Department of International Relations

IR499 Dissertation in International Relations (2022/23)

Assessed thesis submitted in partial fulfilment of the requirements for the Masters in International Relations

Candidate Number: 43366

Number of Words (including footnotes): 9995

AFRI-CAN CHINA BAN PUNS IN ETHI-TROPE-IA?

EVALUATION OF CHINESE CYBER NORM PROMOTION THROUGH THE DIGITAL SILK ROAD IN ETHIOPIA

I have read and understood the School's rules on plagiarism and assessment offences and the work submitted is my own apart from properly referenced quotations.

TABLE OF CONTENTS

1. Introduction

1.1. Background

In 2014, China banned puns for fear of "cultural chaos" resulting from clever wordplay (Lubin, 2014). Though media titles are unlikely to lead to mass upheaval, the CCP finds censorship to be no laughing matter. Though China has been successful in maintaining its freedom to ban anything in cyberspace – any word – the question becomes: how successful are they in exporting this model to other nations?

The growing importance of cyberspace has made its governance an extreme point of contention, with cyberspace evolving into a foreign policy tool that can be wielded by the state. With a lack of clear territorial borders guiding cyberspace sovereignty, different states have taken the liberty to regulate the Internet differently, thereby producing a fragmented global Internet. China perceives the Internet as a threat to its stability but maintains that it is essential to development in the modern world. With a leading number of netizens and a growing information and technology sector (ICT), it is no surprise that Beijing would like to rise to primacy in global cyberspace (CNNIC, 2021). To complete this objective, China has made concerted efforts to promote its cyber norms, especially in response to the diverging Western conceptions of Internet freedom of speech and individual liberties.

In 2017, China inaugurated the Digital Silk Road as a new initiative that would be a crucial component of the BRI strategy to increase technological impact and shift the balance of geopolitical power towards China as a part of the Chinese Dream of National Rejuvenation (Kleinwachter, 2017). Though the main goal of the Digital Silk Road is to boost economic development by creating digital infrastructure, the DSR also allows China to participate in the global cyber environment whilst still enforcing social stability (Griffiths, 2018).

Driven largely by Chinese private companies, the DSR is a branding tool for Beijing to promote its strategic conception of technology (Agebi, 2022). China's involvement in Africa's

digital infrastructure came much before the beginnings of the DSR when Chinese private companies dispersed to African nations in 1999 (Ghiasy & Krishnamurthy, 2020). In this way, countries where Chinese companies have had significant contributions to African technological infrastructure are connected to the DSR whether or not it's formally under the BRI network(Greene & Triolo, 2020). Under the assumption that the DSR is merely a rebranding of China's strategic engagement in Africa's technology sector, it is clear that the influx of Chinese firms has had significant effects on not only Africa's physical telecoms industry but its conception of techno governance structurally, legally, and discursively (Vaidyanathan & Gomera, 2019). The arrival of global telecom companies such as ZTE in countries like Ethiopia has entered them into the global Internet system; with this comes a price: these companies are driving the digital development, creating a landscape for dependence on Chinese tech, and giving China an opportunity to set cyber norms.

1.2. Relevance

The central argument of this dissertation speaks to the current debates on the political, social, and normative questions that arise from the loose regulatory coordination of the Internet, especially within the context of two vastly different dominating cyber governance models. Though much of the current literature examines Chinese cyber norm promotion through international institutional means, such as regional coalition building in front of the UN (Fung, 2022; Flonk, 2021), or attempts to create an attractive alternative model to Western nations through economic private development (Shen, 2016; Demchak, 2016; Segal, 2020), there is a deficit in material on how China reconciles its diplomatic narratives of the BRI & DSR efforts to promote cyber norms of Internet sovereignty. Indeed, this topic is highly contentious: it has been argued that a Chinese model of the Internet might not even exist, much less that it can promote an alternative authoritarian version of the Internet (Gagliardone, 2021). Furthermore, very little of the current literature has framed Chinese cyber norm promotion through an analytical lens that emphasizes both discursive and material aspects of DSR infrastructure building, leaving the

specific chronology of African censorship building with Chinese characteristics largely unexplored.

This paper aims to use China's DSR involvement in Ethiopia to analyze China's cyber norm promotion in foreign nations. I utilize the theoretical framework of the cyber norm promotion cycle to illustrate China's aims and execution at advancing its cyber governance system. I seek to enhance the current discussion of China's attempts at cyber norm promotion through the Digital Silk Road by analyzing China's material and discursive attempts at promoting the China Dream, juxtaposing it to the Western multi-stakeholder model of cyber governance, and utilizing the case study of Ethiopia to process trace China's network development in Africa to subsequent censorship and Internet sovereignty norms.

Though the case study of Ethiopia is useful for understanding the direct link between Chinese DSR activity and host country government censorship and surveillance for cyber norm promotion, Ethiopia exists as an authoritarian regime and has experienced political turmoil, which problematizes the connection between Chinese investment and censorship norms. To address this weakness, I provide a brief section that examines a non-authoritarian regime in Africa where China has successfully promoted cyber norms and a Chinese private company that has been successful in transforming African cyber networks and discourse. Lastly, I conclude that though China cyber norm promotion has been successful in transforming Internet sovereignty in Africa, I offer the nuance that it is more of an unintended consequence of China's economic efforts rather than a concerted plan to shape African cyber ideals. Furthermore, it is helpful to consider that with the high variation in political, economic, and social contexts that exist in Africa, success of cyber norm promotion becomes dependent on the host country's political system and how early China established itself in the nation.

2. Methodology

2.1. Design

This dissertation utilizes a combination of textual analysis, historical tracing, and a case study to investigate China's cyber norm promotion capabilities to foreign nations. The following research questions are addressed: Within the context of the Digital Silk Road, to what extent are China's ambitions as a cyber norm entrepreneur of Internet sovereignty successful? Has China tried to promote an alternative model of cyber governance and how was it executed materially and discursively? In what ways did these nations transform as a result? This dissertation seeks to answer what constitutes cyber promotion and apply it to the country's attempts to fulfill the national rejuvenation of the Chinese nation through cyber means. Currently, most of the literature on Chinese cyber norm promotion focuses on investment along the BRI or qualitative examinations of the transformation of countries – but does not couple it with the role of norm entrepreneurship (Wang, 2020; Ly, 2020).

Most literature on Chinese cyber governance explores why nations are receptive to these norms. However, while these articles point out motivation for all parties involved (the Chinese government, Chinese private companies, host nation's legal systems, Western governance systems), it does not fully capture the theoretical progressions of norms, from conception to promotion, that is fundamentally intertwined with China's material attempts at cyber diplomacy (Greene & Triolo, 2020). This is why I have chosen to use a case study method to answer my research question.

My data collection consists of both primary and secondary data. I have employed online journal directories, collected government reports, looked at official releases of White Papers, and consulted legal codes to draw observable evidence for my research question. Qualitative methodology is the primary research method. Because cyber governance and norm promotion involves the interplay of private and public actors through a discursive and theoretical lens, I employ a descriptive and analytical approach to assess China's success in cyber norm promotion. In order to create a coherent theoretical framework that will guide the analysis of my case study, I have used textual analysis to select the theories that will be defining and specifying the boundaries that will guide the structure of my findings and discussion.

To make sense of my qualitative findings, I will be using a combination of process tracing and diffusion models. The diffusion model will guide my analysis of why African

countries are so inclined to adopt Chinese cyber governance norms over that of Western countries. Diffusion captures exactly this: the adoption of a norm or behavior, cross-nationally, through carrot and stick tactics to entice a group to explicitly adopt preferred policies (Simmons, et al., 2006). Though this dissertation will not be solely focusing on concrete policies that were created and will emphasize the engagement of cyber practices that were more implicitly promoted, it is a useful methodology to frame the influence that China has on African nations in advancing certain norms.

To analyze the case study, I will be utilizing process tracing, which is the identification of the causal chain and causal mechanism between two variables (George & Bennett, 2004). This method helps create the link between a specific event, a different event, and the link that occurs between the two (Mahoney, 2012). In this dissertation, I will be using process tracing to evaluate the "narrative structured by theory, variables, and competing explanations" between the Digital Silk Road in Ethiopia and the resulting Internet sovereignty cyber norms that occurred because of it (Gonzalez-Ocantos, 2021: 106). This method is used specifically to emphasize the direct pathway between China's investment in Africa and the subsequent transformation of Ethiopia's censorship norms; the link between these two events are otherwise unclear given Ethiopia's authoritarian regime and unstable political environment that could be other motives for establishing surveillance, censorship, and data monitoring norms.

2.2. Case Study Sample

Chinese involvement in Ethiopia's "Sheba Valley", the growing tech hub of Africa, is a critical case in China's role in cyber norm promotion in Africa because the two nations have strong relations, there is a clear attempt on Ethiopia's part to develop an ICT hub that imitates China's Shenzhen-based one, and Ethiopia's surveillance and censorship practices have historically proven to resemble that of China's. Furthermore, it is emblematic of the South-South cooperation that China is seeking to foster in its regional diplomatic development plans as a part of its Digital Silk Road (Gong et al., 2019). Ethiopia's imitation of China, propelled by Ethiopia's 2005 elections that highlighted the attractiveness of China's authoritarian model, has

only increased since then, exemplified through occurrences like how the Meles Zenawi Leadership Academy copied the China Executive Leadership Academy (Mueller, 2015). This creates an interesting model of study to examine whether this imitation extends to Chinese cyber norm promotion in the nation. Additionally, Ethiopia can be considered a representative of other African nations and hosts the headquarters for the African Union (AU) and the United Nations Economic Commission for Africa (ECA) (Gravett, 2020). Lastly, Ethiopia also creates an interesting case study because it is the only African nation where the telecommunications network infrastructure is entirely controlled by the SOE Ethio-Telecom, whose partnership has almost been completely with Chinese private company ZTE. This allows for a concentrated examination of norm dispersal from ZTE into Ethiopia's infrastructure and government system without worrying about outside influences.

3. Theoretical Framework

3.1. Cyber norm promotion

Norms reflect a collective expectation for acceptable behavior for a group that shares a common identity (Katzenstein, 1996: 5; Finnemore & Sikkink, 1998). In international politics, norms embody a code of conduct for what these institutions or governments ought to keep doing (Erksine & Carr, 2016). Within the international context, taking the constructivist perspective, international structure is created by the international allocation of ideas (Wendt, 1992). It follows that with the international distribution of these beliefs determining international order, norm shifts are the main vehicle for system transformation (Finnemore & Sikkink, 1998: 894).

Norms are created by norm entrepreneurs, actors that will negotiate new institutional rules, develop new standards of appropriate behavior, and set the standard for acceptable political intervention (Hajer, 2003: 176). Norm entrepreneurs are critical because they call attention to a topic and frame it through language that interprets or dramatizes the problem, creating a basis for a norm to address (Benford & Snow, 2000). They can exist as other nations, international

institutions, and even private corporations and transnational corporations. Once entrepreneurs introduce these standards, as proposed by Finnemore and Sikkink, norms have a three-stage life-cycle: norm emergence, norm acceptance, and internalization (Finnemore & Sikkink, 1998). To create a new normative order, legitimization techniques must be employed for the norm to be fully internalized, until the practice is widely accepted and taken for granted.

Norm adoption can be seen as cyclical in nature. No norm will fit a context entirely and therefore, there will always be a drive to change old norms and develop newer ones. Especially in cyberspace, an ambiguous, new, and ever-changing environment, this cyclical model emphasizes how norm promotion will always be shaped by existing contexts and local environments (Finnemore & Hollis, 2016: 449). Indeed, this is supported by the findings of norm diffusion literature that posits that actors that have similar identities, values, and problems will likely develop similar policies (Winston, 2017).

Even if this makes norm transfer seem like natural progressions, norm cultivation is a serious effort. Scholars of international relations have identified three tools for the development and spread of norms: incentives, socialization, and persuasion (Finnemore & Sikkink, 1998; Glen, 2021). Incentives describe when strong states have resources to encourage norms through inducements such as economic sanctions, investment, or aid (Goodman & Jinks, 2013). Other actors such as private companies and NGOs can provide rewards such as issuing best lists or helping civilian protests. In certain situations, internalization of the norm occurs and even with the incentives reduced, the host country will continue to abide by the norms and adopt it as their own. Socialization refers to the incorporation of these actors into these practices because they want to maintain the relationship and meet the expectations of the alliance (Glen, 2021). Mimicry can be a manner for the state to conform to the behaviors because they perceive that doing so would make them as successful as their model. In this way, developing states will model their behavior after more developed states, as shown through Western-framed education systems or suffrage laws (Finnemore & Hollis, 2016). Professional training is also a manner of socialization: by embedding norms into training, it creates standards for the work force and ensures that certain values are embedded into crucial organizations and their policies. Persuasion is the last component of norm promotion, and describes the use of information or argumentation

to transform attitudes. They are often contextualized and framed through language, dramatization, or a narrative progression to make a compelling case for following a behavior (Finnemore & Hollis, 2016). In the context of cyber norm promotion, all three of these steps are taken in order for a norm to be embedded into the beliefs and understandings of the host state, with discourse power often being used as a tool during the persuasion stage.

3.2. Discourse Power

If norm promotion uses incentives, persuasion, and socialization as the vehicle to spread standards, then discourse power is the engine that drives it. In other words, discourse is an instrumental tool for China to promote its cyber sovereignty as it cycles through the three step process. Discourse, according to Foucault, are practices that form the objects of which they describe by not merely identifying them, but constituting them (Foucault, 1972: 49). In this way, discourse is about what can be said, who can say it, and why they are authorized to do so (Chang, 2023).

In international relations, discourse is a manner for nations to construct a narrative that can influence the development of international affairs, advance their interests, and influence political order and agenda-setting power (Fawcett, 2020). As was made clear in the persuasion step in norm promotion, the framing of a norm has the power to shift perceptions of a convention. As a specification within the persuasion rung, discursive power explains the ability of narratives to purposefully select information to control a viewpoint. In particular, international discursive power is advantageous because it embodies the ability of a power to promote new ideas, with the narrative acting as the filter and carrier that embellishes and interprets these norms (Zhao, 2016). For that discursive power to create tangible action, international norms must be set, and if one's norms prevail, it signifies the power of the discourse creator. Fundamentally, discourse and narrative relates to the ideological appeal of the practice the country is trying to spread, which often translates to how beneficial the doctrine will be to the host country security-wise and economically (Wang, 2016). It would make sense, then, for a nation to pair the

discourse with economic inducements so as to emphasize the appeal of the ideal it is trying to encourage.

Specifically for cyberspace, with its relative lack of rules, policies, and regulations, discourse emerges as a manner to promote norms by strengthening certain best-practices, establishing trust and reliance, and constructing a universally accepted governance system (Chang, 2023). Especially with how quickly cyberspace can evolve and change, values are constantly being transformed and redefined – establishing a strong discursive foundation means cultivating the legitimacy required to be dominant in future norm building. In this way, discursive power is invaluable to norm development by facilitating how other countries shape and perceive a nation, encouraging host countries to voluntarily accept sponsored policies and systems that are being promoted. For China, utilizing discursive power and narrative construction serves multiple purposes. For one, it is a manner of attaining the strategic end of dismantling the dominant Western discourse by creating a new model of the world that supports the Chinese dream (Economy, 2020). Additionally, it is a more diplomatic manner of getting African nations to abide by Chinese cyber rules and laws without the need for military coercion, gently persuading foreign governments to conform to Internet sovereignty and the China Dream through carefully formulated messaging.

4. Literature Review & Conceptual Background

4.1. Cyberspace governance

Much of the current research on cyberspace examines how and whether cyberspace can be regulated (Delacourt, 1997; Grandin, 2023; West, 2014). Cyberspace presents a state of anarchy because there is no single governing authority that regulates all of its components, from the users and information to the physical infrastructure that constitutes root servers and data centers (Pathfinder, 2011). Many scholars emphasize the dichotomy of cyberspace: on the one

hand, cyberspace is notably decentralized, which allows the private sector to take the reigns; on the other hand, its operation by private companies are primarily in the interest of the government, especially in cases where the state takes the initiative to become the main governing actor (Jayawardane et al., 2015: 4). This juxtaposition presents two approaches to governing cyberspace – a state-centric multilateral governance method or a multistakeholder approach that employs non state actors.

The origins of multistakeholderism coincided with the 2003 and 2005 World Summit on the Information Society (WSIS) in which "global internet governance" was identified to be both governmental and non-governmental organizations, creating the Internet Governance Forum (IGF) to be a managing and advisory body (van Eeten & Mueller, 2013). This set the foundations for a multi-party contributory model for cyberspace. Since then, the US has published its International Strategy for Cyberspace in 2011, which outlines policies that align with core American ideas of "fundamental freedoms, privacy, and free flow of information" (Grandin, 2023: 5). Most Western countries share these cyber norms of multi-stakeholderism, which describes a shifting balance of powers between civil society, industry, states, and international governance institutions (Raymond & DeNardis, 2015). With this structure, cyberspace is approached with openness, inclusion, and consensus decision-making. Indeed, key aspects of the multi stakeholder model are characterized by freedom of the Internet, data privacy, and strict stances against censorship (Brotman, 2015).

In contrast, China prefers a multilateral approach to cyberspace (Gao, 2022). A multilateral governance model focuses on approaches in which the government controls the speed, depth, and regulations of the cyber ecosystem (Kurbalija, 2016). This approach puts the policies and powers to govern the Internet in the hands of the state; it suggests that the United Nations is the broader advisory board and that states have their own power to set national policies. In this view, governments perceive the privacy policies of transnational digital companies like Google or Facebook to be threats to national security and digital sovereignty. Countries who support a multilateral governance model support the freedom to create their own regional Intranets, block certain websites they consider to be threats to national security, and collect any data or information from citizens (Wu & Gereffi, 2018). The BRICS – Brazil, Russia,

India, China, and South Africa – are explicitly advocating for enhanced cooperation on these issues and advocating for a more tightly controlled internet by creating the Shanghai Cooperation Organization (SCO) and presenting these policies before the UN (Nocetti, 2015).

In this way, cyberspace governance, with these two opposite conceptions of how it should function, has become an arena for geopolitical rivalry and norm contestation. It has been poignantly noted by the academic international digital community how the development of communication technologies (ICTs) has created a "conceptual space" that is ridden with insecurity, geopolitical competition, and competing frameworks for how to approach it (Chen & Yang, 2022; Cheng & Liu, 2022). Though the US has long been the dominant rule-shaper in the global cyberspace, its leadership has been questioned ever since Edward Snowden's revelations revealed Washington's hypocrisy and the gaps in the Western cyber governance structure (Shen, 2016). Already, emerging powers within the BRICS bloc have challenged the US's hegemonic position and rebuked the US-led regulatory unilateralism by questioning the legitimacy of ICANN and other normative global cyber governance frameworks that are being promoted by Washington (Chen & Yang, 2022).

A large block of literature has explored how many states from the Global South support cyber sovereignty because with decolonization, they have only just begun to claim territorial sovereignty (Choucri, 2012; Adonis, 2019; Wang, 2020). Like natural resources, data is considered a strategic tool for their economy: maintaining governance over it is a practical choice when their autonomy has just been reclaimed (Liu, 2022). This works well for China because support for a multilateral approach is crucial for norm promotion at the international level (Flonk, 2021). This creates a foundation for China's legitimacy in subsequent cyber sovereignty norm promotion: China has realized that for it to successfully diffuse its surveillance and censorship norms, there must be widespread support for its future endeavors in infrastructure ideology.

4.2. China's Dream Through Cyber Means

Scholars who have evaluated the Chinese model of cyber sovereignty have identified several dominant aspects to its policies (Hao, 2017; Flonk, 2021; Goa, 2022; Fung, 2019). First, the state desires to regulate the information space by limiting the role of non-state actors in cyberspace. Second, a consistent demand of the PRC is to reorient internet governance to be regulated by the United Nations and international institutions. Third, sovereign states must be able to exercise control over the Internet. In this way, China's approach to cyber sovereignty constitutes setting both legal and conceptual limitations on Internet sovereignty. This is done by reworking internet governance norms by de-emphasizing the Western multistakeholder standard of a "borderless Internet" in favor of one that allows free range to pursue censorship, surveillance, and data restriction.

Several scholars have researched multiple ways in which China seeks to promote its cyber governance framework and cyber norms (Cheney, 2019; Gao, 2022; Eriet & Streinz, 2021). The Beijing Effect, coined by Eriet & Streinz (2021), describes how Chinese laws can govern outside of their original jurisdiction. For example, the Brussels Effect describes when companies abide by the EU's GDPR when they are not legally obligated. Similarly, current research has found that a combination of push and pull factors encourage foreign governments to abide by China's Cybersecurity Law without explicit pressure to do so from the PRC (Eriet & Streinz, 2021: 21). Other manners in which China has sought to establish itself as a norm entrepreneur has been by exporting China's digital products, providing ICT infrastructure, and providing full kits for executing a Chinese version of the Internet (Adee, 2019; Ghiasy & Krishnamurthy, 2020).

Some of the current literature has touched upon the role of private companies in affecting cyber norms, and the specific way in which China deploys non-state actors to promote them (Hurel & Lobato, 2018; Flohr et al., 2010). Private corporations are able to set a new norm by working as meaning managers by establishing new ways of understanding issues, incorporating best practice codes within their companies, and involving themselves in governance structures through commitments to public expectations (Berndtsson & Kinsey, 2016). They will often take on an authoritative and regulatory role that was previously assigned to states. In this way, private companies are enlisted as tech entrepreneurs for the national agenda. Though many Chinese

private companies may be outwardly private, they are still accountable to the CCP, with many of these companies receiving hundreds of millions of dollars in grants from the Chinese government (Grotto, 2019; Moore, 2023).

It has been shown that China's internet companies have the highest percentage of internal CCP party committees; essentially, the Chinese government and the business sector are intertwined (Shen, 2018). As discussed by Gao (2022), in the style of quid pro quo, Chinese tech giants are often employed to promote the ideas of the central government and in return, they leverage the support they receive from the CCP to influence developing markets: using national economic strategy labels such as BRI & DSR is a powerful tool to legitimize their commercial expansion whilst strategically embedding PRC-led norms (Griffiths, 2019; Fritz, 2017). By conforming to values of the Chinese government, the Chinese private sector is seen as proponents of monitoring and surveillance while also diffusing the China model through products, innovation, and technological knowledge that is upheld by cyber sovereignty and strict Internet governance. Indeed, tech companies can be a mechanism for the Chinese government to export a model of a controlled internet under the veil of economic investment.

4.3. China-Africa Relations

Much of the literature on Sino-African relations has focused on whether China's growing presence is a threat to Western interests (Brautigam, 2010; Hirono & Suzuki, 2014), with many scholars suggesting that the behavior of the Chinese state is not malicious or ill-intended because this perspective primarily arises from the Western influence on Chinese foreign policy. Other debates focus on the motives around China's involvement in Africa (Hilman, 2021; Segal, 2017; Schaffer, 2023). On the one hand, Chinese economic investment is seen as a manner to fulfill China's diplomatic plan of the China Dream and to achieve political clout amongst nations in the Global South. Others have argued that Chinese telecom companies invest in Africa to conduct economic espionage, undermine US norms of internet freedom, and spread Chinese ideas of development and governance (Weber, 2021; Bader, 2019). As pointed out by Taylor and Xia,

China is not a monolithic actor, and a plethora of Chinese actors operate within China's broader cyberspace framework to advance's China's Dream.

Literature on Chinese technology in Africa have two sides: some raise the concern that the Chinese state model will become dominant in implementing security and surveillance in Africa (Gravett, 2020), while others believe that though China heavily involves Africa in its DSR initiatives, African political actors still have agency over how they are impacted when it comes to international relations (Schneider, 2021; Van der Lugt, 2021). China's engagement with Africa's digital infrastructure is considered by some to be hyperbolic, with the "Chinese panopticon over Africa" considered to be a lazy tactic used by Western thinkers to invoke a moral high ground (Kperogi, 2022). Indeed, this argument suggests that though Africa may rely on Chinese tech to achieve their goals, there is no alternative model of the Internet being pushed onto their governance systems. Rather than viewing Chinese solutions as malicious forms of surveillance, this perspective perceives Chinese actors as just one of the many involved in spreading widespread Internet connectivity, without a specific agenda being pushed onto African governments. On the other hand, those who advocate for vigilance and trepidation towards China's cyber norm diffusion in Africa are worried that Africa's nascent technology infrastructure cannot compete with China or the US, and that African states will find it difficult to disentangle themselves from Chinese influence on freedom of expression and data privacy (MacKinnon, 2019). Indeed, the leading worry is that as China continues to develop its censorship model, African governments will find it an alluring prospect, especially when they are combatting destabilizing political environments where inspecting and controlling citizens' data would be highly beneficial.

The following section will examine the case study of how China promotes its cyber norms in Africa by examining the Chinese private company ZTE's involvement in Ethiopia.

5. Case Study

`

5.1. Digital Silk Road

China’s Digital Silk Road (DSR) supplies international communication and data flows as a part of China's global infrastructure economic development plan, the Belt and Road Initiative (BRI). It was formally launched in 2015 and by 2017, it became a central aspect of the PRC’s BRI strategy, only to be later promoted as its own initiative by 2019 (Gordon & Nouwens, 2022). The parameters of the DSR are very broad, ambiguous, and poorly understood. Some primary documents define DSR as the digital tools that increase international connectivity and aid the growth of digital economies, evidencing the submarine fiber-optic cables, data centers, 5G networks, satellite ground tracking stations, security-sector information systems, and integrated proposals for smart cities (Gordon & Nouwens, 2022). However, the DSR has evolved into anything and everything the Chinese government has been involved in as a part of the cyber realm, even if many of these ICT projects have not been formally promoted as a part of the DSR (Triolo, 2020). The DSR is merely a logical deepening of China’s efforts from the early 2000s to diplomatically frame the ‘going out’ of China’s companies from the domestic market in a strategic manner (Gordon & Nouwens, 2022). Chinese tech has been investing in Africa since the beginnings of Africa's introduction to the Internet; the DSR has merely framed it in a manner that promotes a slogan for digital actors who seek to claim national support for their agenda. Chinese foreign policy concepts, such as the BRI and DSR, are rarely complete when introduced and are constantly evolving (Cheng & Zeng, 2023). This case study assumes that the DSR arose from the rapid development of China’s digital sector and is merely a continuance of the early network infrastructure-building that occurred in Africa. Thus, the DSR is best understood as Beijing’s formal and discursive method of promoting its global agenda across the technological economy sector and an extension of what China has already been promoting for years before official structures of intent.

Considered the “China solution” for the digital era, the DSR includes corporate-level digital infrastructure, globalization of Chinese tech companies, and technical Internet development (Huang, 2019). The way the Chinese government is able to execute this is by promising private technological companies that the CCP will provide opportunities if they work towards China’s national strategic objectives in foreign markets. This mutualism is underscored through the “2020 Opinion on Strengthening the United Front Work of the Private Economy in

the New Era" released by the General Office of the Central Committee of the CCP: it stressed the need for CCP ideological influence through private business and economic enterprises (Ye, 2020).

The "Made in China 2025" plan is a concrete manner for China to ensure that foreign governments will become reliant on Chinese companies by developing a global 5G standard (Triolo & Sherlock, 2020). For example, a 5G standard that is systematized across the developing world will encourage cooperation with China because they have an interest in maintaining interoperability with the technical infrastructure (Ye, 2020). Though there is no reason for them to abide by Chinese law, it is advantageous for their economies to have compatible networks that match China's digital framework. Already, when Chinese companies are providing the digital infrastructure at the outset, the host states are not in the position to disagree with China's data sovereignty standards (Huang, 2019). Moreover, once China has gained market access, it is easy to take operational liberties with these nations' legal systems. Of course, the United States and the EU can do the same, but China is unique due to its entanglement between the government and the private sector, making CCP-sponsored cyber norm promotion and diffusion much more seamless.

The DSR targets developing nations to improve their telecommunications networks, cloud computing, surveillance technology, and other digital aspects. In 2018, the Forum on China-Africa Cooperation pledged to foster greater cooperation between China and Africa, with the Action Plan outlining cooperation between authorities, the buildingof smart cities and the enhancement of the internet and digital economy in a mutually beneficial way (Gargliardone, 2021). By 2021, China proposed the China- Africa Partnership Plan on Digital Innovation to support the building of a shared future in cyberspace, with the direct beneficiaries being the nations of Angola, Zambia, Ethiopia, Nigeria, and Zimbabwe (Feldstein, 2020). Africa's interest in the DSR has grown as the offerance of inexpensive, high-quality technological infrastructure is attractive in expanding ICT services, especially for Ethiopia, whose capital, Addis Ababa, seeks to become the tech hub in Africa (Kulantzick, 2020). Ethiopia sees an opportunity to increase connectivity and to be ingrained in the digital economy, while China seeks to improve their production capacity and develop the nations they have partnerships with along their BRI

(Lu et. al, 2018). Private companies like ZTE have been active in taking initiative in creating technological projects under the BRI by creating data centers, building telecom network equipment, and building R&D labs (Feldstein, 2020). ZTE is the private company that will be examined in this case study because it is the main Chinese telecom giant that has been involved in Ethiopia.

5.2. Ethiopia & ZTE

Ethiopia has strong economic relations with China and is linked to China's BRI via Djibouti, where Chinese firms created Africa's first transnational railway linking Ethiopian capital Addis Ababa to the Djibouti Port (Clemoes, 2019). The Ethiopian government wants to focus on digital economic transformation as a part of the GTP II, the Second Growth and Transformation Plan; they desire to become a low middle-income country by 2025 (Van der Lugt, 2021). Politically, Ethiopia has long been considered an authoritarian regime and has not been classified as "free" in terms of Internet freedom (Freedom House, 2020). Indeed, the Ethiopian government considers the Internet a threat to national security and social stability.

In 2016, anti-government protests created an increasingly cautious approach to the Internet – the government singled out social media as the key igniter for political turmoil and instability (Yilma, 2016). The Ethiopian Prime Minister at the United Nations General Assembly condemned the negative effects of the internet and set out his intention to deal with the matter "head-on" (Abraha & Yilma, 2015). The political unrest in Ethiopia, as shown through Hailemariam Desalegn's resignation as Prime Minister in 2018 following the mass protests, has spurred the enactment of the Hate Speech and Disinformation Prevention and Suppression Proclamation Law, which introduces government regulation to control hate speech (Wanyama, 2020). This creates implications for freedom of expression and sets precedence for how the Ethiopian government decides to regulate cyberspace.

The Ethiopian Telecommunications Corporation (ETC) was established in 1952 and has been Ethiopia's only telecommunications provider since then (Sisay, 2013). In 2006, ETC signed a $1.6 billion contract with ZTE, a major Chinese telecommunications company, which became

ETC's only equipment vendor – ZTE sells software, services, network switches, software systems, and mobile handsets (Gagliardone & Geall, 2014). Ethiopia is the country that has most benefited from a partnership with China, with ZTE partnership with Ethio-Telecom resulting in an expansion from 900,000 network users to 17 million users (Gagliardone, 2013). ZTE also operates in other countries, such as for Nigeria's 4G implementation and Zambia's contract for CCTV cameras but has been accused of being corrupt (Malakata, 2013). ZTE was found guilty of bribing high-level employees at the Algerian government-owned network, Algerie Telecom, and its Zambian surveillance cameras were terminated after corrupt processes involving inflated pricing was found (Malakata, 2012).

Despite these charges, ZTE has denied claims that they are using African networks to exploit vulnerabilities for control and surveillance. However, there is growing evidence that African governments are ready to use Chinese technology for political purposes. For example, the Ethiopian government held an "Internet Management" workshop that informed people on how to monitor citizen networks (Reed, 2013). One major sign of the exported surveillance practice facilitated by Chinese ICT companies is the ZSmart, a tool developed by ZTE (Hernandez, 2019). ZSmart allows the monitoring of SMS message content, detailed call logs, and a system that can intercept email, web browsing, and online chats (Human Rights Watch, 2014: 62). Additionally, due to China's Cybersecurity Law, ZTE operations abroad means that data sharing with the CCP for intelligence-gathering purposes is within their jurisdiction (Reed, 2013). In this case, the ZTE is the independent variable, the input, with the effect being the changing cyberspace norms in Ethiopia that results from it.

6. Analysis

6.1. Cyber Norm Promotion - Incentives, Persuasion, and Socialization

In this section, I will be following the cyber norm promotion theoretical framework to explain how the Chinese private company ZTE attempted to promote Chinese norms of surveillance and censorship in Ethiopia. In my theoretical framework, I explained the three

method process that characterizes the advancement and spread of norms in international relations: incentives, persuasion, and socialization. A close reading of ZTE efforts to build Ethiopia's telecommunication infrastructure proves China's attempts at shaping cyber norm content.

6.1.1. Incentives

First, the "incentive" step in norm promotion has been illustrated through ZTE building of network infrastructure, Chinese subsequent pullback in funding, and the enduring surveillance practices that Ethiopia has embraced.

Chinese private companies' provision of incentives along the Digital Silk Road is one of the main objectives of its involvement in Africa. In 2006, the Chinese Import-Export Bank loan allocated 1.9 billion USD to ZTE to lay down the national fiber backbone and expand the borders of 2G in Ethiopia (Workneh, 2014). This illustrates ZTE's "incentive" to Ethiopia because it laid down the basic network infrastructure that would allow Ethiopia to be finally incorporated into the wider Internet global system and bolster job creation through a digital economy. Additionally, this was only possible through the official funding by the PRC, making it clear that the Chinese government is utilizing ZTE as a medium to create development inducements. In 2013, another 1.6 billion USD was awarded to ZTE to improve 3G network and introduce LTE to Ethiopia (Dalton, 2014). Since then, however, China has been scaling back investment in Ethiopia and a drastic downward trend has characterized credit insurance allocation for projects in Addis Ababa (Aglionby & Feng, 2018). Even with these "incentives" coming from China reduced, Ethiopia has turned away from US high-tech surveillance and has started to rely on China for its surveillance needs. In this way, this illustrates the internalization of the Chinese cyber sovereignty norm because despite China's slowdown of investment and interest in Ethiopia's current economy, Ethiopia continues to support ZTE ZSmart tracking of phone records. The Ethiopian government has even begun to block access to information by banning websites and hindering opposition group media outlets (Human Rights Watch, 2014). In this way, the incentive of investment in Ethiopian expansion was mobilized to gain widespread

acceptance of Chinese cyber norms, so much so that the practices were adopted when the reward dwindled.

6.1.2. Socialization

Second, the "socialization" tier of norm promotion has been fulfilled through Ethiopian mimicry of China's development model and Internet sovereignty laws. Moreover, Chinese professional training of Ethiopian technical personnel has embedded key cyber norm values into the workforce.

As the Ethiopian-Chinese partnership was developing, it was made clear to Ethiopia that a strong central government, modeled after China, would be crucial to preventing rent seeking behavior and growing the private sector. China's development success of rapid modernization is very attractive to Ethiopia; the admiration for the "China Model" that emphasized development without political liberalization was actualized through former Prime Minister Zenawi's pursuit of centrality of state in Ethiopia's economy (Ziso, 2020). Indeed, the creation of Ethio Telecom, an SOE, mimicked the pervasiveness of state-owned enterprises in China's economic strategy. This shows Ethiopia's socialization to China's cyber norms, even if it's just the broader institutional structure from which they diffuse from, because mimicking China's behavior could lead to the same success for Ethiopia.

More specifically, Ethiopian cyber sovereignty laws, or lack thereof, tend to mimic the ambiguity of Chinese data localization laws. From the very small library of laws that address data, cyber governance, or Internet freedom, Ethiopia notably has the Telecom Fraud Offense Proclamation that criminalizes a list of activities related to telecommunications services or attempts to undermine the monopoly of Ethio Telecom (Human Rights Watch, 2014). Under this umbrella, it is punishable with up to eight years' imprisonment to produce a "terrorizing" message or to use voice over Internet protocol services like Skype or Google Talk (Telecom Fraud Offense Proclamation, 2012). It should be noted that what constitutes a "terrorizing" message is undefined. The Anti-Terrorism Proclamation similarly uses vague language that allows the National Intelligence and Security Service (NISS) to prevent a "terrorist act", though

the means of doing so is open to interpretation – and certainly includes surveillance of any citizen (Human Rights Watch, 2009). These laws mirror the ambiguity in China's own data localization regulation laws, even if China's laws are both broad and comprehensive enough to leave room for government intervention and surveillance in any industry. Indeed, Article 37 of China's Cybersecurity Law requires "critical information infrastructure" to store important data within mainland China, including all personal information (Wei, 2018). In this way, the socialization of data freedom infringement, actualized through the Ethiopian information laws mimicking structure and ambiguity to Chinese cyber sovereignty laws, evidences the norm promotion of Chinese cyber practices.

In addition to Internet sovereignty laws, professional training of Ethiopian technical personnel by Chinese private companies represents another aspect of the socialization aspect of norm promotion. As part of the initial effort to build the national telecom network, ZTE trained over 1,000 engineers, localized the Ethiopia office through ZTE university, and pledged to lead 15,000 technical personnel in professional training (Lili, 2019). The socialization of the Ethiopian developers occurred by embedding norms into training, as many of the local ICT engineers and technical staff, trained by Chinese managers, personnel, and handbooks, instilled Chinese cultural values. The exposure helped develop the labor force with necessary skills to support the new and burgeoning telecommunications network infrastructure, and in doing so, it also familiarized the staff with the Chinese value system and with it, norms of surveillance and censorship in cyberspace. This was most notably executed through the Addis Ababa Confucius Institute 12-week training program that runs for ZTE Corp employees, teaching Mandarin, Chinese cultural information, Confucianism, and Chinese values to Ethiopian team members (Lin, 2013). Thus, in Ethiopia's mimicry of China's cybersecurity laws and the infusion of these values in the workforce, there is a clear indication of Chinese norm promotion into Ethiopia and diffusion of cyber standards and practices through the process of socialization.

6.1.3. Persuasion

Lastly, the "persuasion" component of norm promotion is illustrated through ZTE's sponsorship in discourse and narrative building of a venerable China, its alignment to key values of the DSR, and the official rebuke of the internet by Ethiopia.

Persuasion, the use of information and narratives to discursively promote norms and transform attitudes, occurred when ZTE projected positive ideas of China onto Ethiopia, creating a conducive environment for Internet sovereignty norm promotion. First, China has long been successful in its image-building in Ethiopia, especially with the aid of ZTE's partnership in building the national telecommunication network: Former Ethiopian Prime Minister Meles Zenawi, following praise for ZTE's contribution to the ETC's millennium project, expressed China's impact on Ethiopia: "The Great Wall is a symbol of China, and the opening of the national mobile network in Ethiopia has an equal significance as that of the Great Wall to Chinese people," (Lili, 2009). By comparing the most common symbol of China to this DSR effort, Ethiopia is expressing gratitude to China as a nation and communicating its intention to follow in its greatness and eminence.

Additionally, ZTE's official statements of its intentions in Ethiopia painted a discursive narrative that aligned with key components of the DSR by using slogans like "Enhancing Knowledge Transfer for Mutual Benefit" and "Joint Cooperation of Our Wisdom and Strength for the Great Future of Ethiopia" (Lili, 2009). These statements, though not explicit in its endorsement of the China Model, uses the same language as official China-Africa DSR proposals. The phrases "formulating global rules on digital governance" and seeking to "develop stability, community, and regional economies" underscores China's readiness to stand with the African side to strengthen dialogue in cybersecurity (Ministry of Foreign Affairs, 2021). These discursive ideological constructions that ZTE is endorsing deliver a message of digital economic cooperation and shared common development goals in China's involvement in Ethiopia, creating a positive breeding ground for easy acceptance of China's cyber norms. As a result, they were readily accepted: in 2016, Ethiopian Prime Minister Hailemariam Dessalegn condemned the Internet and outlined his political intention to address the issue "head-on" (Yilma, 2016). This demonstrates the success of the "persuasion" tier, as the narrative building of China as a

trustworthy and helpful resource made a compelling case for Ethiopia to adopt its norms of cyber sovereignty and censorship.

6.2. ZTE & Ethio-Telecom Alliance Process Tracing

In this section, I will show that Ethiopia has adopted the Chinese cyber norms of cyber sovereignty, censorship, and surveillance after China penetrated its market through process tracing. I will prove this direct link by tracing the entrance of Chinese private companies into Ethiopia to the Ethiopian government's use of technology to surveille, control, and censor its citizens.

The first connection that can be tested is whether the Ethiopian government intentionally requested surveillance tools from China. The Ethiopian government is the one that initially established cooperation with Chinese firms, as shown by Ethio Telecom's employment of ZTE to build the national telecommunication network backbone. The introduction of the Internet in Ethiopia occurred in 1993 and by 1997, the Ethiopian Telecommunications Corporation (ETC) provided full internet to users (Jensen, 2015). ZTE entered Ethiopia in 1996, merely three years after the Internet was introduced to the nation, and by 2006, ZTE and the ETC entered the early stages of mutual cooperation through the Sino-African Cooperation, commencing the three-phase development project (Lili, 2009). ZTE allows for the government to make use of its surveillance software, and evidence gathered by Human Rights Watch deduced that Ethiopia had been using it for that purpose (Human Rights Watch, 2014). Though it is difficult to prove that the Ethiopian government specifically requested it for surveillance purposes, it was an unintentional advantage that came from its employment.

The second relationship that can be shown is that China provides Ethiopia with software and hardware that can be used for surveillance. In 2008, ZTE exclusively developed the nationwide network for fourteen of the largest cities in Ethiopia and was deployed to create a city security surveillance system that placed 200 cameras in Addis Ababa (Van der Lugt, 2021). With ZTE as the main telecom infrastructure provider for government-sponsored Ethio Telecom, Ethiopia was able to access citizen's information on all calls and text messages, as well as record

them, through ZSmart, the customer management system, and ZXMT, the ZTE monitoring system (Human Rights Watch, 2014). By March 2019, there had been talks of establishing a joint innovation center between Ethio Telecom and ZTE, proving that Chinese firms certainly supply Ethiopia with surveillance technologies.

A third nexus to be proven is that the Ethiopian government can seize personal data at any time, especially with the help of ZTE. Though the 1995 Ethiopian Constitution has privacy as a safeguard, it is only if certain conditions, such as national security or public peace, are met (Taye & Teshome, 2018). The Ethiopian government also has the right to collect personal data. The Registration of Vital Events Proclamation means personal data can be given to intelligence agencies without consent, which consists of all of the information ZTE & the ETC collects, like address, name, photograph, and call and text history (Taye & Teshome, 2018). This proves that the government does collect data on citizens and employs the help of ZTE to do so.

The last connection to make is the adoption of cybersecurity law in Ethiopia following ZTE entrance into the economy. Legally, official policies in Ethiopia about telecom fraud, commitment to monopolies, and bans on international calling applications like WhatsApp, WeChat, and Skype were not formed until 2012. Indeed, proclamation no 761, article 9/1/b in Ethiopia's Penal Code outlines that the circumvention of established telecom infrastructure would be punishable from 10 to 20 years (Cheng, 2022). Not only does this reinforce the multilateral governance style of state control in the data space, but it shows that the creation of official cyber structures did not commence until far after the establishment of Chinese private industry companies in Ethiopia. Additionally, it is believed that the first deployment of censorship in Ethiopia was committed in 2006 when the ETC blocked access to the Internet to confuse users by suggesting website owners were responsible for technical glitches (Reporters without Borders, 2006). Only four years later, former Prime Minister Meles Zenawi reiterated his right to defend Ethiopia's Internet sovereignty and proceeded to jam Voice of America's broadcasts (BBC, 2010). These acts of censorship coincide chronologically with ZTE's cooperation with the ETC. Furthermore, as outlined in the International Strategy of Cooperation on Cyberspace, Chinese technology exports and Internet firms are encouraged to serve goals of the Chinese government, like political stability and Internet sovereignty (Ministry of Foreign

Affairs of the PRC, 2017). The Chinese technology exports to Ethiopia makes it seamless for the nation to experience the benefits of Internet sovereignty, thereby supporting the fact that Ethiopia consciously models its laws after China's.

6.3. Addressing Limitations

In this section, I address the weaknesses of using the case study of Ethiopia by examining two examples: an African non-authoritarian regime's adoption of China's promoted cyber norms and a Chinese private company that has been successful in transforming the broader African continent's cyber networks and discourse.

Ethiopia is one of the few countries in the world which maintains a state monopoly over telecommunications and internet services, which may make the selectivity of Ethiopia as a case study a convenient parallel to China's own regulated digital environment. Additionally, given that Ethiopia is an authoritarian regime characterized by political unrest, it could be argued that its similarity to China in government models makes norm promotion extremely favorable. However, if we consider the case of Botswana, the longest uninterrupted democracy in Africa, Chinese influence on cyber governance norms still endure.

6.3.1. Botswana

Botswana is a multi-party democracy that boasts a stable political environment (World Bank, 2023). General elections are held every five years and the president is elected indirectly by the people through the National Assembly; both the Southern African Development Community and African Union observed free and fair elections, with little record of widespread political unrest or violence (Freedom House, 2021). Despite this, Botswana lacks comprehensive data protection laws or policy addressing e-governance, with a Data Protection Act passing in 2018 that has not yet applied to the wider population (Mudongo, 2021). Additionally, similar to Ethiopia and China, Section 59 of the Penal Code, that claims that spreading misinformation is punishable by law, is broad enough that it allows for the discretion to be taken by the government

(Sarefo et al., 2023). There have been records of the Botswana government arresting opposition members for their online activities, illustrating a governance structure that is too wide in breadth to be sufficiently regulated.

In 2018, the Botswana Police Service signed a deal with Chinese private company Huawei to build surveillance cameras through the DSR Safe City projects (Agbebi, 2022). Much like the lack of an updated data governance structure, Botswana has not addressed the use of data gathered from CCTV surveillance by the government and Huawei, a private company that is larger than ZTE with a record of both privacy and human rights violations (Wang & Li, 2023). As it follows, Botswana has a democratic government that does not parallel the Chinese authoritarian regime. Despite this, its nascent and vulnerable digital infrastructure makes it susceptible to Chinese investment and by proxy, the easily diffusible cyber norms of surveillance and censorship. Though it is more difficult to prove the direct link between China's involvement in Botswana through private companies and Botswana's lack of cyberspace regulation, it is clear government structure and political stability is not a factor in how successful China can promote its cybernorms. It is a more likely explanation that the stage in which Chinese private companies enter the African digital infrastructure – early enough and economically enticing enough to lay sound technologically foundations – affects the possibility of surveillance and censorship norms.

6.3.2. Transsion

Transsion is a private company that provides smart devices and mobile services; it has become Africa's top provider for smartphones (Dahir, 2018). Transsion is cheaper than other brands like Apple or Samsung, caters to the local African diverse market, and encourages modernization demands for locals in Ethiopia, Tanzania, Nigeria, Kenya, and Egypt (Kazeem, 2019). Transsion has explicitly and implicitly acknowledged the norms and values of the CCP by incorporating language in their core messaging and has officially adopted the "Africa first" policy (Bayes, 2019). Indeed, with Transsion providing affordable products that would boost the local economies in Africa, it is fulfilling the China-Africa partnership of guiding a new era of cooperation, mutual benefit, and development.

On the technological side, Transsion developed a location accuracy platform that could locate devices, people, and objects faster (Hoffman, 2019). The Chinese company has expanded its domain to the Internet industry, created face recognition technology that recognizes dark skin tones better, and has funded research that would advance Chinese monitoring systems (Triolo, 2020). In all of these manners, it is clear that Transsion is engaging in data collection practices to advance the technical accuracy of future developments and thereby paving the surveillance and monitoring future of Africa.

Not only can they access vast amounts of data that can serve the CCP's interest in mass control, but Transsion has been successful in promoting the Chinese way of dealing with cyberspace. The African public have high opinions of Transsion, as there is an appreciation for Transsion's help in innovation and efforts to cater to local markets. More crucially, China's narrative has resonated with multiple government officials in Africa, with Zambia's minister Brian Mushimba praising China for their interesting model, "very different from how the Western world interacted with Africa. China serves as a model worth replicating" (Prasso, 2019: 4). Additionally, in terms of cyber norms, Mushimba aligned himself with China's value of Internet sovereignty: "the Internet is a powerful tool that can't be left to run wild," (Prasso, 2019: 6). He has had a record of supporting self-censorship, the need for the government to monitor all digital devices and supporting surveillance to keep security and order in a country. In Zambia, there is a push to pass a cyber-law that would create an institution that can determine when information threatens national security; this shows similarities to the Chinese Cybersecurity Law, highlighting China's successful cyber norm promotion and ideological push (Sun, 2016). In sum, Transsion represents another example of a private company that has been successful in promoting Chinese discursive power and cyber norms of surveillance and censorship. With Transsion's presence in multiple countries in Africa, and its success in spreading a Chinese data governance model, it clarifies that ZTE in Ethiopia is perhaps not such a specialized case study, and Africa's reception of China's norm promotion in cyberspace is indicative of a larger trend that can be more broadly applied.

7. Conclusion

Rather than focusing merely on how China has attempted to promote cyber norms against the backdrop of Western hegemony in cyberspace, this dissertation wrestled with whether China was advancing alternative models of cyber governance, how it has sought to do so, and the role of private companies in executing this techno-strategy along the DSR in Africa. The construction utilized a cyber norm promotion framework (Finnemore & Sikkink, 1997) of incentives, socialization, and persuasion to guide the full implementation of surveillance, censorship, and data monitoring. The theory of discourse power was used to inform the persuasion step of the cyber norm promotion cycle and to advise the narrative aspect of the DSR to aid China's efforts in digital infrastructure-building in foreign countries. Though much of the literature on China's advancement of its cyber norms focused on its contrast to the Western model (Gao, 2022; McKune, 2018; Segal, 2020), this dissertation focused less on China's attempts to dethrone the US as the major norm promoter and more on China's reconciliation between the PRC's interests and Chinese private companies' involvement in Africa.

I found that though the BRI, and by extension, the DSR, explicitly outlines intentions to shape cyber norms in foreign nations, China does not seem to have a comprehensive objective in explicitly promoting censorship, Internet sovereignty, and surveillance. Indeed, there is little evidence that the government is actively dispersing cyber operations and building digital infrastructure for the precise purpose of creating a global cyber governance network that abides by the same values as China. However, whether intentional or not, the effect of building telecommunication networks, smart cities, and striking deals with monopolies that dominate the tech world in African nations means cyber norms are certainly diffused. Of course, this is not meant to discount the agency of African nations; however, it appears that the Chinese surveillance technologies and manners of controlling Internet and data aligns conveniently with authoritarian governments in Africa, leading to the adoption of these cyber norms.

Specifically for ZTE in Ethiopia, it is very easy for Chinese cyber norms to be folded into the fabric of Ethiopia's legal and social digital infrastructure due Ethio Telecom's monopoly over the networks industry and how early China was able to penetrate its market. The investment that China has made in Ethiopia has been very welcome to Ethiopia's burgeoning digital economy and the advancement of its telecom network has been invaluable to interconnecting Ethiopia with

the rest of the world. In this way, Ethiopia has viewed China as a model for its own development and has mimicked China's legal and structural cyber sovereignty norms. Even so, it is true that the political instability of Ethiopia as well as its authoritarian regime makes it especially vulnerable to copying the surveillance and censorship habits of China. To address these gaps, I bring in Botswana's lack of data governance regime as well as Transsion's diffusion across Africa to show China's endurance in cyber norm promotion across the continent regardless of government type.

To answer the main question: this study has found that though China's cyber norm promotion has been an intentional aspect of the DSR, China's cyber diplomatic efforts in Africa, executed through digital infrastructure building and dispersal of private companies like ZTE in Ethiopia, has been an inadvertent, albeit successful, effect of China's economic contributions. This does not contradict the very real and sizable effects that China has had on the cyber governance structures in African nations, regardless of whether they exist as authoritarian nations or not, and points to the complexity of the ever-evolving field of technopolicy that is presently occurring in Africa. Indeed, the rapid changes in Africa's telecommunications landscape and how it is impacted by Chinese private companies, and by extension, the government, warrants more specific study by researchers who are eager to see how Africa intends to balance its agency and priorities with attractive Chinese investments and alluring discursive narratives.

Bibliography

Adee, S. (2019) The Global Internet is Disintegrating – What Comes Next? *BBC*, Retrieved from https://www.bbc.com/future/article/20190514-the-global-internet-is-disintegrating-what-comes-next.

Adonis, A. A. (2019) Critical engagement on digital sovereignty in international relations: actor transformation and global hierarchy. *Global: Jurnal Politik Internasional*, *21*(2), 262-282.

Agbebi, M. (2022). China's Digital Silk Road and Africa's Technological Future. *Council on Foreign Relations.* https://www.cfr.org/blog/chinas-digital-silk-road-and-africas-technological-future

Aglionby, J. & Feng, E. (2018) China scales back investment in Ethiopia. *Financial Times.* Retrieved from https://www.ft.com/content/06b69c2e-63e9-11e8-90c2-9563a0613e56

Bader, J. (2019). To Sign or Not to Sign. Hegemony, Global Internet Governance, and the International Telecommunication Regulations. *Foreign Policy Analysis*, *15*(2), 244-262.

Bader, J. A. (2016). *A framework for US policy toward China*. Foreign Policy at Brookings.

Barrie, J., Buckley, K., Caminade, C., Chen, J., Cortez, F., Emejulu, D. A., ... & Wäspi, F. (2022). Recommendations on Using Digitalisation for Our Common Future: A Report by the Policy Network on Environment and Digitalisation. Internet Governance Forum.

Bayes, T. (2019) African networks, smartphones – and surveillance. *Mercator Institute for China Studies.* Retrieved from https://merics.org/en/comment/african-networks-smartphones-and-surveillance

BBC (2010) Ethiopia admits jamming VOA radio broadcasts in Amharic. *BBC.* Retrieved from http://news.bbc.co.uk/1/hi/8575749.stm

Benford, R. D., & Snow, D. A. (2000). Framing processes and social movements: An overview and assessment. *Annual review of sociology*, *26*(1), 611-639.

Berndtsson, J. & Kinsey, C. (2016) *The Routledge Research Companion to Security Outsourcing*. London: Routledge.

Bräutigam, D. (2009). The dragon's gift: the real story of China in Africa. Oxford University Press.

Brautigam, D. (2010). China, Africa and the international aid architecture. *African Development Bank Group Working Paper*, *107*.

Brotman (2015) Multistakeholder Internet governance: A pathway completed, the road ahead. *Center for Technology Innovation.* Brookings Institute.

Carr, M. M., & Erskine, T. (2016). Beyond "quasi-norms": The challenges and potential of engaging with norms in cyberspace. *NATO Cooperative Cyber Defence Centre of Excellence*.

Chang, Y. Y. (2023). China beyond China, establishing a digital order with Chinese characteristics: China's growing discursive power and the Digital Silk Road. *Politics & Policy*.

Chen, X., & Yang, Y. (2022). Contesting Western and Non-Western Approaches to Global Cyber Governance beyond Westlessness. *The International Spectator*, *57*(3), 1-14.

Cheney, C. (2019) China's Digital Silk Road: strategic technological competition and exporting political illiberalism. *Issues & Insights*, *19*.

Cheng, J., & Zeng, J. (2023). "Digital Silk Road" as a Slogan Instead of a Grand Strategy. *Journal of Contemporary China*, 1-16.

Cheng, L., & Liu, X. (2022). Exploring Chinese cyber discourse: integrating political and legal perspectives. *International Journal of Legal Discourse*, *7*(1), 33-52.

Choucri, N. (2012) *Cyberpolitics in international relations*. MIT press.

Clemoes, C. (2019) Cities on the New Silk Road: Djibouti City. *Topos.* Retrieved from https:// www.toposmagazine.com/ cities-on-the-new-silk-road-djibouti/.

CNNIC. (2021) The 47th Statistical Report on the Development of Internet in China" Retrieved from http://www.cnnic.cn/hlwfzyj/hlwxzbg/hlwtjbg/202102/t20210203_71361.htm.

Dalton, M. (2014) ZTE at Risk of Losing Ethiopia Contract. *Wall Street Journal.* Retrieved from http://www.tadias.com/11/14/2014/zte-at-risk-of-losing-ethiopia-telecom-contract/

Degterev, D. A., Ramich, M. S., & Piskunov, D. A. (2021). US & China approaches to global Internet governance: "New bipolarity" in terms of "the network society". *International Organisations Research Journal*, *16*(3), 7-33.

Delacourt, John T. 1997. The International Impact of Internet Regulation. *Harvard International Law Journal*. 38(1): 207–35.

Demchak, C. C. (2016). Uncivil and Post-Western Cyber Westphalia: Changing interstate power relations of the cybered age. *The Cyber Defense Review*, *1*(1), 49-74.

Economy, E. C. (2020). Exporting the China model. *Testimony before the US-China Economic and Security Review Commission. Testimony before the US-China Economic and Security Review Commission.* Washington. *URL: https://www. uscc. gov/sites/default/files/ testimonies/USCCTestimony3-13-20*, *20*.

Erie, M. S., & Streinz, T. (2021). The Beijing effect: China's Digital Silk Road as transnational data governance. *NYU Journal of International Law and Politics*, *54*, 1.

Fawcett, Alicia. 2020. Chinese Discourse Power. *The Atlantic Council.* https:// www.atlanticcouncil.org/wp-content/uploads/2020/10/Chinese-Discourse-Power.pdf.

Feldstein, S. (2020) Testimony before the U.S.-China Economic and Security Review Commission Hearing on China's Strategic Aims in Africa. *Information Technology and Innovation Foundation.*

Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. *American Journal of International Law*, *110*(3), 425-479.

Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization*, *52*(4), 887–917. http://www.jstor.org/stable/2601361

Flohr, A., Rieth, L., Schwindenhammer, S., & Wolf, K. (2010). *The role of business in global governance: Corporations as norm-entrepreneurs*. Springer.

Flonk, D. (2021) Emerging Illiberal Norms: Russia and China as Promoters of Internet Content Control. *International Affairs.* 97 (6): 1925–1944. doi:10.1093/ia/iiab146

Foucault M. (1972) *The Archaeology of Knowledge*. New York: Harper Colophon.

Freedom House (2020). 'Countries'. Retrieved from https://

freedomhouse.org/countries/freedom-net/scores?sort=asc&order=Total%20

Fritz, J. R. (2017).*China's cyber warfare: the evolution of strategic doctrine*. Lexington books.

Fung, C. J. (2022). China's role in shaping a global information order: cyber-sovereignty, norms and information technology. *Macquarie University*.

Gagliardone, I. (2013) China as a persuader: CCTV Africa's first steps into the African mediasphere. *Ecquid Novi: African Journalism Studies*, 34(3).

Gagliardone, I. (2021) Chinese digital tech in Africa: moral panics and the messy reality of surveillance. *China Dialogues: LSE Blogs*. Retrieved https://blogs.lse.ac.uk/cff/2021/05/20/chinese-digital-tech-in-africa-moral-panics-and-the-messy-reality-of-surveillance/

Gagliardone, I., & Geall, S. (2014). China in Africa's media and telecommunications: cooperation, connectivity and control. *Norwegian Peacebuilding Resource Centre (NOREF) Expert Analysis*, 1-6.

Gao, X. (2022). An attractive alternative? China's approach to cyber governance and its implications for the Western model. *The International Spectator*, *57*(3), 15-30.

Gargliardone, I. (2021) Going beyond the stereotypes: China's digital Infrastructure in Africa, In *FOCAC AT 21: Future trajectories of China-Africa relations*, China Foresight, LSE

Ideas. Retrieved from https://www.lse.ac.uk/ideas/Assets/Documents/reports/LSE-IDEAS-FOCAC-at-21.pdf

George, A. L., & Bennett, A. (2005). Case studies and theory development in the social sciences. MIT Press: Cambridge.

Ghiasy, R. & Krishnamurthy, R. (2020) China's Digital Silk Road—Strategic Implications for the EU and India. *Special Report* 208. IPCS-Leiden Asia Centre, August. http://www.ipcs.org/issue_select.php?recNo=6153.

Ghiasy, R. & Krishnamurthy, R. (2020). China's Digital Silk Road: Strategic Implications for the EU and India. *Institute for Peace and Conflict Studies and Leiden Asia Centre*.

Glen, C. M. (2021). Norm entrepreneurship in global cybersecurity. *Politics & Policy*, *49*(5), 1121-1145.

Gong, S., Gu, J., & Teng, F. (2019). The impact of the Belt and Road Initiative investment in digital connectivity and information and communication technologies on achieving the SDGs. *K4D Emerging Issues Report.* Brighton, UK: Institute of Development Studies.

Gonzalez-Ocantos, E., & LaPorte, J. (2021) Process Tracing and the Problem of Missing Data. *Sociological Methods & Research*, *50*(3), 1407-1435.

Goodman, R., & Jinks, D. (2013). *Socializing states: Promoting human rights through international law*. Oxford University Press.

Gordon, D. & Nouwens, M. (2022). "The Digital Silk Road: Introduction." *International Institute for Strategic Studies.* Retrieved from https://www.iiss.org/online-analysis/online-analysis/2022/12/digital-silk-road-introduction/

Grandin, A. (2023). Cyberspace Geography and Cyber Terrain: Challenges Producing a Universal map of Cyberspace. *European Conference on Cyber Warfare and Security*. 22 (1) 207-213.

Gravett, W. (2020). Digital neo-colonialism: The Chinese model of internet sovereignty in Africa. *African Human Rights Law Journal*, *20*(1), 125-146.

Greene, R. & Triolo, P. (2020) Will China Control the Global Internet via its Digital Silk Road? *Carnegie Endowment for International Peace*. Retrieved from https:// carnegieendowment.org/2020/05/08/will-china-control-global-internet-via-its-digital-silk-road- pub-81857.

Griffiths, J. (2019) The great firewall of China: How to build and control an alternative version of the internet. London: Zed Books.

Griffiths, James. (2019) *The great firewall of China: How to build and control an alternative version of the internet*. London: Zed Books.

Grotto, A. (2019). The Huawei problem: A risk assessment. *Global Asia*, *14*(3), 13-15.

Hajer, M. (2003). Policy without polity? Policy analysis and the institutional void. *Policy sciences*, *36*(2), 175-195.

Hernandez, K. (2019) Achieving Complex Development goals along China's Digital Silk Road. *Institute of Development Studies.*

Hillman, J. E. (2021). *The digital silk road: China's quest to wire the world and win the future*. Profile Books.

Hirono, M., & Suzuki, S. (2014). Why do we need 'myth-busting'in the study of Sino–African relations?. *Journal of Contemporary China*, *23*(87), 443-461.

Hoffman, S. (2019) Engineering Global Consent. *International Cyber Policy Centre.* Australian Strategic Policy Institute.

Huang, Y. (2019) Construction of Digital Silk Road Lights Up BRI Cooperation.*People's Daily*. Retrieved from http://en.people.cn/n3/2019/0424/c90000-9571418.html.

Human Rights Watch (2009) Analysis of Ethiopia's Draft Anti-Terrorism Law. *Human Rights Watch.* Retrieved from https://www.hrw.org/news/2009/06/30/analysis-ethiopias-draft-anti-terrorism-law

Human Rights Watch (2014). They Know Everything We Do: Telecom and Internet Surveillance in Ethiopia. *Human Rights Watch.* Retrieved 20 March 2020 from https://www. hrw.org/ report/2014/03/25/they-know-everything-we-do/telecom-and-internet- surveillance-ethiopia.

Hurel, L. M., & Lobato, L. C. (2018). Unpacking cyber norms: private companies as norm entrepreneurs. *Journal of Cyber Policy*, *3*(1), 61-76.

Jayawardane, S., Larik, J.& Jackson, E. (2015) Cyber Governance: Challenges, Solutions, and Lessons for Effective Global Governance. *The Hague: The Hague Institute for Global Justice.* Retrieved from https://www.thehagueinstituteforglobaljustice.org/portfolio/cyber-governance-challenges-solutions-and-lessons-for-effective-global-governance/.

Jensen T. (2015). Cyber Sovereignty: The Way Ahead. *Texas International Law Journal*. 50 (2) 274-302.

Katzenstein, P. J. (1996). *Cultural Norms and National Security: Police and Military in Postwar Japan*. Cornell University Press.

Kazeem, Y. (2019). The Biggest Mobile Phone Maker in Africa Is Going Public in China. *Quartz Africa*. Retrieved from https://qz.com/africa/1583473/chinas-transsion-of-african-tecno-phones-to-ipo-in-shanghai/.

Kleinwachter, W. (2017) Internet Governance Outlook 2017: Nationalistic Hierarchies vs. Multistakeholder Networks? *CircleID.* Retrieved from https://circleid.com/posts/ 20160106_internet_outlook_2017_nationalistic_hierarchies_multistakeholder

Kperogi, F. A. (Ed.). (2022). *Digital dissidence and social media censorship in Africa*. Taylor & Francis.

Kurbalija, J. (2016). *An introduction to internet governance*. Diplo Foundation.

Kurlantzick, J. (2020) China's Digital Silk Road Initiative: A Boon for Developing Countries or a Danger to Freedom? *Diplomat*. Retrieved from https://thediplomat.com/2020/12/ chinas-digital-silk-road-initiative-a-boon-for-developing-countries-or-a-danger-to-freedom.

Lewis, J. A. (2010). Cyber war and competition in the China-US relationship. *Remarks delivered at the China Institutes of Contemporary International Relations*, *13*.

Lili, Z. (2009) Contributing to the Development of Ethiopia with Wisdom and Strength. *ZTE.* Retrieved from https://www.zte.com.cn/global/about/magazine/zte-technologies/2009/6/en_414/172517.html#:~:text=According%20to%20him%2C%20ZTE%20entered,not%20been%20made%20until%202006

Lin, D. (2013) Addis Ababa Confucius Institute Provides Chinese Training Program to ZTE. *Tianjin University of Technology and Education.* Retrieved from https://en.tute.edu.cn/info/1057/1208.htm

Liu, J. (2022). China's data localization. In *China's Globalizing Internet* (pp. 83-102). Routledge.

Lu, H., Rohr, C., Hafner, M., & Knack, A. (2018) China Belt and Road Initiative. *Cambridge & Santa Monica: RAND Corporation*.

Lu, Y. & Lu, K. & Zeng, L. (2018) China's outward foreign direct investment and the margins of trade: Empirical evidence from "one belt, one road" countries. *China: An International Journal*, 16, 129–151

Lubin, G. (2014) China's Ban On Puns Comes Straight Out Of '1984. *Business Insider*. Retrieved from https://www.businessinsider.com/chinas-orwellian-ban-on-puns-2014-12?r=US&IR=T

Ly, B. (2020). Challenge and perspective for Digital Silk road. *Cogent Business & Management*, *7*(1), 1804180.

Mackinnon, A. (2019). For Africa, Chinese-Built Internet is Better Than No Internet at All. *Foreign Policy.* Retrieved from https://foreignpolicy.com/2019/03/19/for-africa-chinese-built-internet-is-better-than-no-internet-at-all/

MacKinnon, R. (2011). China's" networked authoritarianism". *J. Democracy*, *22*, 32.

Mahoney, J. (2012) The Logic of Process Tracing Tests in the Social Sciences. *Sociological Methods & Research*. 41(4): 570–597.

Malakata, M. (2012) Algerian ban on ZTE, Huawei highlights corruption controversy. *ComputerWorld Zambia.* Retrieved from http://news.idg.no/cw/art.cfm?id=D7DAD3FD-F26D-177C- 2EF38733406952D7

Malakata, M. (2013) Zambian terminates KSh. 18.4 billion ZTE contract over corruption allegations. *CIO.* Retrieved from http://www.cio.co.ke/news/top-stories/ zambian-terminates-ksh.-18.4-billion-zte-contract-over- corruption-allegations

McKune, S.L. & Ahmed, S. (2018). Authoritarian Practices in the Digital Age| The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda. *International Journal of Communication, 12* (21).

Ministry of Foreign Affairs of the PRC (2017). *International Strategy of Cooperation on Cyberspace*. Retrieved from https://www.fmprc.gov.cn/mfa_eng/

Ministry of Foreign Affairs. (2021) China Will Work with Africa to Formulate and Implement a China-Africa Partnership Plan on Digital Innovation. China.

Moore, G. J. (2023). Huawei, cyber-sovereignty and liberal norms: China's challenge to the west/democracies. *Journal of Chinese Political Science*, *28*(1), 151-167.

Mueller, F. (2015) Model transfer in the making: changing development strategies of, and expectations towards, the state in Ethiopia and Ghana, DFG Working Papers.

Nocetti, J. (2015) Contest and conquest: Russia and global internet governance. *International Affairs*, *91*(1), 111-130.

Pathfinder. (2011) *What Is Cyberspace? Examining its Components*. Australia. https:// airpower.airforce.gov.au/APDC/media/PDF-Files/Pathfinder/PF153-What-is-Cyberspace_-Examining-its-Components.pdf.

Prasso, S. (2019) China's Digital Silk Road Is Looking More Like an Iron Curtain. *Bloomberg Businessweek*. Retrieved from https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain.

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: anatomy of an inchoate global institution. *International Theory*, *7*(3), 572-616.

Reed, J. (2013). Is Tech Firm a Front for China to Spy? *IOL.* Retrieved http://www.iol.co.za/scitech/technology/security/is-tech- firm-a-front-for-china-to-spy1.1556887#.UvQBwmJ5Pcw.

Reporters Without Borders (2006) Desperate Meles blocked ethiomedia. *Cyber Ethiopia.* Retrieved from https://www.cyberethiopia.com/warka14/viewtopic.php?f=1&t=17395#p161346

Sarefo, S. & Dawson, M. & Mphago, B. (2023) An exploratory analysis of the cybersecurity threat landscape for Bostswana. *Procedia Computer Science.* 219, 1012-1022.

Schaffer, B. (2023). *From Rising Power to Cyber Influencer?: China's Norm Entrepreneurship in Global Cyber Governance through Cyber Sovereignty and Multilateralism Unraveling China's Impact on Kenya's Domestic Regulatory Framework* (Bachelor's thesis, University of Twente).

Schneider, Florian (2021). *Global Perspectives on China's Belt and Road Initiative: Asserting Agency through Regional Connectivity*. Amsterdam, Amsterdam University Press.

Segal, A. (2017) Chinese cyber diplomacy in a new era of uncertainty. *Hoover Institution, Aegis Paper Series*, 1703, 1-23.

Segal, A. (2020). China's alternative cyber governance regime. *Council on Foreign Relations*, 1-8.

Shen, H. (2016). China and global internet governance: toward an alternative analytical framework. *Chinese Journal of Communication*, *9*(3), 304-324.

Shen, H. (2018). Building a digital silk road? Situating the internet in China's belt and road initiative. *International Journal of Communication*, *12*, 19.

Simmons, B. A., Dobbin, F., & Garrett, G. (2006). Introduction: The international diffusion of liberalism. *International organization*, *60*(4), 781-810.

Sisay, A. (2013) Ethiopia Telecom Sector to Remain a Monopoly. *Africa Review.* Retrieved from http://www.africareview.com/Business---Finance/Ethiopia-telecom-sector-to-remain-a-state-monopoly/-/979184/1896796/-/9hitv4/-/index.html

Sun, Y. (2016) Political Party Training: China's Ideological Push in Africa? *Brookings Institute*. Retrieved from https://www.brookings.edu/blog/africa-in-focus/2016/07/05/political-party-training-chinas-ideological-push-in-africa/.

Taye, B. & Teshome, R. (2018) Privacy and Personal Data Protection in Ethiopia. *Collaboration on International ICT Policy in East and Southern Africa (CIPESA)*. Retrieved from https://cipesa. org/?wpfb_dl=301.

Triolo, P. (2020). The Digital Silk Road and the evolving role of Chinese technology companies. *Adelphi Series*, *60* (487-489), 65-88.

United Nations Office on Drugs and Crime, *Telecom Fraud Offence Proclamation*, Proclamation No. 761 (2012), available from https://sherloc.unodc.org/cld/document/eth/2012/telecom_fraud_offence_proclamation.html

Vaidyanathan, V. & Gomera, J. (2019) Power and Communication Infrastructure in China's Infrastructure Development, in *Africa: An Examination of Projects in Tanzania and Kenya*, ed. Veda Vaidyanathan. Delhi: Institute of Chinese Studies.

Van der Lugt, S. (2021). Exploring the political, economic, and social implications of the Digital Silk Road into East Africa. *Global Perspectives on China's Belt and Road Initiative: Asserting Agency through Regional Connectivity*, 315-346.

Van Eeten, M. J., & Mueller, M. (2013).Where is the governance in Internet governance? *New media & society*, *15*(5), 720-736.

Wang, A. (2020). Cyber Sovereignty at Its Boldest: A Chinese Perspective. *Ohio St. Tech. LJ*, *16*, 395.

Wang, Jiangyu. (2016)Geopolitics, Discursive Power and International Law-Making behind the One Belt, One Road Initiative. *China Law Review* 2: 39-45.

Wang, Y., & Li, H. (2023). African Media Cultures and Chinese Public Relations Strategies in Kenya and Ethiopia. *Carnegie Endowment for International Peace.*

Wanyama, E. (2020) Ethiopia's New Hate Speech and Disinformation Law Weights Heavily on Social Media Users and Internet Intermediaries. *CIPESA.* Retrieved from https://cipesa.org/2020/07/ethiopias-new-hate-speech-and-disinformation-law-weighs-heavily-on-social-media-users-and-internet-intermediaries/

Weber, V. (2021) *The diffusion of cyber norms: technospheres, sovereignty, and power* (Doctoral dissertation, University of Oxford).

Wei, Y. (2018) Chinese Data Localization Law: Comprehensive but Ambiguous. *The Henry M. Jackson School of International Studies,* University of Washington. Retrieved from https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/

Wendt, A. (1992). Anarchy is what states make of it: the social construction of power politics. *International organization*, *46*(2), 391-425.

West, S. (2014). Globalizing Internet governance: negotiating cyberspace agreements in the post-snowden era. In *2014 TPRC Conference Paper*.

Winston, C. (2018). Norm structure, diffusion, and evolution: A conceptual approach. *European Journal of International Relations*, *24*(3), 638-661.

Workneh, T. W. (2014). The politics of telecommunications and development in Ethiopia (Doctoral dissertation, University of Oregon).

Wu, X., & Gereffi, G. (2018) Amazon and Alibaba: Internet governance, business models, and internationalization strategies. In *International business in the information and digital age* (pp. 327-356). Emerald Publishing Limited.

Yau, H. M. (2021). Fragmenting Cyberspace and Constructing Cyber Norms: China's Efforts to Reshape Global Cyber Governance. *Contemporary Chinese Political Economy and Strategic Relations: An International Journal*, *7*, 691-715.

Ye, Q. (2020). Promoting the Organic Integration of the Party's Leadership System and the Governance System of Private Enterprises. Beijing.

Yeli, H. (2017). A three-perspective theory of cyber sovereignty. *Prism : A Journal of the Center for Complex Operations, 7*(2), 108-120. Retrieved from https://www.proquest.com/scholarly-journals/three-perspective-theory-cyber-sovereignty/docview/2002984208/se-2

Yilma K.M. & Abraha H.H., (2015) The Internet and regulatory responses in Ethiopia: Telecoms, cybercrimes, privacy, e-commerce, and the new media. *Mizan Law Review* 9 (1) 108–153.

Yilma, K. M. (2017) Fake news and its discontent in Ethiopia. *Mekelle ULJ*, *5*, 98.

Yilma, M. (2016) 'Some Remarks on Ethiopia's New Cybercrime Legislation. *African Journals Online.* 10(2) 448-458.

Zhao, Kejin. 2016. "China's Rise and its Discursive Power Strategy." *Chinese Political Science Review.* **1**: 539–64.

Ziso, E. (2020) The Political Economy of the Chinese Model in Ethiopia. *Politics Policy*, 48: 908-931. https://doi.org/10.1111/polp.12374