.1177/0162243906293883

Geels, F. W., & Schot, J. (2007). Typology of sociotechnical transition pathways. *Research Policy*, *36*(3), 399–417. https://doi.org/10.1016/j.respol.2007.01.003

Geertz, C. (1973). Thick description: Toward an interpretive theory of culture. In Y. S. Lincoln & N. K. Denzin (Eds.), *Turning points in qualitative research: Tying knots in a handkerchief* (pp. 143–168). AltaMira Press.

Gibson, C. (2009, July 8). China's Facebook Status: Blocked. *ABC News*. https://abcnews.go.com/theworldnewser/2009/07/chinas-facebook-status-blocked.html

Global Times. (2009, August 20). Typhoon Morakot and the fragile Web world. *Global Times*. https://www.globaltimes.cn/content/459303.shtml

Global Times. (2011, February 18). *Great Firewall father speaks out*. Sina. http://english.sina.com/china/p/2011/0217/360409.html

Global Times. (2021, March 8). China's 5-year plan to lead global recovery. *Global Times*. https://www.globaltimes.cn/page/202103/1217749.shtml

Goffman, E. (1974). *Frame Analysis: An Essay on the Organization of Experience*. Harvard University Press.

Goldenberg, S. (2006, February 16). Congress accuses Google of collusion. *The Guardian*. https://www.theguardian.com/technology/2006/feb/16/news.newmedia

Goldsmith, J., & Wu, T. S. (2006). *Who Controls the Internet?: Illusions of a Borderless World*. Oxford University Press.

Goldstein, L. J. (2015). *Meeting China Halfway: How to Defuse the Emerging US-China Rivalry*. Georgetown University Press.

Green, W. A. (1992). Periodization in European and World History. *Journal of World History*, *3*(1), 13–53.

Greenwald, G., & MacAskill, E. (2013, June 7). NSA Prism program taps in to user data of Apple, Google and others. *The Guardian*. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Griffiths, J. (2019). *The Great Firewall of China: How to Build and Control an Alternative Version of The Internet* (1st ed.). Zen Books Ltd.

Gross, A., & Murgia, M. (2020, March 27). China and Huawei propose reinvention of the internet. *Financial Times*. https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2

Hachigian, N. (2002). The internet and power in one-party East Asian states. *Washington Quarterly*, *25*(3), 41–58. https://doi.org/10.1162/01636600260046226

Hamilton, C., & Ohlberg, M. (2020). *Hidden Hand: Exposing How the Chinese Communist Party is Reshaping the World*. Hardie Grant.

Hanson, L. (2015, February 24). The Chinese Internet Gets A Stronger Backbone. *Forbes*. https://www.forbes.com/sites/lisachanson/2015/02/24/the-chinese-internet-gets-a-stronger-backbone/?sh=799299351ff4

Hao, X., Zhang, K., & Yu, H. (1996). The Internet and Information Control: The Case of China. *The Electronic Journal of Communication*, *6*(2).

Hartman, L. (2020, December 17). *Expanded Clean Network initiative safeguards data*. ShareAmerica. https://share.america.gov/expanded-clean-network-initiative-safeguards-data/

Harwit, E. (2008). *China's Telecommunications Revolution*. Oxford University Press.

Harwit, E., & Clark, D. (2001). Shaping the Internet in China. Evolution of Political Control over Network Infrastructure and Content. *Asian Survey*, *41*(3), 377–408. https://doi.org/10.1525/as.2001.41.3.377

He, Y. (2015, July 17). Internet media should drive digital Silk Road: Ren. *China Daily*.

http://www.chinadaily.com.cn/business/fourmoninternet/2015-07/17/content_21308346.htm
Helft, M. (2009, March 24). YouTube Being Blocked in China, Google Says. *The New York Times*. https://www.nytimes.com/2009/03/25/technology/internet/25youtube.html?scp=18&sq=google+china&st=nyt
Herman, A. (2018, December 10). Huawei's (And China's) Dangerous High-Tech Game. *Forbes*. https://www.forbes.com/sites/arthurherman/2018/12/10/huaweis-and-chinas-dangerous-high-tech-game/?sh=3489ba8211ab
Herold, D. K., & de Seta, G. (2015). Through the Looking Glass: Twenty Years of Chinese Internet Research. *Information Society*, *31*(1), 68–82. https://doi.org/10.1080/01972243.2014.976688
Herold, D. K., & Marolt, P. (2011). *Online society in China: Creating, celebrating and instrumentalising the online carnival*. Routledge.
Hess, D. J., & Sovacool, B. K. (2020). Sociotechnical matters: Reviewing and integrating science and technology studies with energy social science. *Energy Research and Social Science*, *65*, 101462. https://doi.org/10.1016/j.erss.2020.101462
Hobbs, W. R., & Roberts, M. E. (2018). How sudden censorship can increase access to information. *American Political Science Review*, *112*(3), 621–636. https://doi.org/10.1017/S0003055418000084
Hoffmann, S., Lazanski, D., & Taylor, E. (2020). Standardising the splinternet: how China's technical standards could fragment the internet. *Journal of Cyber Policy*, *5*(2), 239–264. https://doi.org/10.1080/23738871.2020.1805482
Hong, J., & Huang, L. (2005). A split and swaying approach to building information society: The case of Internet cafes in China. *Telematics and Informatics*, *22*(4), 377–393. https://doi.org/10.1016/j.tele.2004.11.005
Hong, Y. (2017a). *Networking China: The Digital Transformation of the Chinese Economy*. University of Illinois Press.
Hong, Y. (2017b). Reading the 13th five-year Plan: Reflections on China's ICT policy. *International Journal of Communication*, *11*, 1755–1774.
Hong, Y., & Goodnight, G. T. (2020). How to think about cyber sovereignty: the case of China. *Chinese Journal of Communication*, *13*(1), 8–26. https://doi.org/10.1080/17544750.2019.1687536
Hong, Y., & Harwit, E. (2020). China's globalizing internet: history, power, and governance. *Chinese Journal of Communication*, *13*(1), 1–7. https://doi.org/10.1080/17544750.2020.1722903
Hou, L. (2015, July 1). Alibaba's Ma elected co-chairman of Netmundial Initiative. *People's Daily Online*. http://en.people.cn/n/2015/0701/c98649-8914025.html
Hounsel, A., Mittal, P., & Feamster, N. (2018). Automatically generating a large, culture-specific blocklist for China. *8th USENIX Workshop on Free and Open Communications on the Internet, FOCI 18*.
Hu, A. G. Z., Jefferson, G. H., & Jinchang, Q. (2005). R&D and technology transfer: firm-level evidence from Chinese industry. *Review of Economics and Statistics*, *87*(4), 780–786.
Hu, J., Li, G., & Zhu, F. (2017). Regional Financial Developments and Research and Development Investment–Cash Flow Sensitivity: Evidence on Chinese Public High-Tech Companies. *International Review of Finance*, *17*(4), 627–643. https://doi.org/10.1111/irfi.12122
Huang, Y. (2016). Understanding China's Belt & Road Initiative: Motivation, framework and assessment. *China Economic Review*, *40*(2016), 314–321. https://doi.org/10.1016/j.chieco.2016.07.007
Huang, Z. (2017, December 28). *All the things you can—and can't—do with your WeChat account in China*. Quartz. https://qz.com/1167024/all-the-things-you-can-and-cant-do-with-your-wechat-

account-in-china/
Huawei. (n.d.). *A Brief Introduction about New IP Research Initiative*. Huawei. Retrieved May 9, 2021, from https://www.huawei.com/en/industry-insights/innovation/new-ip
Hughes, C. R., & Ermert, M. (2003). What's in a name?: China and the domain name system. In C. R. Hughes & G. Wacker (Eds.), *China and the Internet: Politics of the Digital Leap Forward* (pp. 127–138). Routledge.
Hughes, T. P. (1979). The Electrification of America: The System Builders. *Technology and Culture*, *20*(1), 124–161.
Hughes, T. P. (1983). *Networks of Power: Electrification in Western Society, 1880-1930*. The John Hopkins University Press.
Hughes, T. P. (1986). The Seamless Web: Technology, Science, Etcetera, Etcetera. *Social Studies of Science*, *16*(2), 281–292. https://doi.org/10.1177/0306312786016002004
Hughes, T. P. (1987). The Evolution of Large Technological Systems. In W. E. Bijker, T. P. Hughes, & T. Pinch (Eds.), *The Social Construction of Technological Systems: New Directions in the Sociology and History of Technology*. The MIT Press.
Hughes, T. P. (1995). Technological Momentum. In M. R. Smith & L. Marx (Eds.), *Does Technology Drive History?* (pp. 101–114). MIT Press.
Hughes, T. P. (1998). *Rescuing Prometheus*. Pantheon Books.
IANA. (n.d.). *Root Servers*. Internet Assigned Numbers Authority. Retrieved April 25, 2021, from https://www.iana.org/domains/root/servers
ICANN. (2016, October 1). *Stewardship of IANA Functions Transitions to Global Internet Community as Contract with U.S. Government Ends*. ICANN. https://www.icann.org/en/announcements/details/stewardship-of-iana-functions-transitions-to-global-internet-community-as-contract-with-us-government-ends-1-10-2016-en
Inkster, N. (2019). The Huawei Affair and China's Technology Ambitions. *Survival*, *61*(1), 105–111. https://doi.org/10.1080/00396338.2019.1568041
ISO. (n.d.). *Members: SAC*. International Organization for Standardization. Retrieved May 27, 2021, from https://www.iso.org/member/1635.html
ITU. (n.d.). *The Root zone file and the root server system*. International Telecommunications Union. Retrieved April 25, 2021, from https://www.itu.int/itunews/manager/display.asp?lang=en&year=2005&issue=06&ipage=root&ext=html
Jaipragas, B. (2017, March 22). Alibaba launches Malaysian hub for electronic world trade platform – and plans a 'new Silk Road.' *South China Morning Post*. https://www.scmp.com/business/companies/article/2081154/alibaba-launches-malaysian-hub-electronic-world-trade-platform
Jia, L., & Winseck, D. (2018). The political economy of Chinese internet companies: Financialization, concentration, and capitalization. *International Communication Gazette*, *80*(1), 30–59. https://doi.org/10.1177/1748048517742783
Jing, M. (2018, September 15). China to boost its 'national team' to meet goal of global AI leadership by 2030. *South China Morning Post*. https://www.scmp.com/tech/innovation/article/2173345/china-boost-its-national-team-meet-goal-global-ai-leadership-2030
Jing, M., & Dai, S. (2017, November 21). China recruits Baidu, Alibaba and Tencent to AI 'national team.' *South China Morning Post*. https://www.scmp.com/tech/china-tech/article/2120913/china-

recruits-baidu-alibaba-and-tencent-ai-national-team
Joerges, B. (1988). Large Technical Systems: Concepts and Issues. In R. Mayntz & T. P. Hughes (Eds.), *The Development of Large Technical Systems* (pp. 9–36). Campus Verlag.
Johannesson, P., & Perjons, E. (2014). An introduction to design science. In P. Johannesson & E. Perjons (Eds.), *An Introduction to Design Science* (pp. 39–73). Springer International Publishing. https://doi.org/10.1007/978-3-319-10632-8
Johnson, B. (2010, March 22). Google stops censoring Chinese search engine: How it happened. *The Guardian*. https://www.theguardian.com/technology/blog/2010/mar/22/google-china-live
Johnson, B., & Katz, I. (2010, March 24). Google co-founder Sergey Brin urges US to act over China web censorship. *The Guardian*. https://www.theguardian.com/technology/2010/mar/24/google-china-sergey-brin-censorship
Jolly, J. (2018, November 28). New Zealand blocks Huawei imports over 'significant security risk.' *The Guardian*. https://www.theguardian.com/business/2018/nov/28/new-zealand-blocks-huawei-5g-equipment-on-security-concerns
Joyce, D. (2015). Internet freedom and human rights. *European Journal of International Law*, *26*(2), 493–514. https://doi.org/10.1093/ejil/chv021
Kaghan, W. N., & Bowker, G. C. (2001). Out of machine age?: complexity, sociotechnicalsystems and actor network theory. *Journal of Engineering and Technology Management*, *18*, 253–269.
Kahn, J. (2005, September 8). Yahoo helped Chinese to prosecute journalist. *The New York Times*. https://www.nytimes.com/2005/09/08/business/worldbusiness/yahoo-helped-chinese-to-prosecute-journalist.html
Kaiman, J. (2013, September 10). China cracks down on social media with threat of jail for "online rumours." *The Guardian*. https://www.theguardian.com/world/2013/sep/10/china-social-media-jail-rumours
Kang, C., & Sanger, D. E. (2019, May 15). Huawei Is a Target as Trump Moves to Ban Foreign Telecom Gear. *New York Times*. https://www.nytimes.com/2019/05/15/business/huawei-ban-trump.html
Keane, S. (2019, June 13). *Huawei exclusion from 5G sends "bad signal," Chinese ambassador warns UK*. CNET. https://www.cnet.com/news/chinese-ambassador-warns-britain-huawei-exclusion-from-5g-sends-bad-signal/
Kennedy, A. B., & Lim, D. J. (2018). The innovation imperative: Technology and US-China rivalry in the twenty-first century. *International Affairs*, *94*(3), 553–572. https://doi.org/10.1093/ia/iiy044
Kessler, G. (2016, September 21). Cruz's claim that ICANN's transition will empower foes to censor the Internet. *Washington Post*. https://www.washingtonpost.com/news/fact-checker/wp/2016/09/21/cruzs-claim-that-icanns-transition-will-empower-foes-to-censor-the-internet/?variant=116ae929826d1fd3
Kharpal, A. (2019, January 15). Huawei CEO: We would refuse a Chinese government request for user data. *CNBC*. https://www.cnbc.com/2019/01/15/huawei-ceo-we-would-refuse-a-chinese-government-request-for-user-data.html
Kharpal, A. (2020, April 26). Power is 'up for grabs': Behind China's plan to shape the future of next-generation tech. *CNBC*. https://www.cnbc.com/2020/04/27/china-standards-2035-explained.html
King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review*, *107*(2), 326–343. https://doi.org/10.1017/S0003055413000014
Kist, R. (2015, November 9). Dit is de Chinese versie van internet. *NRC*.

https://www.nrc.nl/nieuws/2015/11/09/dit-is-de-chinese-versie-van-internet-a1494574
Knight, W. (2002, September 13). *On-off access for Google in China*. New Scientist. https://www.newscientist.com/article/dn2795-on-off-access-for-google-in-china/
Köhler, J., Geels, F. W., Kern, F., Markard, J., Onsongo, E., Wieczorek, A., Alkemade, F., Avelino, F., Bergek, A., Boons, F., Fünfschilling, L., Hess, D., Holtz, G., Hyysalo, S., Jenkins, K., Kivimaa, P., Martiskainen, M., McMeekin, A., Mühlemeier, M. S., … Wells, P. (2019). An agenda for sustainability transitions research: State of the art and future directions. *Environmental Innovation and Societal Transitions*, *31*, 1–32. https://doi.org/10.1016/j.eist.2019.01.004
Koty, A. C. (2020, July 2). *What is the China Standards 2035 Plan and How Will it Impact Emerging Industries?* China Briefing. https://www.china-briefing.com/news/what-is-china-standards-2035-plan-how-will-it-impact-emerging-technologies-what-is-link-made-in-china-2025-goals/
Kozłowski, K. (2018). BRI and its digital dimension: twists and turns. *Journal of Science and Technology Policy Management*. https://doi.org/10.1108/JSTPM-06-2018-0062
Kuchinke, B. A., & Vidal, M. (2016). Exclusionary strategies and the rise of winner-takes-it-all markets on the Internet. *Telecommunications Policy*, *40*(6), 582–592. https://doi.org/10.1016/j.telpol.2016.02.009
Latour, B. (1999). On Recalling Ant. *The Sociological Review*, *47*(1_suppl), 15–25. https://doi.org/10.1111/j.1467-954x.1999.tb03480.x
Lau, J. (2010, July 9). A history of Google in China. *Financial Times*. http://ig-legacy.ft.com/content/faf86fbc-0009-11df-8626-00144feabdc0#axzz6j3o6pf22
Layton, R. (2020, September 4). State Department's 5G Clean Network Club Gains Members Quickly. *Forbes*. https://www.forbes.com/sites/roslynlayton/2020/09/04/state-departments-5g-clean-network-club-gains-members-quickly/?sh=586c90ef7536
Lee, D. (2016, October 1). Has the US just given away the internet? *BBC News*. https://www.bbc.com/news/technology-37527719
Lee, J.-A. (2018). *Great Firewall* (No. 2018–10; The Chinese University of Hong Kong Faculty of Law Research Paper).
Lee, K., & Ho, M. (2014). The Maoming Anti-PX Protest of 2014. *China Perspectives*, *2014*(3), 33–39. https://doi.org/10.4000/chinaperspectives.6537
Lei, Y. W. (2011). The political consequences of the rise of the internet: Political beliefs and practices of Chinese Netizens. *Political Communication*, *28*(3), 291–322. https://doi.org/10.1080/10584609.2011.572449
Leskin, P. (2019, October 10). *Here are all the major US tech companies blocked behind China's "Great Firewall."* Business Insider. https://www.businessinsider.nl/major-us-tech-companies-blocked-from-operating-in-china-2019-5?international=true&r=US
Levy, S. (2011). *In The Plex: How Google Thinks, Works, and Shapes Our Lives*. Simon & Schuster.
Li, C. (2015, January 9). *Sogou's New Chinese Input Method Integrated Search*. China Internet Watch. https://www.chinainternetwatch.com/11772/sougo-chinese-input-method-launched-new-version-obtain-traffic-for-sogou-search/
Li, K. (2010, July 9). Google confident of China licence renewal. *Financial Times*. https://www.ft.com/content/ec5a1d4a-8afe-11df-bead-00144feab49a
Li, S. (2018). Exploring the relationships between freedom of information and institutional information management in the Chinese government: An empirical study. *Proceedings of the Association for Information Science and Technology*, *55*(1), 859–861.

https://doi.org/10.1002/pra2.2018.14505501148
Liang, B., & Lu, H. (2010). Internet development, censorship, and cyber crimes in China. *Journal of Contemporary Criminal Justice*, *26*(1), 103–120. https://doi.org/10.1177/1043986209350437
Liebowitz, S. J., & Margolis, S. E. (1995). Path Dependence, Lock-in, and History. *Journal of Law, Economics, and Organization*, *11*(1), 205–226. https://doi.org/10.2139/ssrn.1706450
Lin, L., Wang, W., Gan, C., Cohen, D. A., & Nguyen, Q. T. . (2019). Rural Credit Constraint and Informal Rural Credit Accessibility in China. *Sustainability*, *11*(7), 1935. https://doi.org/10.3390/su11071935
Lin, T. T. C. (2012). Prospect of mobile TV broadcasting in china: Socio-technical analysis of CMMB's development. *Chinese Journal of Communication*, *5*(1), 88–108. https://doi.org/10.1080/17544750.2011.640543
Lindsay, J. R., Cheung, T. M., & Reveron, D. S. (Eds.). (2015). *China and Cubersecurity: Espionage, Strategy, and Politics in the Digital Domain*. Oxford University Press.
Liu, T., & Woo, W. T. (2018). Understanding the U.S.-China Trade War. *China Economic Journal*, *11*(3), 319–340. https://doi.org/10.1080/17538963.2018.1516256
Liyakasa, K. (2015, June 23). *Alibaba CEO: 'We're Not Just An Ecommerce Company – We're A Data Company.'* AdExchanger. https://www.adexchanger.com/ecommerce-2/alibaba-ceo-were-not-just-an-ecommerce-company-were-a-data-company/
Ljunggren, D. (2020, August 25). Canada has effectively moved to block China's Huawei from 5G, but can't say so. *Reuters*. https://www.reuters.com/article/us-canada-huawei-analysis-idUSKBN25L26S
Lobato, R. (2016). Introduction: The New Video Geography. In R. Lobato & J. Meese (Eds.), *Geoblocking and Global Video Culture*. Institute of Network Cultures.
Lubman, S. (2013, September 17). The "Legalization" of China's Internet Crackdown. *Wall Street Journal*. https://www.wsj.com/articles/BL-CJB-18898
Lukman, E. (2013, July 2). *Lionel Messi: WeChat Hires World's Best Footballer as TV Ad Star*. Tech in Asia. https://www.techinasia.com/wechat-lionel-messi-ad
Lum, T. (2006). *Internet Development and Information Control in the People's Republic of China*.
Ma, B. (2020). *Understanding Family Businesses in China: the Path, the Trend, and the Future*.
Makinen, J., Yang, Y., & Li, A. (2015, December 15). "Freedom requires strict order": China preps for second World Internet Conference. *Los Angeles Times*. https://www.latimes.com/world/asia/la-fg-china-internet-20151215-story.html
Mascitelli, B., & Chung, M. (2019). Hue and cry over Huawei: Cold war tensions, security threats or anti-competitive behaviour? *Research in Globalization*, *1*, 100002. https://doi.org/10.1016/j.resglo.2019.100002
Mayring, P. (2002). *Einführung in die qualitative Sozialforschung* (5th ed.). Beltz.
McHugh, J. (2003, January 1). *Google vs. Evil*. Wired. https://www.wired.com/2003/01/google-10/
McLaughlin, A. (2006, January 27). *Google in China*. Official Google Blog. https://googleblog.blogspot.com/2006/01/google-in-china.html
Melnik, J. (2019). China's "National Champions" Alibaba, Tencent, and Huawei. *Education About Asia*, *24*(2), 28–33. https://tinyurl.com/y3vkvzd5.
Miao, W., & Lei, W. (2016). Policy review: The Cyberspace Administration of China. *Global Media and Communication*, *12*(3), 337–340. https://doi.org/10.1177/1742766516680879
Miao, W., Zhu, H., & Chen, Z. (2018). Who's in charge of regulating the Internet in China: The history and evolution of China's Internet regulatory agencies. *China Media Research*, *14*(3), 1–7.

Mina, A. X. (2014). Batman, pandaman and the blind man: A case study in social change memes and internet censorship in china. *Journal of Visual Culture*, *13*(3), 359–375. https://doi.org/10.1177/1470412914546576

Ministry of Foreign Affairs of the People's Republic of China. (2015, December 16). *Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference*. Ministry of Foreign Affairs of the People's Republic of China. https://www.fmprc.gov.cn/mfa_eng/wjdt_665385/zyjh_665391/t1327570.shtml

Mondschein, J., Clark-Ginsberg, A., & Kuehn, A. (2021). Smart cities as large technological systems: Overcoming organizational challenges in smart cities through collective action. *Sustainable Cities and Society*, *67*(January), 102730. https://doi.org/10.1016/j.scs.2021.102730

Montag, C., Becker, B., & Gan, C. (2018). The Multipurpose Application WeChat: A Review on Recent Research. *Frontiers in Psychology*, *9*, 2247. https://doi.org/10.3389/fpsyg.2018.02247

Moon, A. (2019, May 19). Exclusive: Google suspends some business with Huawei after Trump blacklist - source. *Reuters*. https://www.reuters.com/article/us-huawei-tech-alphabet-exclusive/exclusive-google-suspends-some-business-with-huawei-after-trump-blacklist-source-idUSKCN1SP0NB

Mou, Y., Wu, K., & Atkin, D. (2016). Understanding the use of circumvention tools to bypass online censorship. *New Media & Society*, *18*(5), 837–856. https://doi.org/10.1177/1461444814548994

Mueller, M. L. (2011). China and Global Internet Governance: A Tiger by the Tail. In R. J. Deibert, J. Palfrey, R. Rohozinski, & J. L. Zittrain (Eds.), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace* (pp. 177–194). MIT Press.

Mueller, M. L. (2012, May 24). *Threat Analysis of ITU's WCIT (Part 1): Historical context*. Internet Governance Project. https://www.internetgovernance.org/2012/05/24/threat-analysis-of-itus-wcit-part-1-historical-context/

Murgia, M., & Gross, A. (2020, March 27). Inside China' s controversial mission to reinvent the internet. *Financial Times*. https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f

Musil, S. (2018, June 6). *Facebook gave Huawei special access to user data*. CNET. https://www.cnet.com/news/facebook-reportedly-gave-huawei-special-access-to-user-data/

Negro, G. (2020). A history of Chinese global Internet governance and its relations with ITU and ICANN. *Chinese Journal of Communication*, *13*(1), 104–121. https://doi.org/10.1080/17544750.2019.1650789

NETmundial. (n.d.). *NETmundial: the beginning of a process.* NETmundial. Retrieved May 26, 2021, from https://netmundial.br/about/

Nicola, S. (2019, March 19). Merkel Takes a Stand Against U.S. Pressure to Bar Huawei From 5G. *Bloomberg*. https://www.bloomberg.com/news/articles/2019-03-19/merkel-takes-a-stand-against-u-s-pressure-to-bar-huawei-from-5g

Nicolaci da Costa, A. (2019, April 22). Why the US-China rivalry will not end with a trade deal. *BBC*. https://www.bbc.com/news/business-47848861

Nieva, R. (2018, June 7). *Congress calls out Google over ties with Huawei*. CNET. https://www.cnet.com/news/congress-calls-out-google-over-ties-with-huawei/

Ning, N. (2007, March 8). .cn domain name costs 1 yuan. *China Daily*. http://www.chinadaily.com.cn/bizchina/2007-03/08/content_822992.htm

O'Hara, K., & Hall, W. (2018). Four Internets: The Geopolitics of Digital Governance. *CIGI Papers*, *206*. https://www.cigionline.org/sites/default/files/documents/Paper no.206web.pdf

Ou, C. X., & Davison, R. M. (2009). Why eBay Lost to TaoBao in China: The Glocal Advantage.

Communications of the ACM, *52*(1), 145–148. https://doi.org/10.1145/1435417.1435450
PA Media. (2020, November 30). Huawei: UK bans new 5G network equipment from September. *The Guardian*. https://www.theguardian.com/technology/2020/nov/30/huawei-uk-bans-new-5g-network-equipment-from-september
Palladino, N., & Santaniello, M. (2021). IANA Functions, ICANN, and the DNS War. In N. Palladino & M. Santaniello (Eds.), *Legitimacy, Power, and Inequalities in the Multistakeholder Internet Governance*. Palgrave Macmillan. https://doi.org/https://doi.org/10.1007/978-3-030-56131-4_3
Pancevski, B., & Germano, S. (2019, March 11). Drop Huawei or See Intelligence Sharing Pared Back, U.S. Tells Germany. *Wall Street Journal*. https://www.wsj.com/articles/drop-huawei-or-see-intelligence-sharing-pared-back-u-s-tells-germany-11552314827
Parkhe, A. (1993). "Messy" Research, Methodological Predispositions, and Theory Development in International Joint Ventures. *Academy of Management Review*, *18*(2), 227–268. https://doi.org/10.5465/amr.1993.3997515
Petty, M., Morales, N. J., & Lema, K. (2019, March 1). Pompeo says world should have eyes wide open about Chinese tech risks. *Reuters*. https://www.reuters.com/article/us-philippines-usa-technology-china-idUSKCN1QI3FV
Pinchuk, D. (2012, June 23). Huawei denies using Chinese subsidies to grab more business. *Reuters*. https://www.reuters.com/article/us-china-huawei-subsidies-idUSBRE85M02U20120623
Pompeo, M. R. (2019, December 2). Europe must put security first with 5G. *Politico*. https://www.politico.eu/article/europe-must-put-security-first-with-5g-mike-pompeo-eu-us-china/
Pompeo, M. R. (2020a, April 29). *Secretary Michael R. Pompeo At a Press Availability*. United States Department of State. https://2017-2021.state.gov/secretary-michael-r-pompeo-at-a-press-availability-4/index.html
Pompeo, M. R. (2020b, August 5). *Secretary Michael R. Pompeo At a Press Availability*. United States Department of State. https://2017-2021.state.gov/secretary-michael-r-pompeo-at-a-press-availability-10/index.html
Puel, G., & Fernandez, V. (2012). Socio-technical Systems, Public Space and Urban Fragmentation: The Case of "Cybercafés" in China. *Urban Studies*, *49*(6), 1297–1313. https://doi.org/10.1177/0042098011410333
Qian, X. (2019). Cyberspace Security and U.S. - China Relations. *2019 International Conference on Artificial Intelligence and Computer Science*, 709–712.
Qiang, C. Z.-W., Bhavnani, A., Hanna, N. K., Kimura, K., & Sudan, R. (2009). Rural Informatization in China. In *World Bank Working Paper* (No. 172).
Qiu, J. L. (1999). Virtual Censorship in China: Keeping the Gate Between the Cybersapces. *International Journal of Communications Law and Policy*, *4*(1), 1–25.
Qiu, W. (2011, March 19). *Submarine Cables Cut after Taiwan Earthquake in Dec 2006*. Submarine Networks. https://www.submarinenetworks.com/news/cables-cut-after-taiwan-earthquake-2006
Rao, L. (2015, September 25). *Jack Ma and Jerry Yang talk about Yahoo's big Alibaba investment*. Fortune. https://fortune.com/2015/09/25/yahoo-alibaba-investment-jack-ma/
Reddy, S. K., Wang, Z. Z., & Dong, D. H. (2015). China's Digital Landscape : Breaking Barriers to Innovation. *Asian Management Insights*, *2*(2), 18–23. https://ink.library.smu.edu.sg/lkcsb_research
Reuters. (2010, March 21). China state media accuses Google of political agenda. *Reuters*. https://www.reuters.com/article/idUSTRE62K0A120100321
Reuters. (2021, February 26). Brazil regulator approves 5G spectrum auction rules, no Huawei ban.

Reuters. https://www.reuters.com/business/media-telecom/brazil-regulator-approves-5g-spectrum-auction-rules-no-huawei-ban-2021-02-26/

Rifkin, J. (2014). *The zero marginal cost society: The internet of things, the collaborative commons, and the eclipse of capitalism*. St. Martin's Press.

Roberts, Hal, Zuckerman, E., & Palfrey, J. (2011). *2011 Circumvention Tool Evaluation*. http://www.rand.org/pubs/rgs_dissertations/RGSD127.html.

Roberts, Huw, Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI and Society*, *36*(1), 59–77. https://doi.org/10.1007/s00146-020-00992-2

Roberts, M. E. (2018). Censored: Distraction and Diversion Inside China's Great Firewall. In *Censored*. Princeton University Press. https://doi.org/10.23943/9781400890057

Rolland, N. (2015, April 2). *A Fiber-Optic Silk Road*. The Diplomat. https://thediplomat.com/2015/04/a-fiber-optic-silk-road/

Rongji, Z. (2010). Measures for the Management of Internet Information Services. *Chinese Law and Government*, *43*(5), 30–35. https://doi.org/10.2753/CLG0009-4609430504

Rühlig, T. N. (2020). *Technical standardisation, China and the future international order: A European perspective*.

Rutherford, J., & Coutard, O. (2014). Urban Energy Transitions: Places, Processes and Politics of Socio-technical Change. *Urban Studies*, *51*(7), 1353–1377. https://doi.org/10.1177/0042098013500090

Sabbagh, D., & Kuo, L. (2020, July 14). Huawei to be stripped of role in UK's 5G network by 2027, Dowden confirms. *The Guardian*. https://www.theguardian.com/technology/2020/jul/14/huawei-to-be-stripped-of-role-in-uk-5g-network-by-2027-dowden-confirms

Sahari, S. (2017, June 14). *The root of a robust Internet*. Asia-Pacific Network Information Centre. https://blog.apnic.net/2017/06/14/root-robust-internet/

Salinas, S. (2018, February 13). TECH Six top US intelligence chiefs caution against buying Huawei phones. *CNBC*. https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html

Schlæger, J., & Jiang, M. (2014). Official microblogging and social management by local governments in China. *China Information*, *28*(2), 189–213. https://doi.org/10.1177/0920203X14533901

Schlenzig, N. (2020, March 13). *The Belt and Rebranding Initiative*. Lowy Institute. https://www.lowyinstitute.org/the-interpreter/belt-and-rebranding-initiative

Schmidt, E., Work, E., Catz, S., Horvitz, E., Chien, S., Jassy, A., Clyburn, M., Louie, G., Darby, C., Mark, W., Ford, K., Matheny, J., Griffiths, J.-M., McFarland, K., & Moore, A. (2021). *Final Report - National Security Commission on Artificial Intelligence*.

Schubert, C., Sydow, J., & Windeler, A. (2013). The means of managing momentum: Bridging technological paths and organisational fields. *Research Policy*, *42*, 1389–1405. https://doi.org/10.1016/j.respol.2013.04.004

Schuller, K. (2019, April 7). USA verlangen von Deutschland keinen Huawei-Bann mehr. *Frankfurter Algemeine*. https://www.faz.net/aktuell/politik/inland/usa-verlangen-von-deutschland-keinen-huawei-bann-mehr-16128222.html

Seaman, J. (2020). *China and the New Geopolitics of Technical Standardization* (Issue January). French Institute of International Relations: Center for Asian Studies & Policy Center for the New South. https://doi.org/10.1093/oso/9780190680190.003.0001

Seawnght, J., & Gerring, J. (2008). Case selection techniques in case study research: A menu of

qualitative and quantitative options. *Political Research Quarterly*, *61*(2), 294–308. https://doi.org/10.1177/1065912907313077

Segal, A. (2020). *China's Vision for Cyber Sovereignty and the Global Governance of Cyberspace* (N. Rolland (Ed.); Vol. 87). https://www.nbr.org/wp-content/uploads/pdfs/publications/sr87_aug2020.pdf

Serpstat. (n.d.). *Which search engines are the most popular on the Internet: a comparison of regions*. Serpstat. Retrieved May 31, 2021, from https://serpstat.com/blog/which-search-engines-are-the-most-popular-on-the-internet-a-comparison-of-regions/

SESEC. (2018, May 24). *24/05/2018 Chinese Standards 2035, the standardization strategy research is kicked off*. Seconded European Standardization Expert for China. https://sesec.eu/2018/news-events/news/24-05-2018-chinese-standards-2035-the-standardization-strategy-research-is-kicked-off/

Shapiro, C., & Varian, H. R. (1998). *Information Rules: a Strategic Guide to the Network Economy*. Harvard Business Press. https://doi.org/10.1145/776985.776997

Sharp, H., & Kolkman, O. (2020). *Discussion Paper: An analysis of the "New IP" proposal to the ITU-T*. https://www.internetsociety.org/wp-content/uploads/2020/04/ISOC-Discussion-Paper-NewIP-analysis-29April2020.pdf

Shen, H. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication*, *9*(3), 304–324. https://doi.org/10.1080/17544750.2016.1206028

Shen, H. (2018). Building a Digital Silk Road? Situating the Internet in China's Belt and Road Initiative. *International Journal of Communication*, *12*, 2683–2701.

Shepardson, D. (2020, October 27). U.S. appeals court rejects immediate WeChat ban. *Reuters*. https://www.reuters.com/article/usa-wechat-idUSKBN27C059

Shepardson, D. (2021, January 26). Biden Commerce nominee vows to protect U.S. networks from Huawei, ZTE. *Reuters*. https://www.reuters.com/article/us-usa-biden-commerce-idUSKBN29V119

Shida, Y., & Takemoto, Y. (2018, December 7). Japan government to halt buying Huawei, ZTE equipment: sources. *Reuters*. https://www.reuters.com/article/us-japan-china-huawei/japan-government-to-halt-buying-huawei-zte-equipment-sources-idUSKBN1O600X

Shove, E., Pantzar, M., & Watson, M. (2012). *The Dynamics of Social Practice: Everyday Life and how it Changes*. SAGE Publications Inc.

Smith, T. (2019, June 25). *How The Triffin Dilemma Affects Currencies*. Investopedia. https://www.investopedia.com/financial-edge/1011/how-the-triffin-dilemma-affects-currencies.aspx

So, S., & Westland, J. C. (2009). *Red Wired: China's Internet Revolution* (1st ed.). Marshall Cavendish Limited.

Soo, Z. (2016, December 2). ZTE to play integral role in creating 'information superhighway' to connect One Belt, One Road countries. *South China Morning Post*. https://www.scmp.com/business/article/2051219/zte-play-integral-role-creating-information-superhighway-connect-one-belt

Sovacool, B. K., & Hess, D. J. (2017). Ordering theories: Typologies and conceptual frameworks for sociotechnical change. *Social Studies of Science*, *47*(5), 703–750. https://doi.org/10.1177/0306312717709363

Sovacool, B. K., Hess, D. J., Amir, S., Geels, F. W., Hirsh, R., Rodriguez Medina, L., Miller, C., Alvial Palavicino, C., Phadke, R., Ryghaug, M., Schot, J., Silvast, A., Stephens, J., Stirling, A., Turnheim, B., van der Vleuten, E., van Lente, H., & Yearley, S. (2020). Sociotechnical agendas: Reviewing

future directions for energy and climate research. *Energy Research & Social Science*, *70*(December), 101617. https://doi.org/10.1016/j.erss.2020.101617

Srivastava, P., & Hopwood, N. (2009). A Practical Iterative Framework for Qualitative Data Analysis. *International Journal of Qualitative Methods*, *8*(1), 76–84. https://doi.org/10.1177/160940690900800107

Standartisation Administration of China. (2020). *Notice of Standardisation Administration of China on Releasing "Main Points of National Standardisation Work in 2020."* https://www.sesec.eu/app/uploads/2020/04/Main-Points-of-National-Standardisation-Work-in-2020.pdf

State Council. (2015a, March 13). *Internet Plus: Premier Li's new tech tool*. The State Council of the People's Republic of China. http://english.www.gov.cn/premier/news/2015/03/13/content_281475070887811.htm

State Council. (2015b, June 25). *Premier urges use of Internet Plus to boost growth*. The State Council of the People's Republic of China. http://english.www.gov.cn/premier/news/2015/06/25/content_281475134144826.htm

Stevens, T. (2015, July 1). *BRICS vision for international information security*. Thesigers. http://thesigers.com/analysis/2015/7/3/brics-set-out-vision-for-international-information-security

Stirland, S. L. (2008, May 20). *Cisco Leak: "Great Firewall" of China Was a Chance to Sell More Routers*. WIRED. https://www.wired.com/2008/05/leaked-cisco-do/

Sun, Y., Von Zedtwitz, M., & Simon, D. F. (2007). Globalization of R&D and China: An introduction. *Asia Pacific Business Review*, *13*(3), 311–319. https://doi.org/10.1080/13602380701291867

Swanson, A. (2020, August 7). Trump's Orders on WeChat and TikTok Are Uncertain. That May Be the Point. *The New York Times*. https://www.nytimes.com/2020/08/07/business/economy/trump-executive-order-tiktok-wechat.html

Tai, Q. (2014). China's media censorship: A Dynamic and diversified regime. *Journal of East Asian Studies*, *14*(2), 185–209. https://doi.org/10.1017/s1598240800008900

Tamma, P. (2020, October 15). Europe wants 'strategic autonomy' — it just has to decide what that means. *POLITICO*. https://www.politico.eu/article/europe-trade-wants-strategic-autonomy-decide-what-means/

Tan, J., & Tan, A. E. (2012). Business Under Threat, Technology Under Attack, Ethics Under Fire: The Experience of Google in China. *Journal of Business Ethics*, *110*(4), 469–479. https://doi.org/10.1007/s10551-012-1494-0

Tan, J., Wang, L., Zhang, H., & Li, W. (2020). Disruptive innovation and technology ecosystem: The evolution of the intercohesive public – private collaboration network in Chinese telecommunication industry. *Journal of Engineering and Technology Management*, *57*. https://doi.org/10.1016/j.jengtecman.2020.101573

Tan, Z. (1999). Regulating China's Internet: Convergence toward a coherent regulatory regime. *Telecommunications Policy*, *23*(3), 261–276. https://doi.org/10.1016/S0308-5961(99)00007-5

Tannen, D. (1993). *Framing in Discourse*. Oxford University Press.

TASS. (2016, June 17). Alibaba plans to expand business in Russia — Jack Ma. *TASS*. https://tass.com/economy/882894

Taubman, G. (1998). A Not-So World Wide Web: The Internet, China, and the Challenges to Nondemocratic Rule. *Political Communication*, *15*(2), 255–272. https://doi.org/10.1080/10584609809342369

TelecomLead. (2018, December 7). *Huawei grabs 28% share in global telecom equipment market*. TelecomLead. https://www.telecomlead.com/telecom-equipment/huawei-grabs-28-share-in-global-telecom-equipment-market-87863

The Associated Press. (2004, June 16). Technology Briefing | Deals: Google Takes Stake In Chinese Search Engine. *The New York Times*. https://www.nytimes.com/2004/06/16/business/technology-briefing-deals-google-takes-stake-in-chinese-search-engine.html?scp=33&sq=google+china&st=nyt

The Economist. (2017, April 20). China's internet giants go global. *The Economist*. https://www.economist.com/business/2017/04/20/chinas-internet-giants-go-global

The Guardian. (2002, September 4). China blocks Google as congress looms. *The Guardian*. https://www.theguardian.com/technology/2002/sep/04/internetnews.china

Thompson, C. (2006, April 23). Google's China Problem (and China's Google Problem). *The New York Times*. https://www.nytimes.com/2006/04/23/magazine/googles-china-problem-and-chinas-google-problem.html

Thomson, E., & Sigurdson, J. (2008). *China's Science and Technology Sector and the Forces of Globalization*. World Scientific.

Traynor, I. (2014, February 12). Internet governance too US-centric, says European commission. *The Guardian*. https://www.theguardian.com/technology/2014/feb/12/internet-governance-us-european-commission

Tsui, L. (2003). The Panopticon as the Antithesis of a Space of Freedom: Control and Regulation of the Internet in China. *China Information*, *17*(2), 65–82.

Tu, F. (2016). WeChat and civil society in China. *Communication and the Public*, *1*(3), 343–350. https://doi.org/10.1177/2057047316667518

US Department of State. (n.d.). *The Clean Network*. US Department of State. Retrieved May 3, 2021, from https://2017-2021.state.gov/the-clean-network/index.html

Van Boom, D. (2018, February 14). *Don't use phones from Huawei or ZTE, FBI director says*. CNET. https://www.cnet.com/news/huawei-zte-fbi-chris-wray-nsa/

Van der Aalst, W., Hinz, O., & Weinhardt, C. (2019). Big Digital Platforms Growth, Impact, and Challenges. *Business & Information Systems Engineering*, *61*(6), 645–648. https://doi.org/10.1007/s12599-019-00618-y

van der Vleuten, E. (2004). Infrastructures and Societal Change. A View from the Large Technical Systems Field. *Technology Analysis & Strategic Management*, *16*(3), 395–414. https://doi.org/10.1080/0953732042000251160

Van der Vleuten, E. (2009). Large Technical Systems. In J. K. B. Olsen, S. A. Pedersen, & V. F. Hendricks (Eds.), *A Companion to the Philosophy of Technology* (pp. 218–222). Blackwell Publishing Ltd. https://doi.org/10.1002/9781444310795.ch39

van der Vleuten, E., & Högselius, P. (2012). Resisting Change? The Transnational Dynamics of European Energy Regimes. In G. Verbong & D. Loorbach (Eds.), *Governing the energy transition: Reality, Illusion, or Necessity?* (pp. 75–100). Routledge.

van der Vleuten, E., & Kaijser, A. (2005). Networking Europe. *History and Technology*, *21*(1), 21–48. https://doi.org/10.1080/07341510500037495

van der Vleuten, E., & Kaijser, A. (2006). *Networking Europe: Transnational Infrastructures and the Shaping of Europe, 1850-2000*. Science History Publications.

Vascellaro, J. E. (2010, March 24). Brin Drove Google to Pull Back in China. *Wall Street Journal*. https://www.wsj.com/articles/SB10001424052748704266504575141064259998090

Velasquez, M. (2009). Development, justice, and technology transfer in China:The case of HP and Legend. *Journal of Business Ethics*, *89*(2), 157–166. https://doi.org/10.1007/s10551-010-0373-9

Vila Seoane, M. F. (2020). Alibaba's discourse for the digital Silk Road: the electronic World Trade Platform and 'inclusive globalization.' *Chinese Journal of Communication*, *13*(1), 68–83. https://doi.org/10.1080/17544750.2019.1606838

Volz, D., & Chin, J. (2019, January 23). U.S. Believes It Doesn't Need to Show 'Proof' Huawei Is a Spy Threat. *Wall Street Journal*. https://www.wsj.com/articles/u-s-believes-it-doesnt-need-to-show-proof-huawei-is-a-spy-threat-11548288297?mod=article_inline

Wallach, O. (2020, December 23). *Visualizing Facebook's Global Social Network Monopoly*. Visual Capitalist. https://www.visualcapitalist.com/map-facebook-path-social-network-domination/

Wan, W. S., Dastane, O., Mohd Satar, N. S., & Ma'arif, M. K. (2019). What WeChat can Learn from WhatsApp? Customer Value Proposition Development for Mobile Social Networking (MSN) Apps: A Case Study Approach. *Journal of Theoretical and Applied Information Technology*, *97*(4).

Wang, D., & Mark, G. (2015). Internet Censorship in China: Examining User Awareness and Attitudes. *ACM Transactions on Computer-Human Interaction*, *22*(6), 1–22. https://doi.org/10.1145/2818997

Wang, H. H. (2010, September 12). How EBay Failed In China. *Forbes*. https://www.forbes.com/sites/china/2010/09/12/how-ebay-failed-in-china/?sh=74bacda55d57

Wang, J. (2020). *From Banning to Regulating TikTok: Addressing concerns of national security, privacy, and online harms*.

Wang, Y. (2020, September 1). In China, the "Great Firewall" is Changing a Generation. *POLITICO*. https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385

Waters, R., Hille, K., & Anderlini, J. (2010, January 14). Breaches push Google on back foot. *Financial Times*. https://www.ft.com/content/10f06734-fff1-11de-ad8c-00144feabdc0

Watts, J. (2006, January 25). Backlash as Google shores up great firewall of China. *The Guardian*. https://www.theguardian.com/technology/2006/jan/25/news.citynews

Watts, J. (2009, June 24). China blocks Google services. *The Guardian*. https://www.theguardian.com/world/2009/jun/24/google-china-censors

Weitzenboeck, E. M. (2014). Hybrid net: the regulatory framework of ICANN and the DNS. *International Journal of Law and Information Technology*, *22*(1), 49–73. https://doi.org/10.1093/ijlit/eat016

Wernberg-Tougaard, E. (2021, February 23). *China's AI champions*. China Experience. https://www.china-experience.com/china-experience-insights/chinas-ai-champions

Wheeler, A. (2020, February 19). *China's Digital Silk Road (DSR): the new frontier in the Digital Arms Race?* Silk Road Briefing. https://www.silkroadbriefing.com/news/2020/02/19/chinas-digital-silk-road-dsr-new-frontier-digital-arms-race/

Wildau, G. (2014, September 29). Alibaba affiliate wins approval for bank licence. *Financial Times*. https://www.ft.com/content/605c26bc-47d3-11e4-ac9f-00144feab7de

Wildau, G. (2015, January 5). Tencent launches China's first online-only bank. *Financial Times*. https://www.ft.com/content/ccc5a6dc-9488-11e4-82c7-00144feabdc0

Wilson, N. (2020, June 3). *China Standards 2035 and the Plan for World Domination—Don't Believe China's Hype*. Council on Foreign Relations. https://www.cfr.org/blog/china-standards-2035-and-plan-world-domination-dont-believe-chinas-hype

Wines, M. (2011, May 4). China Creates New Agency to Regulate the Internet. *New York Times*. https://www.nytimes.com/2011/05/05/world/asia/05china.html

Winner, L. (1980). Do Artifacts Have Politics? *Daedalus*, *109*(1), 121–136.
Winseck, D. (2017). The geopolitical economy of the global internet infrastructure. *Journal of Information Policy*, *7*, 228–267. https://doi.org/10.5325/jinfopoli.7.2017.0228
Wiseman, P. (2008, April 24). Cracking the "Great Firewall" of China's Web censorship. *ABC News*. https://abcnews.go.com/Technology/story?id=4707107&page=1
Wong, E. (2009, June 19). China Disables Some Google Functions. *The New York Times*. https://www.nytimes.com/2009/06/20/world/asia/20beijing.html
Wong, E. (2012, November 14). Ending Congress, China Presents New Leadership Headed by Xi Jinping. *The New York Times*. https://www.nytimes.com/2012/11/15/world/asia/communists-conclude-party-congress-in-china.html
Wu, J., & Lam, O. (2017, September 3). *The evolution of China's Great Firewall: 21 years of censorship*. Hong Kong Free Press. https://hongkongfp.com/2017/09/03/evolution-chinas-great-firewall-21-years-censorship/
Wu, T. S. (1997). Cyberspace Sovereignty? - The Internet and the International System. *Harvard Journal of Law & Technology*, *10*(3), 647–666.
Wu, W. (1996). Great leap or long march: Some policy issues of the development of the Internet in China. *Telecommunications Policy*, *20*(9), 699–711. https://doi.org/10.1016/S0308-5961(96)00050-X
Wu, X. (2005). *Chinese Cyber Nationalism: How China's online public sphere affected its social and political transitions*. University of Florida.
Wübbeke, J., Meissner, M., Zenglein, M. J., Ives, J., & Conrad, B. (2016). *Made in China 2025: The making of a high-tech superpower and consequences for industrial countries*.
Xia, B., & Fuchs, C. (2017). *The Financialisation of Digital Capitalism in China* (No. 4; Westminster Advanced Studies).
Xinhua. (2010, March 23). China: Google breaks promise, totally wrong to stop censoring. *China Daily*. https://www.chinadaily.com.cn/china/2010-03/23/content_9625554.htm
Xu, X., Mao, Z. M., & Halderman, J. A. (2011). Internet censorship in China: Where does the filtering occur? In N. Spring & G. F. Riley (Eds.), *International Conference onf Passive and Active Network Management* (pp. 133–142). Springer. https://doi.org/10.1007/978-3-642-19260-9
Xuetong, Y. (2020). Bipolar Rivalry in the Early Digital Age. *The Chinese Journal of International Politics*, *June*, 313–341. https://doi.org/10.1093/cjip/poaa007
Yan, X., & Huang, M. (2020). Leveraging university research within the context of open innovation: The case of Huawei. *Telecommunications Policy*, *March*. https://doi.org/10.1016/j.telpol.2020.101956
Yang, F., Yu, X., Liu, Y., & Yang, M. (2012). Automatic detection of rumor on Sina Weibo. *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 1–7. https://doi.org/10.1145/2350190.2350203
Yang, G. (2014). The Return of Ideology and the Future of Chinese Internet Policy. *Critical Studies in Media Communication*, *31*(2), 109–113. https://doi.org/10.1080/15295036.2014.913803
Yang, Q., & Ji, Y. (2016). The platform economy and natural monopoly: regulating or laissez-faire? *Fudan University, Shanghai*.
Yang, Y. (2018, March 5). China's WeChat hits 1bn user accounts worldwide. *Financial Times*. https://www.ft.com/content/8940f2d0-2059-11e8-a895-1ba1f72c2c11
Yang, Y., & Liu, X. (2018, January 2). Tencent denies storing WeChat conversations. *Financial Times*. https://www.ft.com/content/b12fdba6-ef9b-11e7-b220-857e26d1aca4
Yang, Z., Liu, H., Li, W., & Lv, X. (2012). The applied research on Internet of Things engineering

surveillance's records management. *2012 IEEE International Conference on Computer Science and Automation Engineering*, 689–693. https://doi.org/10.1109/ICSESS.2012.6269560

Yeo, S. (2016). Geopolitics of search: Google versus China? *Media, Culture and Society*, *38*(4), 591–605. https://doi.org/10.1177/0163443716643014

Yep, C.-W., Strumpf, D., Volz, D., O'Keeffe, K., & Viswanatha, A. (2019, May 25). Huawei's Yearslong Rise Is Littered With Accusations of Theft and Dubious Ethics. *Wall Street Journal*. https://www.wsj.com/articles/huaweis-yearslong-rise-is-littered-with-accusations-of-theft-and-dubious-ethics-11558756858

Yin, Q., & Li, X. (2020). Exploring the roles of government involvement and institutional environments in the internationalization of Chinese Internet companies. *Chinese Journal of Communication*, *13*(1), 47–67. https://doi.org/10.1080/17544750.2019.1653340

Yin, R. K. (2018). *Case study research and applications: Design and methods* (6th ed.). SAGE Publications.

Yuan, L. (2018, August 6). *A Generation Grows Up in China Without Google, Facebook or Twitter*. The New York Times. https://www.nytimes.com/2018/08/06/technology/china-generation-blocked-internet.html

Zeller, T. (2006, February 16). Web Firms Are Grilled on Dealings in China. *The New York Times*. https://www.nytimes.com/2006/02/16/technology/web-firms-are-grilled-on-dealings-in-china.html

Zeng, J., Stevens, T., & Chen, Y. (2017). China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of "Internet Sovereignty." *Politics & Policy*, *45*(3), 432–464. https://doi.org/10.1111/polp.12202

Zhang, H., Tang, Z., & Jayakar, K. (2018). A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-government services. *Telecommunications Policy*, *42*(5), 409–420. https://doi.org/10.1016/j.telpol.2018.02.004

Zhang, Lixuan, & Pentina, I. (2012). Motivations and Usage Patterns of Weibo. *Cyberpsychology, Behavior, and Social Networking*, *15*(6), 312–317. https://doi.org/10.1089/cyber.2011.0615

Zhang, Longmei, & Chen, S. (2019). China's Digital Economy: Opportunities and Risks. In *IMF Working Paper* (Vol. 16). https://doi.org/10.17323/1996-7845-2019-02-11

Zhang, P. (2020, July 6). *Huawei, ZTE hold 48.9 percent share of 5G telecom equipment market*. CnTechPost. https://cntechpost.com/2020/07/06/huawei-zte-hold-48-9-percent-share-of-5g-telecom-equipment-market/

Zhang, T. (2016, September 2). Alibaba's Jack Ma advocates the eWTP at G20 Hangzhou summit. *China's Daily Online*. http://en.people.cn/n3/2016/0902/c90000-9109449.html

Zhang, W. (1990). Fire and blood: Censorship and books in China. *International Library Review*, *22*(1), 61–72. https://doi.org/10.1016/0020-7837(90)90040-M

Zhao, H. (2015, July 27). Web companies asked to support "digital Silk Road." *The Telegraph*. https://www.telegraph.co.uk/sponsored/china-watch/technology/11764541/tech-companies-to-build-digital-silk-road.html

Zhao, S. (2015). A New Model of Big Power Relations? China–US strategic rivalry and balance of power in the Asia–Pacific. *Journal of Contemporary China*, *24*(93), 377–397. https://doi.org/10.1080/10670564.2014.953808

Zhao, Y., & Cao, Y. (2014, November 21). China wants its voice heard in cyberspace. *China Daily*. http://usa.chinadaily.com.cn/business/2014-11/21/content_18951166.htm

Zittrain, J. L., & Edelman, B. (2003). Internet Filtering in China. In *IEEE Internet Computing* (Issue

April).
Zittrain, J. L., Faris, R., Noman, H., Clark, J., Tilton, C., & Morrison-Westphal, R. (2017). The Shifting Landscape of Global Internet Censorship. In *Berkman Klein Center Research Publication* (No. 2017–4). https://doi.org/10.2139/ssrn.2993485