Check for updates

The geopolitics of infrastructuralized platforms: The case of Alibaba

Hong Shen[a] and Yujia He [b]

aHuman-Computer Interaction Institute, Pittsburgh, Carnegie Mellon University, USA; bPatterson School of Diplomacy and International Commerce, University of Kentucky, USA

ABSTRACT

Contemporary digital platforms have become increasingly infrastructuralized, and started to raise geopolitical tensions with their global expansion. Amidst the heightened geopolitical competition between the US and China, the growing power of Chinese infrastructuralized platforms has made them the center of recent geopolitical dynamics. Drawing from an exploratory case study, this paper discusses Alibaba, one of the most prominent Chinese Internet giants, as an infrastructuralized platform, and highlights its geopolitical struggles. Often perceived as an e-commerce company, Alibaba has become 'infrastructuralized': its now-massive digital empire has moved beyond e-commerce, expanding into almost every aspect of China's and global digital economy such as logistics, finance, offline retailing, and cloud computing. This paper traces three highly visible cases in Alibaba's global journey – its failed deal with MoneyGram in 2017, the uneven global journey of Alibaba Cloud, and the construction of the electronic World Trade Platform – to illustrate three key dimensions of the geopolitics of infrastructuralized platforms – namely, the geopolitics of everyday data, the geopolitics of the visibility-invisibility tension, and the geopolitics of modularity. By doing so, it contributes to the following two areas of scholarship. On the one hand, it contributes to the growing literature on 'infrastructures and platforms' by foregrounding the geopolitical dimensions of Chinese infrastructuralized platforms. On the other hand, it adds to the literature on the 'geopolitics of infrastructures' by bringing in a new type of infrastructure, complementing previous discussions on the geopolitics of traditional material infrastructures.

Introduction

Digital platforms have exercised enormous power over many aspects of our everyday lives, controlling which advertisements, social media posts, and search results we see, how we receive our online purchases and offline rides, and how we are represented to our peers. In some sense, they are being 'infrastructuralized,' comparable to the roles of traditional infrastructures like water, electricity, and gas in supporting the functioning

CONTACT Hong Shen ✉ hongs@cs.cmu.edu; hongshenus@gmail.com 🖼 Human-Computer Interaction Institute, Carnegie Mellon University, 5000 Forbes Ave, Pittsburgh, PA 15213

of society (Plantin et al., 2018). Such unprecedented power, once expanded internationally, can generate geopolitical tensions. For example, since 2010, several antitrust investigations by the European Union have been launched against Google for violating the EU's competition laws (European Commission, 2019).

Among all the infrastructuralized platforms that have experienced geopolitical tensions, Chinese digital platforms stand out as particularly significant. Amidst heightened geopolitical competition between the US and China over the global technology landscape, the growing power of Chinese digital platforms and their global expansion have made them the center of recent geopolitical dynamics. For example, the overseas expansion of digital services provided by firms such as Alibaba, Baidu, Tencent, and ByteDance has led to diverse reactions in Europe, the US, Asia, and Africa, ranging from enthusiastic fanfare to outright bans (Cartwright, 2020; Gray, 2021; Logan, 2015; Naughton, 2020).

Previous literature on the geopolitics of infrastructures has surveyed the geopolitics around a range of traditional material infrastructures such as roads, bridges, energy pipelines, and undersea cables (Anastasiadou, 2019; Bahgat, 2002; Headrick, 1991; Jia & Bennett, 2018; Starosielski, 2015). Yet the emergent tensions around infrastructuralized platforms have received limited attention. Meanwhile, literature concerning how digital platforms, including Chinese platforms, have become infrastructuralized has so far primarily focused on the domestic side (Plantin & De Seta, 2019; Shen et al., 2020; Zhang, 2021). What remains underexplored is the geopolitics of these infrastructuralized platforms when they actively expand into the global Internet. What are the key features of their geopolitical struggles?

This paper aims to fill this gap by examining the rising geopolitical tensions of a major Chinese infrastructuralized platform: Alibaba. As scholars posit, infrastructures assume some key properties (Bowker & Star, 2000; Star, 1999). For example, they often have a ubiquitous reach and scope. They are deeply embedded in existing technical structures and social environments; thus, they tend to become invisible and transparent. According to this definition, Alibaba has indeed become 'infrastructuralized' (Shen, 2021): Its now-massive digital empire has moved beyond e-commerce, expanding into almost every aspect of China's and global digital economy – from logistics to finance to cloud computing. Deeply embedded in existing technical systems and social practices, it also becomes invisible in terms of people's awareness of the underlying technological system supporting their actions and interactions. However, Alibaba also represents a new type of infrastructure: as an 'infrastructuralized platform,' it commands an enormous scale of everyday data, navigates between visibility and invisibility, and connects a variety of complementary components both online and offline via modular interfaces. All of them have introduced new types of geopolitical tensions.

This paper makes several contributions. Empirically, we contribute detailed case analyses of Alibaba's global expansion, adding to the literature on the international expansion of Chinese infrastructuralized platforms. Using Alibaba's three highly visible geopolitical endeavors as cases (Ragin & Becker, 1992) – its failed deal with MoneyGram, the uneven global journey of Alibaba Cloud, and the construction of the electronic World Trade Platform, this paper discusses the geopolitical implications of Alibaba as an infrastructuralized platform in today's contentious landscape of the global Internet. Moreover, the findings from the case also illustrate several key dimensions of the geopolitics of infrastructuralized platforms, an emerging but vital type of infrastructures

of our time, thus enriching our understanding of the geopolitics of infrastructures. Indeed, the geopolitical incidents are not merely challenges for a particular Chinese Internet company facing an intensifying geopolitical environment. They also exemplify the complicated geopolitics surrounding corporate-owned, profit-oriented digital platforms when they increasingly become the basic infrastructure of the global Internet.

Literature review

In this section, we outline past work in two areas. First, we present an overview of existing work on infrastructures and platforms, a growing field in media and communication studies, and describe how our work contributes to this research. Next, we illustrate how our work on the geopolitics of infrastructuralized platforms relates to and contrasts with extant literature on the geopolitics of traditional infrastructure, making contributions by bringing in features related to this new type of infrastructure.

Infrastructures and platforms

Infrastructures – often referring to capital-intensive material outcomes, such as railways, electricity grids and cable networks – have been extensively studied in political science, geography, and area studies (Edwards et al., 2009; Graham & Marvin, 2001; Hughes, 1983). Science and Technology Studies (STS) scholars add to this literature by highlighting the socio-technical aspects of infrastructures (Bowker & Star, 2000; Star, 1999), such as embeddedness and transparency. Meanwhile, media and communication scholarship concerning modern digital platforms examine how computing devices and software have a critical influence on the properties of applications built on them (Bogost & Montfort, 2009; Gillespie, 2010; Langlois & Elmer, 2013). Recently, Plantin et al. (2018) argued that the rapid development of digital technologies has made possible a '"platformization" of infrastructures and an "infrastructuralization" of platforms'. Using Google and Facebook as examples, they showed how corporate-owned digital platforms have increasingly assumed properties associated with public-controlled infrastructures, such as ubiquity, indispensability, and invisibility, and how this process has introduced new tensions.

Since then, studies have emerged in the context of the Chinese Internet, highlighting how digital platforms have been infrastructuralized in China. For example, Plantin and De Seta (2019) examined how WeChat, one of the most popular Chinese social media applications, has become infrastructuralized in the context of China's techno-nationalist media regulations and increasingly overt cyber-sovereignty agenda. Based on interviews and survey data, Shen et al. (2020) studied how mobile payment platforms, such as Alipay and WeChat Pay, have become basic financial infrastructures in China. Zhang (2021) discussed the infrastructuralization of TikTok in China and highlighted the changing power relationships between different players of the Chinese government and video entertainment platforms. Chen and Qiu (2019) investigated the ride-hailing platform Didi Chuxing to demonstrate that it has become a digital utility provider in urban China, adding to the discussions of 'infrastructuralization of platforms'.

Despite this growing attention, discussions around the geopolitics of Chinese infrastructuralized platforms in the global Internet, however, are still lacking. Although recent literature has examined the geopolitics of specific Chinese Internet companies

(Cartwright, 2020; Gray, 2021; Jia & Liang, 2021; Tang, 2020), relatively little attention has been paid to the geopolitics of these companies through the theoretical lens of infrastructuralized platforms.

Geopolitics of infrastructures

Scholarship in international relations, geography, communication, and area studies has discussed the geopolitics of a range of large-scale material infrastructures, in sectors such as energy (Bahgat, 2003), transport (Anastasiadou, 2019), and communications (Bueger & Liebetrau, 2021; He, 2019; Headrick, 1991; Schiller, 2011; Starosielski, 2015; Winseck, 2017). In particular, media and communication scholars argue that the control of global information infrastructure – from submarines cables in the nineteenth century, to wireless telegraphy in the early twentieth century, to the global network system in World War I and II – has long been a priority of imperialist state powers (Schiller, 2011; Tworek, 2019).

The rise of infrastructrualized platforms in the global Internet, however, raised new questions. As critical platform studies scholars argue, digital platforms possess unique characteristics, such as programmability, affordances and constraints, the connection of heterogeneous actors, and the accessibility of data (Bogost & Montfort, 2009; Gillespie, 2010; Langlois & Elmer, 2013; Plantin et al., 2018). Those features generate new geopolitical implications when platforms become infrastructuralized in their global expansion. Below we compare, discuss and illustrate how the geopolitics of infrastructuralized platforms connect with but also differentiate from the geopolitics of traditional infrastructures, in three key dimensions.

The geopolitics of everyday data

The first key dimension concerns the geopolitics of everyday data. Keohane and Nye (1998), in their study about information in international relations, distinguished three types of information as sources of state power. Specifically, they emphasized that strategic information, such as information about key weapons programs, is what states seek to acquire and protect, for they could confer advantages on states if the competing states do not possess it. Literature concerning the geopolitics of communications infrastructures also shows how strategic information traveled via cables and wires can be used to influence geopolitical competition (Bueger & Liebetrau, 2021; Headrick, 1991). For example, Headrick (1991) argued that telecommunications infrastructure conferred strategic advantages on nation-states, particularly in the conduct of war.

Yet the distinction between strategic information and non-strategic information is increasingly blurred in today's geopolitical context (Rosenbach & Mansted, 2019), partly owing to the rise of powerful transnational digital platforms. A central feature of these infrastructuralized platforms is the possession of enormous amounts of everyday and seemingly non-strategic data, contributed actively or inactively via their large-scale user bases (Plantin et al., 2018). Even the most mundane types of data - from locations, emails to daily behaviors - can become strategic once aggregated, processed, and analyzed via computational methods such as machine learning (Napoli, 2019). For example, data about exercise routes shared by soldiers via the fitness tracking app Strava can be used to

pinpoint US overseas military facilities (Hern, 2018). In addition, the data about foreign citizens in their everyday lives can be used to influence how they think and act, thus becoming a strategic tool of state influence. Different from traditional information infrastructures, whose geopolitical tension arises often because of their ability to carry strategic information for nation-states, infrastructuralized platforms that operate across national boundaries and gather huge amounts of everyday information from ordinary citizens, have increasingly become the prime targets for state scrutiny and geopolitical pressures.

The geopolitics of the visibility-invisibility tension

The second key dimension concerns the geopolitics of the visibility-invisibility tension. Literature on the geopolitics of traditional infrastructures suggests that highly visible infrastructures may lead to more geopolitical interests at stake, greater geopolitical tensions, and stronger public opposition to potential negative impacts. For instance, electricity grids, hydropower dams, cross-border railways, transport corridors, or smart cities built from scratch are likely to generate public opposition, due to the high visibility of their construction and their socio-economic and environmental impacts (He & Tritto, 2022; Jia & Bennett, 2018). Particularly for projects backed by transnational partnerships, even when host country governments enthusiastically support the projects, concerns may grow among political elites, opposition parties, and the public about the strategic implications of foreign influence. In comparison, infrastructure built wholly within a country, in remote locations with less visibility in the public eye, for example, domestic energy pipelines, are less likely to incur geopolitical concerns and public opposition (Jia & Bennett, 2018).

However, geopolitics surrounding infrastructuralized digital platforms are growing today despite their continued 'invisibility' in the public eye, or more precisely, because of the growing tension between their continued 'invisibility' and other efforts to make them 'visible'. On the one hand, unlike some traditional infrastructures mentioned above, information systems can become deeply 'embedded' or 'sunk' into existing technical systems and social/cultural practices, thus becoming 'invisible' to the public, in terms of people's awareness of the underlying technological system (Bowker & Star, 2000). Such invisibility has been further reinforced by popular imaginations and public discourses portraying digital platforms as 'invisible' and 'borderless' (Mosco, 2014). On the other hand, scholars, activists, and governments have made significant efforts in the past decade to make such 'invisible' platforms 'visible' – for example, scholars have pointed out that many core services of contemporary Internet platforms are supported by massive physical networks (e.g., data centers, undersea cables), instead of being 'immaterial' (Hu, 2015; Mosco, 2014; Starosielski, 2015). Indeed, recent geopolitical incidents have demonstrated that these perceived 'invisible' platforms are territorially bounded, subject to state power and geopolitical pressures.

The geopolitics of modularity

The third key dimension of the geopolitics of infrastructuralized platforms concerns the geopolitics of 'modularity'. We borrow this term from management and organizational

studies, which identify three key elements to the architecture of platforms: the low-variety core components, the high-variety complementary components, and the modular interfaces. For platforms, modularity enables the connection and coordination across different components of a system that are produced by different organizations, thus reducing frictional transaction costs (Baldwin & Clark, 2000; Baldwin & Woodard, 2009; Jacobides et al., 2018). However, as scholars from critical platform studies argue, there are uneven power relations embedded in modularity – digital platforms often leverage such programmability and interconnection to achieve control, and modularity is constantly 'negotiated between a core unit with low variability and heterogeneous components of high variability' (Plantin et al., 2018, p. 298).

Unlike traditional infrastructure often meant to provide essential services with broader public value and to achieve interoperability through negotiable standards, infrastructuralized platforms remain 'centrally controlled and designed system (often under corporate control) but benefit from the innovations of a large penumbra of third-party developers' (Plantin et al., 2018, p. 299). While modularity allows for the coordination of independent yet interdependent firms (Jacobides et al., 2018), the process of negotiating modularity confers unequal power among the different players within the system. Geopolitical tensions may arise when smaller, independent firms and users face increasing dominance of the firm in control of the platform's core component.

Furthermore, an infrastrctrualized platform's expansion, particularly in a foreign country, does not take place in a vacuum: The contexts for negotiating modularity are not just technical, but also social, cultural, and political. Different from purely material infrastructures (Anastasiadou, 2019), infrastructuralized platforms' expansion occurs in both offline and online spaces, producing both material components such as data centers or logistics centers, and immaterial components such as user data. The core firm's advantage in the platform may incur political implications, which various government units and corporate players may, in turn, seek to exploit, challenge, or avoid.

Methodology

In this paper, we asked: How can we better understand the geopolitics of Chinese infrastructuralized platforms when they have actively expanded into the global Internet? What are the key features of their geopolitical struggles?

To answer these questions, we adopted an exploratory case study approach (Ragin & Becker, 1992), using Alibaba, one of the most prominent Chinese Internet giants, as our case. There are several considerations behind our focus on Alibaba. First, although seen primarily as an e-commerce company, Alibaba was actually 'infrastructuralized' not only in China but also the global Internet (Shen, 2021). Its enormous corporate system consists not only of its core in e-commerce, but also the supporting layers of logistics, payment and finance, cloud computing, and the outermost layer that extends from media and entertainment to healthcare. Secondly, Alibaba is unique among Chinese Internet giants as an excellent example of an 'infrastructure-based platform,' because it has an exceptional presence both online and offline, deeply integrating its virtual businesses (e-commerce, finance, cloud computing) with the real world.

Specifically, we looked for important subcases with rich empirical data in Alibaba's history that serve as vehicles to illustrate the unique geopolitical dimensions of

infrastructuralized platforms digested via literature review. Eventually, we settled on three examples in Alibaba's global journey – its failed deal with MoneyGram in 2017, the uneven global journey of Alibaba Cloud, and the construction of the electronic World Trade Platform – to illustrate three key dimensions of the geopolitics of infrastructuralized platforms – namely, the geopolitics of everyday data, the geopolitics of the visibility-invisibility tension, and the geopolitics of modularity.

We conducted a two-tiered document analysis of English- and Chinese-language sources. We began by conducting a systematic review of trade journals, news articles, and scholarly literature on the geopolitics of Alibaba to understand the larger political and socioeconomic context. Following our review, we went on to find and analyze relevant documents, such as official government policies, interviews and speeches from government officials and Internet executives. A deeper analysis of policy discourse was then combined with the knowledge from the first step, to create a comprehensive understanding of both policy discourses and geopolitical and political-economic contexts (Shen, 2016, 2018). Data analysis was performed concurrently with data collection to compare the initial findings of the case against the theoretical lens, derived from the literature review. We seek to discover patterns and develop further mappings by sifting through the empirical data, theoretical perspectives, and relevant literature.

MoneyGram and the geopolitics of everyday data

Alibaba's unsuccessful $1.2 billion deal with money transfer company MoneyGram signifies the first key dimension of infrastructuralized platforms: The geopolitics of everyday data. In April 2017, Ant Financial, Alibaba's financial arm, proposed to acquire Money-Gram, a Dallas-based money transfer company, for an $18 per share all-cash deal. Alibaba considered MoneyGram as a good opportunity for its expansion to the markets outside of China, as MoneyGram has approximately 350,000 remittance outlets in more than 200 countries. Only Western Union, which owns more than 550,000 locations worldwide, has a comparable global footprint (Mashayekhi, 2020). In December 2017, however, Ant Financial announced that it decided to terminate the deal after the Committee on Foreign Investment in the United States (CFIUS), a Treasury Department interagency committee that reviews foreign investments in US companies, rejected its proposals based on concerns over the potential national security impact of foreign investment (Roumeliotis, 2018).

Unlike Chinese networking and hardware companies (e.g., Huawei), which were historically subject to scrutiny on national security concerns when entering the US market, Alibaba as an e-commerce service provider has had a much less controversial record in overseas mergers and acquisitions (Shen, 2017; Shen, 2021). For example, Alibaba started investing large amounts of capital overseas in 2013. From 2013 to 2017, Alibaba executed 18 successful overseas deals each valued at $100 million or above. These deals targeted not only neighboring countries such as India, Singapore, and Japan, but also the center of global digital capitalism, the US. They were also diversified into different market sectors, including the e-commerce sector such as deals with ShopRunner in the US and Lazada in Singapore, logistics such as deals with Singapore Post, and social media and online gaming segments such as deals with TangoMe and Snapchat. The failed $1.2 billion acquisition of MoneyGram at the end of 2017, therefore, represented Alibaba's first

major failure in overseas mergers and acquisitions (Please see Table 1 for major overseas deals initiated by Alibaba from 2013 to 2017).

Admittedly, the failed Ant-MoneyGram deal was not the only Chinese investment rejected by the CFIUS under the Trump administration. For instance, just before the Ant-MoneyGram deal, the CFIUS rejected China-based buyout fund Canyon Bridge's $1.3 billion purchase of US chip maker Lattice Semiconductor (Roumeliotis, 2018). It should indeed be understood within the increasingly heightened geopolitical competition between the US and China over the global technology landscape as well as the increasingly toughened stance of the US government towards Chinese investments, which can also be observed via the significant power expansion of the CFIUS (Zimmerman, 2019). However, different from the Canyon Bridge-Lattice Semiconductor case, which happened in the highly sensitive semiconductor industry, the Ant-MoneyGram deal shows how the centrality of everyday data in infrastructuralized platforms can ignite significant geopolitical tensions.

Reportedly, Ant Financial decided to terminate the deal because the CFIUS rejected their proposal to mitigate the safety of data that can be used to 'identify US citizens' (Roumeliotis, 2018). However, since MoneyGram does not operate in the defense sector nor does it deal with critical infrastructure such as semiconductors, even within the seemingly unified US policy circles, there were divergent views regarding whether the data MoneyGram holds should be considered as related to 'national security'. For example, James Pethokoukis, a senior fellow at the American Enterprise Institute (AEI), questioned such national security reasoning. He argued that since the average transfer of MoneyGram is only about $300, the personal data it holds is similar to 'what you would hand over when signing up for a fitness club membership' (Pethokoukis, 2018). Others suggested that the proposed deals might involve much more detailed financial information (Barfield, 2018). For example, if the deal succeeded, the data

Table 1 . Major overseas deals initiated by Alibaba (2013–2017). The Ant-MoneyGram deal was the first failure in Alibaba's overseas mergers and acquisitions.

Year	Month	Transaction Party	Quantity in Million (USD)	Country	Status
2013	October	ShopRunner (consumer)	$110	USA	Successful
2014	Feb.	One 97 (consumer)	$200	India	Successful
2014	March	TangoMe (technology)	$220	USA	Successful
2014	May	Singapore Post (logistics)	$210	Singapore	Successful
2014	July	Kabam (entertainment)	$120	USA	Successful
2015	March	Snapchat (entertainment)	$200	USA	Successful
2015	July	Singapore Post (logistics)	$150	Singapore	Successful
2015	August	Snapdeal (consumer)	$200	India	Successful
2015	Sept.	One 97 (consumer)	$680	India	Successful
2016	Feb.	Groupon (consumer)	$130	USA	Successful
2016	Feb.	Magic Leap (Entertainment)	$160	USA	Successful
2016	April	Lazada (consumer)	$1,000	Singapore	Successful
2017	Feb.	Kakao (consumer)	$200	South Korea	Successful
2017	Feb.	Mynt (consumer)	$190	Philippines	Successful
2017	March	Paytm Mall (consumer)	$180	India	Successful
2017	June	Lazada (consumer)	$1,000	Singapore	Successful
2017	August	Tokopedia (consumer)	$500	Indonesia	Successful
2017	October	Magic Leap (entertainment)	$100	USA	Successful
2017	Dec.	MoneyGram (finance)	$1,810	USA	Failed

Source: American Enterprise Institute, 'China Global Investment Tracker'. Note that only deals valued over $100 million are included in the dataset.

MoneyGram holds might be further integrated, processed and analyzed via computing techniques, which might then generate concerns over national security. Indeed, given the central position of everyday customer data in the business operations of contemporary digital platforms, the line between strategic versus non-strategic data has become increasingly blurred.

Alibaba Cloud and the geopolitics of the visibility-invisibility tension

The uneven development of the Alibaba Cloud illustrates the second geopolitical dimension of infrastructuralized platforms: The geopolitics of the visibility-invisibility tension. Cloud computing has increasingly become the utility infrastructure of our time for its ability to serve and connect a variety of services and functions – from online shopping, to databases, to storage, to AI and machine learning applications (Hillman, 2021). Cloud providers rent out computers, networks and services to users around the world, so corporations don't have to build their own technological infrastructure. These globally distributed clouds, however, have also led to increasing concerns about where the infrastructure underneath these services is built and how it is administered (Herr, 2020).

As an infrastructuralized platform, Alibaba has increasingly considered cloud computing as a core competitive advantage among its services. Alibaba set foot in the fast-growing cloud business in 2009 and has since grown in bounds and strengths. By March 2020, its cloud computing facilities were already the third largest globally, and the largest in China and the Asia Pacific region, competing directly with Amazon Web Services (AWS) (Alibaba Group, 2020a). In 2020, Alibaba further announced that it would spend $28 billion over the next three years to compete with major Western providers in the global cloud computing market (Herr, 2020).

Despite this significant progress, Alibaba Cloud remains largely 'invisible' from the public eye. Different from traditional material infrastructures, cloud computing is deeply embedded within existing technical systems to support the operations of other businesses. They therefore largely remain 'hidden' to policymakers (Herr, 2020). In addition, similar to many contemporary information systems, the pervasiveness and ubiquity of cloud computing also led to its sinking into people's everyday practices, thus becoming 'invisible' to its users in terms of their awareness of the underlying technological systems. Alibaba itself has also actively taken advantage of and negotiated such 'invisibility' by branding its cloud service as 'lighter,' 'thinner,' and 'boundless' (Guo, 2021). Recently, however, such invisibility has been challenged in the geopolitical context.

First, the geopolitics of Alibaba Cloud can be observed via the unequal geographical distribution of Alibaba's data centers supporting its massive operation. As scholars posit, cloud computing, far from being 'immaterial' and 'boundless,' is supported by massive physical data centers and grew out of previous network infrastructures (Hu, 2015; Mosco, 2014). Indeed, despite its significant global expansion, Alibaba's overseas data centers, so far, have largely constrained themselves to countries in Southeast Asia - a region that traditionally has closer diplomatic relations with China. For example, in 2020, Alibaba owns 60 data centers globally, among them an overwhelming majority – 49 located in East and Southeast Asia, only 4 in North America, and 4 in Europe. This offers a sharp comparison with Amazon AWS, which owns 76 global data centers, among which 25 are in North America, 18 in Europe, and 21 in East and Southeast Asia (Herr, 2020).

Second, apart from the uneven geographical distribution of its data centers, Alibaba Cloud has also increasingly become visible at the center of US-China technology disputes. Sometimes, when complex situations can be framed as a rivalry between 'us' and 'them,' public fear and opposition can be mobilized to generate strong policy interventions and escalate geopolitical tensions towards 'foreign cloud infrastructures,' even without their physical presence in the host country. For example, in 2020, the US State Department announced the 'Clean Network' initiative, specifically including a 'Clean Cloud' program, which deems the cloud services of Alibaba as unsafe. The Trump administration claimed that more than thirty countries and territories, including the ones not yet covered by Alibaba's data centers, have committed to the initiative. This means that corporations operating in those regions would not be able to rely on China-based cloud providers, which might effectively limit the ability of Alibaba Cloud to grow outside of China (Chitkara, 2020; US Department of State, 2020).

Finally, the seemingly 'invisibility' of Alibaba Cloud can become apparent when its collaboration with home country partners breaks down. On the one hand, Alibaba Cloud has increasingly become the basic infrastructure to help other Chinese firms in their ventures abroad. It is reported that in 2017, more than 100 Chinese software companies used Alibaba's cloud services for their global operation, including Musical.ly, the predecessor of TikTok (Lu, 2017). On the other hand, under escalating geopolitical tensions, such collaboration might also break down, which reveals the geopolitical boundary of cloud computing. In 2021, facing near-nonstop pressure from the US authorities, ByteDance (the parent company of TikTok) dropped Alibaba Cloud for its businesses outside China, moving to cloud services run by US companies like Amazon's AWS, which caused a significant loss to Alibaba Cloud (Yang et al., 2021).

In sum, contrary to the popular imagination of platforms as being 'immaterial' and 'invisible,' there have been growing efforts in the past decade from states, scholars and activists that tried to make 'invisible' platforms 'visible'. We saw similar tensions arise in Alibaba Cloud's global expansion, as illustrated by the uneven geographical distribution of its data centers, its central role in US-China technology disputes, and its complicated relationship with home country partners. As an infrastructuralized platform, Alibaba Cloud's invisibility arises not only from its 'embeddedness' into existing technical systems and users' daily practices, but also from its persistent branding efforts to promote itself as 'boundless'. However, significant geopolitical tensions have ensued from this seemingly 'invisible' service.

Electronic World Trade Platform (eWTP) and the geopolitics of modularity

The development of Alibaba's electronic World Trade Platform (eWTP) signifies the third dimension of the geopolitics of infrastructuralized platforms – namely the geopolitics of modularity. As chair of the 2016 B20 SME (small and medium-sized enterprises) Development Taskforce, Jack Ma called for establishing an electronic World Trade Platform (eWTP) to reduce trade barriers and promote SMEs' participation in e-commerce worldwide (Alibaba Group, 2016; Vila Seoane, 2020). By 2020, Alibaba has established eWTP hubs with local partners in Malaysia, Thailand, Rwanda, Ethiopia, and Belgium, besides its domestic hubs in Hangzhou, Yiwu, Hainan and Hong Kong (Alibaba Group, 2020b). As a private-sector-led initiative, eWTP aims to work with national

and local governments and firms to develop global networks in trading, logistics, financial services and public services critical to cross-border e-commerce. This new chapter in Alibaba's expansion in the global Internet may yield an Alibaba-centered global trade regime for e-commerce, with significant geopolitical implications.

Alibaba's eWTP hub in Malaysia, the Digital Free Trade Zone (DFTZ), is the first eWTP hub outside of China and has seen notable progress on the ground, thus presenting a suitable example. The Malaysian government had the goal of doubling the nation's e-commerce growth and increasing its GDP contribution to RM211 billion (US$47.68 billion) by 2020 (MDEC, 2016). Thus, it is keen to develop a free trade zone supported by one of the world's largest e-commerce platforms. In 2017, then Malaysian Prime Minister Najib Razak jointly launched the DFTZ with Jack Ma in the KLIA Aeropolis, the airport city hosting the Kuala Lumpur International Airport (Malaysian Ministry of Transport, 2017). DFTZ has received high-level support from the Malaysian government and other public entities despite the change of administration in the past few years (MDEC, n.d.).

As scholars of platform architecture posit, modularity in a platform can enable the coordination of independent and interdependent actors responsible for different parts of the production process, thus reducing transaction costs. In the case of the DFTZ, Alibaba's role, as the 'ecosystem builder,' has indeed connected a variety of different actors, as high-variety complementary components, to its platform (MITI, 2018). For instance, in Phase One of the e-fulfillment logistics hub development, Pos Malaysia, Malaysia's national postal service, partnered with Lazada, Alibaba's flagship e-commerce platform in Southeast Asia, to upgrade and renovate the former Low-Cost Carrier Terminal (LCCT) in KLIA (Yean, 2018). In the current Phase Two, Cainiao, Alibaba's logistics arm, partnered with Malaysia Airports Holdings, Malaysia's largest airport operator, to build its regional e-fulfillment hub in the KLIA Aeropolis DFTZ Park (Alibaba Group, 2020b). The hub, which opened in November 2020, has a centralized customs clearance, warehousing, and e-fulfillment facility. It connects to air and sea freight infrastructure and railway cargo, facilitating single-day delivery within Malaysia and later 72-hour delivery across Southeast Asia. In addition, the Malaysian government also does not envision the DFTZ as exclusive to Alibaba, thus bringing in an additional group of heterogeneous players. For example, apart from Alibaba and its affiliates, other platforms such as Amazon.com, eBay, Jocom, eRomman, Jin-BaoMen, tradeindia.com, DagangHalal.com, AladdinStreet.com.my, and Buy-Malaysia have been operating in the DFTZ (Kumar & Kuar, 2018).

However, through building and achieving modularity, Alibaba also shows the increasing potential of exercising power over the basic infrastructures critical to cross-border e-commerce in the DFTZ. For instance, in trading and logistics, Alibaba-controlled Lazada is among the first users of Malaysia's DFTZ e-fulfilment hub. In financial services, one in three e-commerce consumers in Malaysia already use Lazada Wallet powered by Alipay (The Edge Markets, 2020). Ant Financial has also partnered with Maybank and CIMB, Malaysia's two largest banks in merchant sales volume, to facilitate Alipay payment acceptance by offline merchants (Yean, 2018).

Alibaba's centralized position in the DFTZ extends beyond simple market domination. As the 'ecosystem builder,' the company has also leveraged programmability and interconnection to achieve control (Plantin et al., 2018). In other words, the high-variety

complementary components have been connected to the DFTZ in a landscape defined and controlled by the Alibaba platform. For example, taking the digital payment further to a ubiquitous offline presence, Alibaba's Ant Financial has formed a joint venture with Touch'N'Go, a unit of CIMB that runs the e-payment system for Malaysia's toll expressway and highway operators, to offer a mobile wallet modeled after Alipay. Literally every Malaysian aged over 12 has a TnG card (Touch'N'Go, 2017).

This has generated geopolitical concerns over whether the core position occupied by Alibaba and its affiliates could lead to the consolidated market power that affects the participating smaller firms and users in Malaysia. For instance, some Malaysian politicians are concerned that without a sufficient export-led growth strategy, the potential for local SMEs to boost export through cross-border e-commerce to the Chinese market would be limited, while local markets could be flooded with cheap imports (Tzin, 2021). As Alibaba collects large volumes of data through both online and offline segments of its business, concerns have also been voiced about data security for the average user, including the security of financial data stored on a service platform run by a foreign firm (Yean, 2020). Concerns also arise over whether competing platforms or services will continue to have a level playing field in the future or will need to follow the rules and standards defined by Alibaba (Chandran, 2018).

Discussion and conclusion

Among all the infrastructuralized platforms that have been subject to geopolitical tensions, Alibaba stands out as a particularly significant case. On the one hand, it has become a representation of China's growing digital power – the 'symbol of China's new tech strength' (McDonald, 2014). It has been consistently ranked as one of the ten largest Internet applications firms by market capitalization, competing directly with global giants like Amazon, Alphabet (Google), and Meta (Facebook) (Seth, 2018). The heightened tensions between the US and China in the global Internet have therefore made Alibaba increasingly susceptible to geopolitical conflicts. On the other hand, it has also become a basic infrastructural component for supporting the functioning of both the Chinese and the global economy. Such a ubiquitous market position has also brought new tensions into Alibaba's international endeavors.

Although this study was drawn from three examples of Alibaba's global expansion, the case study generates concepts that may be transferrable from one setting to another, and to situate our study's contribution, we summarize some key propositions to provide a roadmap for future research in the geopolitics of infrastructuralized platforms.

Empirically, this study builds on earlier conceptual frameworks (e.g., Plantin et al., 2018) of 'platforms as infrastructures' to map out the geopolitics of Chinese infrastructuralized platforms. First, the centrality of everyday data in contemporary infrastructuralized platforms can subject platforms in traditionally non-sensitive, non-strategic sectors to geopolitical tensions, as evidenced by Alibaba's failed deal with MoneyGram. Second, the seemingly 'invisible' and 'immaterial' infrastructuralized platforms are in fact territorially bounded, subject to state power and geopolitical pressures, as shown by the uneven global journey of Alibaba Cloud. Finally, modularity in infrastructuralized platforms enables the coordination between various independent and interdependent components of the system, yet tensions among players may emerge from the process of

negotiating modularity. Geopolitical concerns may arise from the core firm's market consolidation potential and defining power, as shown by the case of the eWTP.

More broadly, we also contribute to the discussion on the geopolitics of global cyberspace. Scholarship in media and communications has contributed important insights to this area in domains such as cybersecurity (e.g., Fichtner, 2018), standard-setting (e.g., DeNardis, 2009, 2011), Internet governance (e.g., Mueller, 2002, 2010) as well as from the perspective of critical political economy (Schiller, 2011; Winseck, 2017). The rise of infrastructrualized platforms in the global Internet, with their capacity to control unprecedented amounts of everyday data, negotiate visibility and invisibility, define the landscape for a large number of heterogeneous services across both online and offline channels, however, raises new questions.

First, as scholars have demonstrated, the control of transnational communication infrastructures has long been a priority for imperialist states, for both geopolitical control and capital accumulation (Schiller, 2011). Specifically, the control of 'strategic information' traveled via cables and wires bears important geopolitical implications (Headrick, 1991). The rise of infrastructuralized platforms and their capacity to control enormous amounts of everyday data, which can then be mined to reveal patterns of strategic value, however, have blurred the lines between 'strategic' and 'non-strategic'. This raises immediate implications for discussions around data localization and cybersecurity. For example, China's ride-hailing platform, Didi, had to withdraw from the New York Stock Exchange, precisely because of the large amount of everyday data – personal, traffic, and mapping information – it has collected as a transport utility supplier in urban China (Kubota & Lin, 2021).

Second, different from traditional infrastructures that often generate geopolitical tensions due to their high visibility, the geopolitics of infrastructuralized platforms arises from the tension between visibility and invisibility. That is, instead of being viewed as material, physical, and capital-intensive projects, digital platforms have often branded themselves as 'immaterial' and 'boundless'. However, growing efforts from scholars and activists as well as geopolitical concerns from nation-states have increasingly cast such 'invisibility' into question. Geopolitical pressures will likely move beyond merely focusing on physical telecom infrastructures to include those 'invisible' platforms. We have already seen such visibility-invisibility tension play out in the US 'Clean Network' initiative (US State Department, 2020).

Third, in contrast to traditional infrastructures that integrate other components via often negotiable standards, online and offline services have been plugged into infrastructuralized platforms based on the rules and landscape defined by the central platform via modularity. Such uneven power relations have become increasingly visible and controversial when platforms expand beyond their national markets. Concerns about market domination, standard formulation, and foreign control over basic infrastructure services will likely intensify in the years to come.

Finally, with the rise of private-owned, profit-oriented infrastructuralized platforms on the global Internet, we witness unprecedented corporate control over the basic infrastructure of the global political economy. Recently, scholars and policymakers have developed strong policy proposals to regulate digital infrastructures in the public interest (e.g., Schiller, 2020). However, how to understand and regulate the exterritorial behaviors of these corporate-controlled digital infrastructures remains an open question. For

example, what are the implications for the existing 'multi-stakeholder model' of global Internet governance, which identifies government, the private sector, and civil society as the primary actors in governing the global Internet, while leaving the uneven power relations undetermined (Mueller, 2010)? If corporate-owned digital platforms increasingly become the 'de facto governors' of global Internet infrastructures, what are the implications for reshaping the global communication order?

Toward this end, the Alibaba case studied here is not only about a particular Chinese platform infrastructuralized in its global expansion, but also about how such consolidated corporate power over the global Internet infrastructure, partially enabled by the specific features of digital platforms, has generated significant geopolitical frictions. Indeed, as evidenced by the recent disputes between Google and the European Union, there are growing geopolitical tensions and concerns around infrastructuralized platforms worldwide (European Commission, 2019). To what extent can the three dimensions – the geopolitics of everyday data, visibility-invisibility tension, and modularity – be useful to analyze infrastructuralized platforms from other countries? What are the limitations of this framework in understanding infrastructuralized platforms beyond the Chinese context? Those are important questions for future research.

Acknowledgements

Disclosure statement

No potential conflict of interest was reported by the author(s).

Notes on contributors

Hong Shen is an Assistant Research Professor in the Human-Computer Interaction Institute at Carnegie Mellon University. Her research focuses on the social and policy implications of digital platforms and algorithmic systems. She received her Ph.D. in Communications from the University of Illinois at Urbana-Champaign. Email: hongshenus@gmail.com

Yujia He is an assistant professor at the Patterson School of Diplomacy and International Commerce, University of Kentucky. Her areas of expertise are international and comparative political economy, science and technology policy, and governance issues in the Asia Pacific region. Email: yujia.he@uky.edu

ORCID

Yujia He ⓘ http://orcid.org/0000-0002-0931-2698

References

Alibaba Group. (2016). Fact sheet electronic World Trade Platform. https://www.alizila.com/wp-content/uploads/2016/09/eWTP.pdf?x95431
Alibaba Group. (2020a). SEC Form 20-F. https://otp.investis.com/clients/us/alibaba/SEC/sec-show.aspx?Type=html&FilingId=14266295&CIK=0001577552&Index=10000

Alibaba Group. (2020b). Malaysia airports and Alibaba announce operation commencement of Cainiao Aeropolis eWTP Hub, Malaysia. https://www.alibabagroup.com/en/news/article?news=p201103

Anastasiadou, I. (2019). Iron silk roads: The geopolitics of past and present initiatives for the revival of Eurasian trade through overland transport corridors. *Cambridge Journal of Regions, Economy and Society*, *12*(1), 57–75. https://doi.org/10.1093/cjres/rsy035

Bahgat, G. (2002). Pipeline diplomacy: The geopolitics of the Caspian Sea region. *International Studies Perspectives*, *3*(3), 310–327. https://doi.org/10.1111/1528-3577.00098

Baldwin, C. Y., & Clark, K. B. (2000). *Design rules: The power of modularity* (vol. 1). MIT Press.

Baldwin, C. Y., & Woodard, C. J. (2009). The architecture of platforms: A unified view. *Platforms, Markets and Innovation*, 19–44. Research collection school of information systems. https://ink.library.smu.edu.sg/sis_research/2452

Barfield, C. (2018). CFIUS and China: The MoneyGram case and beyond. AEI. https://www.aei.org/economics/international-economics/cfius-and-china-the-moneygram-case-and-beyond

Bogost, I., & Montfort, N. (2009). Platform studies: Frequently questioned answers. *Digital Arts and Culture*, *12–15*(December), 1–6.

Bowker, C. G., & Star, S. L. (2000). *Sorting things out: Classification and its consequences*. MIT Press.

Bueger, C., & Liebetrau, T. (2021). Protecting hidden infrastructure: The security politics of the global submarine data cable network. *Contemporary Security Policy*, 1–23. https://doi.org/10.1080/13523260.2021.1907129

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

Chandran, N. (2018). Alibaba's 'Digital Free Trade Zone' has some worried about China links to Malaysia. CNBC. https://www.cnbc.com/2018/02/12/concerns-over-alibaba-led-digital-free-trade-zone-in-malaysia.html

Chen, J. Y., & Qiu, J. L. (2019). Digital utility: Datafication, regulation, labor, and DiDi's platformization of urban transport in China. *Chinese Journal of Communication*, *12*(3), 274–289. https://doi.org/10.1080/17544750.2019.1614964

Chitkara, H. (2020). Alibaba Cloud's future is still bright, despite US efforts to thwart its growth. *Business Insider*, https://www.businessinsider.com/alibaba-cloud-sees-momentum-despite-potential-us-sanctions-2020-8

DeNardis, L. (2009). *Protocol politics: The globalization of Internet governance*. MIT Press.

DeNardis, L. (ed.) (2011). *Opening standards: The global politics of interoperability*. MIT Press.

The Edge Markets. (2020). Lazada becomes go-to e-commerce platform for merchants and consumers during uncertain times. https://www.theedgemarkets.com/content/advertise/lazada-becomes-go-to-e-commerce-platform-for-merchants-and-consumers-during-uncertain-times

Edwards, P. N., Bowker, G. C., Jackson, S. J., & Williams, R. (2009). Introduction: An agenda for infrastructure studies. *Journal of the Association for Information Systems*, *10*(5), 364–374. https://doi.org/10.17705/1jais.00200

European Commission. (2019). Antitrust: Commission fines Google €1.49 billion for abusive practices in online advertising. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_1770

Fichtner, L. (2018). What kind of cyber security? Theorising cyber security and mapping approaches. *Internet Policy Review*, *7*(2), 1–19. https://doi.org/10.14763/2018.2.788

Gillespie, T. (2010). The politics of 'platforms'. *New Media & Society*, *12*(3), 347–364. https://doi.org/10.1177/1461444809342738

Graham, S., & Marvin, S. (2001). *Splintering urbanism: Networked infrastructures, technological mobilities and the urban condition*. Routledge.

Gray, J. (2021). The geopolitics of 'platforms': The TikTok challenge. *Internet Policy Review*, https://policyreview.info/articles/analysis/geopolitics-platforms-tiktok-challenge

Guo, C. F. (2021). "Zuowei yijia yunjisuan changshang, Aliyun shifou you bianjie," 作为一家云计算厂商⍰阿里云是否有边界 [Whether Alibaba Cloud has boundaries], https://cloud.ofweek.com/news/2021-10/ART-178800-8500-30531196.html

He, Y. (2019). Connecting the emerging markets: China's growing role in global digital infrastructure. HKUST Institute for emerging market studies thought leadership Brief No. 26. https://iems.ust.hk/assets/publications/thought-leadership-briefs/tlb20/tlb26/hkust-iems-tlb26-he.pdf

He, Y., & Tritto, A. (2022). Urban Utopia or pipe dream? Examining Chinese-invested smart city development in Southeast Asia. *Third World Quarterly*, *43*(9), 2244–2268. https://doi.org/10.1080/01436597.2022.2089648

Headrick, D. R. (1991). *The invisible weapon: Telecommunications and international politics, 1851-1945*. Oxford University Press.

Hern, A. (2018). Fitness tracking app Strava gives away location of secret US army bases. *The Guardian*, *28*, 7. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases

Herr, T. (2020). Four myths about the cloud: The geopolitics of cloud computing. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2020/09/CLOUD-MYTHS-REPORT.pdf

Hillman, J. E. (2021). U.S. at risk of losing cloud computing edge to China. Politico. https://www.politico.com/newsletters/politico-china-watcher/2021/08/26/us-at-risk-of-losing-cloud-computing-edge-to-china-494105

Hu, T. (2015). *A prehistory of the cloud*. MIT Press.

Hughes, T. P. (1983). *Networks of power: Electrification in western society, 1880-1930*. Johns Hopkins University Press.

Jacobides, M. G., Cennamo, C., & Gawer, A. (2018). Towards a theory of ecosystems. *Strategic Management Journal*, *39*(8), 2255–2276. https://doi.org/10.1002/smj.2904

Jia, F., & Bennett, M. M. (2018). Chinese infrastructure diplomacy in Russia: The geopolitics of project type, location, and scale. *Eurasian Geography and Economics*, *59*(3-4), 340–377. https://doi.org/10.1080/15387216.2019.1571371

Jia, L., & Liang, F. (2021). The globalization of TikTok: Strategies, governance and geopolitics. *Journal of Digital Media & Policy*, *12*(2), 273–292. https://doi.org/10.1386/jdmp_00062_1

Keohane, R. O., & Nye Jr., J. S. (1998). Power and interdependence in the information age. *Foreign Affairs*, *77*(5), 81. https://www.foreignaffairs.com/articles/1998-09-01/power-and-interdependence-information-age https://doi.org/10.2307/20049052

Kubota, Y., & Lin, L. (2021). In the New China, Didi's data becomes a problem. *The Wall Street Journal*, https://www.wsj.com/articles/in-the-new-china-didis-data-becomes-a-problem-11626606002

Kumar, P. P., & Kuar, D. (2018). DFTZ not dependent only on Alibaba. *The Malaysian Reserve.* https://themalaysianreserve.com/2018/07/27/dftz-not-dependent-only-on-alibaba/?__cf_chl_jschl_tk__=pmd_.J7eaubLydXQpgu6PWfcJ4GK4rlw029LTZRhXvdE0KA-1633714776-0-gqNtZGzNAmWjcnBszQjR

Langlois, G., & Elmer, G. (2013). The research politics of social media platforms. *Culture Machine*, *14*, 1–17.

Logan, S. (2015). The geopolitics of tech: Baidu's Vietnam. *Internet Policy Observatory*, https://repository.upenn.edu/internetpolicyobservatory/10/

Lu, J. (2017). "Jishu shi yongyuan de diqi," 技术是永远的底气 [Technology is always the bottom link], 光明日报 *[Guangming Daily]*, https://epaper.gmw.cn/gmrb/html/2017-06/07/nw.D110000gmrb_20170607_3-05.htm

Malaysia Digital Economy Corporation (MDEC). (2016). National ecommerce strategic roadmap. https://mdec.my/about-malaysia/government-policies/national-ecommerce-strategic-roadmap/

Malaysia Digital Economy Corporation (MDEC). (n.d.). Digital free trade zone. https://mdec.my/digital-economy-initiatives/for-the-industry/entrepreneurs/dftz/

Malaysian Ministry of Transport. (2017). Media statement on digital free trade zone. https://www.mot.gov.my/my/Kenyataan%20Media/Tahun%202017/Media%20Statement%20By%20Ministry%20of%20Transport%20on%20Digital%20Free%20Trade%20Zone.pdf

Mashayekhi, R. (2020). Could a Western Union–MoneyGram deal help two giants fend off fintech disrupters? *Fortune*, https://fortune.com/2020/06/11/western-union-moneygram-acquisition-remittance-money-transfers/

McDonald, J. (2014). Alibaba, symbol of China's New Tech Giants. AP, https://apnews.com/article/cfe63417b45f46a3aec3fe841c06f564

Ministry of International Trade and Industry of Malaysia (MITI). (2018). Digital free trade zone factsheet. https://www.miti.gov.my/miti/resources/Media%20Release/Fact_Sheet_DFTZ_at_Malaysia_Digital_Economy_2018_SME_Fact_Sheet.pdf

Mosco, V. (2014). *To the cloud: Big data in a turbulent world*. Routledge.

Mueller, M. (2002). *Ruling the root: Internet governance and the taming of cyberspace*. MIT Press.

Mueller, M. (2010). *Networks and states: The global politics of Internet governance*. MIT Press.

Napoli, P. M. (2019). User data as public resource: Implications for social media regulation. *Policy & Internet*, *11*(4), 439–459. https://doi.org/10.1002/poi3.216

Naughton, B. (2020). Chinese industrial policy and the digital silk road: The case of Alibaba in Malaysia. *Asia Policy*, *27*(1), 23–39. https://doi.org/10.1353/asp.2020.0006

Pethokoukis, J. (2018). Trump's foolish economic cold war with China. AEI. https://www.aei.org/articles/trumps-foolish-economic-cold-war-with-china

Plantin, J. C., & De Seta, G. (2019). WeChat as infrastructure: The techno-nationalist shaping of Chinese digital platforms. *Chinese Journal of Communication*, *12*(3), 257–273. https://doi.org/10.1080/17544750.2019.1572633

Plantin, J. C., Lagoze, C., Edwards, P. N., & Sandvig, C. (2018). Infrastructure studies meet platform studies in the age of google and Facebook. *New Media & Society*, *20*(1), 293–310. https://doi.org/10.1177/1461444816661553

Ragin, C. C., & Becker, H. S. (eds.). (1992). *What is a case?: Exploring the foundations of social inquiry*. Cambridge University Press.

Rosenbach, E., & Mansted, K. (2019). *The geopolitics of information*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/publication/geopolitics-information

Roumeliotis, G. (2018). U.S. blocks MoneyGram sale to China's Ant Financial on national security concerns. *Reuters*. https://www.reuters.com/article/us-moneygram-intl-m-a-ant-financial-idUSKBN1ER1R7

Schiller, D. (2011). Geopolitical-economic conflict and network infrastructures. *Chinese Journal of Communication*, *4*(1), 90–107. https://doi.org/10.1080/17544750.2011.544085

Schiller, D. (2020). Reconstructing public utility networks: A program for action. *International Journal of Communication*, *14*, 12.

Seth, S. (2018). World's top 10 Internet companies. *Investopedia*, https://www.investopedia.com/articles/personal-finance/030415/worlds-top-10-internet-companies.asp

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. (2017). *Across the great (Fire) wall: China and the global Internet* [Unpublished doctoral dissertation]. University of Illinois at Urbana-Champaign.

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

Shen, H., Faklaris, C., Jin, H., Dabbish, L., & Hong, J. I. (2020). 'I an't even buy apples if I don't use mobile pay?' When mobile payments become infrastructural in China. *Proceedings of the ACM on Human-Computer Interaction*, *4*(CSCW2), 1–26.

Shen, H. (2021). *Alibaba: Infrastructuring global China*. Routledge.

Star, S. L. (1999). The ethnography of infrastructure. *American Behavioral Scientist*, *43*(3), 377–391. https://doi.org/10.1177/00027649921955326

Starosielski, N. (2015). *The undersea network*. Duke University Press.

Tang, M. (2020). Huawei versus the United States? The geopolitics of exterritorial Internet infrastructure. *International Journal of Communication*, *14*, 4556–4577.

Touch'N'Go. (2017). Touch 'n Go - Alipay JV has every reason to succeed. https://www.touchngo.com.my/CorporateNewsDetails/Corporate/About-Us/Senior-Management-Team/Touch-n-Go-Alipay-JV-Has-Every-Reason-To-Succeed/

Tworek, H. (2019). *News from Germany: The competition to control world communications, 1900-1945*. Harvard University Press.

Tzin, S. T. (2021). My Say: Development plans must make 'Made in Malaysia' great again. *The Edge Malaysia*, https://www.theedgemarkets.com/article/my-say-development-plans-must-make-made-malaysia-great-again

US State Department. (2020). The Clean Network, https://2017-2021.state.gov/the-clean-network/index.html

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

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

Yang, L., Lin, L., & Zhai, K. (2021). Alibaba's winning cloud formula is coming under pressure. *Wall Street Journal*, https://www.wsj.com/articles/alibabas-winning-cloud-formula-is-coming-under-pressure-11621767602

Yean, T. S. (2018). *The Digital Free Trade Zone (DFTZ): Putting Malaysia's SMEs onto the digital silk road*. ISEAS Perspectives. https://www.think-asia.org/bitstream/handle/11540/8137/ISEAS_Perspective_2018_1750.pdf?sequence=1

Yean, T. S. (2020). Alibaba's expansion into Malaysia: A double-edged sword?. ISEAS. https://www.iseas.edu.sg/media/commentaries/alibabas-expansion-into-malaysia-a-double-edged-sword/

Zhang, Z. (2021). Infrastructuralization of Tik Tok: Transformation, power relationships, and platformization of video entertainment in China. *Media, Culture & Society*, *43*(2), 219–236. https://doi.org/10.1177/0163443720939452

Zimmerman, E. J. (2019). The foreign risk review modernization act: How CFIUS became a tech office. *Berkeley Technology Law Journal*, *34*, 1267–1304. https://btlj.org/data/articles2019/34_4/12_Zimmerman_WEB.pdf