The Digital Silk Road: Perspectives
From Affected Countries

Editor:
Rogier Creemers

Contributors:
Molly Bodurtha, Mohammadbagher Forough,
Richard Ghiasy, Sanne van der Lugt

July, 2021
The LeidenAsiaCentre is an independent research centre affiliated with Leiden University and made possible by a grant from the Vaes Elias Fund. The centre focuses on academic research with direct application to society. All research projects are conducted in close cooperation with a wide variety of partners from Dutch society. The project on China and Global Cyberspace (2019-2021) was executed together with and co-financed by the Dutch Ministry of Foreign Affairs.

More information can be found on our website:  
www.leidenasiacentre.nl

For contact or orders: info@leidenasiacentre.nl

M. de Vriehof 3, 2311 BZ Leiden, The Netherlands
## Contents

1. **Introduction**  
   Dr Rogier Creemers  
   3

2. **Cambodian Perceptions of the Digital Silk Road**  
   Molly Bodurtha  
   6

3. **Iran and China Along the Digital Silk Road**  
   Dr Mohammadbagher Forough  
   24

4. **Digital Silk Road – Impact and Perceptions in India**  
   Richard Ghiasy  
   33

5. **What Role Does the Digital Silk Road Have in the Domestic Debate on Digitalization in Ethiopia?**  
   Dr Sanne van der Lugt  
   42
China’s flagship foreign policy engagement programme, the Belt-Road Initiative (BRI) and its technological component, the Digital Silk Road (DSR), have garnered much attention in policy and research circles. As the prime manifestation of China’s ambition to play a greater role in the global digital sphere, the DSR has led to questions concerning whether Beijing might use it as a conduit to export its political system or approach to digital governance, as well as concomitant values, to gain a greater role in global digital standard setting processes, and what its competitive impact is for Western governments and technology companies.

The answer to these questions is, however, often not borne by detailed empirical analysis. To a certain degree, this is unsurprising. For all the attention the DSR has received, it is still more a slogan than an actual institutionalized policy initiative. There are no public plans or documents outlining what the DSR’s objectives are, or how they are to be implemented. The DSR does not have an acknowledged institutional home within the Chinese government, nor is there clearly a coordinating body in charge. As a result, it isn’t always clear what the DSR entails. Obviously, China has numerous agreements with countries in the BRI area for telecommunications infrastructure, and Chinese businesses are increasingly looking abroad for new markets and growth prospects. However, it is not evident that this is the result of a comprehensive policy drive or whether they are simply the result of legacy processes and logical business moves. But perhaps most importantly, the vast majority of existing analysis of the DSR is primarily Beijing-centric, focusing on the objectives and intentions of the Chinese leadership, and paying comparatively scant attention to the local environment of countries affected by the DSR.

Nevertheless, the perspective of DSR-affected and recipient countries is crucial, for several reasons. First, the DSR potentially covers dozens of nations, with significant variation in economic development levels, foreign policy, regime type, ethnicity and religion, geography and many other parameters. As such, the DSR cannot be a one-size-fits-all initiative but will inevitably be shaped by the different environments it will face. Second, while the DSR is often framed through the lens of Sino-US great power competition, the dozens of countries affected by it have significant agency. They may have their own strategic visions and approaches that seek to leverage China’s stated munificence to their own benefit. In other words, in discussing the DSR’s influence and implementation, we must address pull factors and local conditions as much as, if not more than, push factors and Chinese strategic calculations. At the most basic level, it is in recipient countries that the DSR rubber hits the road. To
more accurately evaluate its acceptance and influence, its implementation and potential mishaps, we must look to those places where the initiative will be realized.

This report provides an initial step in this direction, by providing four country-level studies of perceptions of the DSR. Three of the selected countries are smaller, developing countries where China has growing economic and foreign policy interests: Ethiopia, Iran and Cambodia. The fourth country is India, the region’s other major emerging power, also a developing country, whose relationship with China has grown increasingly tense at the strategic level, including bans on Chinese mobile apps, yet whose digital economy is closely intertwined with China. Specifically, the contributors have mapped the extent to which China has a digital presence within the country; surveyed the state of debate on the DSR within the country, in political and media circles, as well as the major debates concerning digital engagement with China; and reviewed the extent to which digital engagement plays a role in their broader relationship with China, and in broader foreign policymaking and strategic considerations.

While the four countries obviously differ considerably on numerous counts, it is nevertheless possible to derive the following general findings with regard to their perspectives on the DSR. First, in none of the four countries has the notion of the “Digital Silk Road” entered the domestic political discourse. It is exclusively used with reference to Beijing’s intentions and policies, and usually not even with reference to the country’s own responses. Second, the DSR is not considered to be a comprehensive, multilateral programme. In none of the countries is there a sense that becoming involved with the DSR entails anything outside the bilateral relationship with Beijing. In other words, where two countries engage with the DSR, they do not see this as having an influence on the relationship between them, only with Beijing. Neither do they consider it to be an international normative project with rule-setting objectives. As such, the DSR is best understood as a “hub-and-spoke” model with Beijing at the centre, where the geometry of each individual spoke is shaped through the specific circumstances of that relationship.

Even so, the question how to engage with China on digital issues is an important one in domestic policymaking. Unsurprisingly, all governments surveyed intend to develop strategies in pursuit of their own perceived national interest. Ethiopia, for instance, values access to Chinese technologies for its own development agenda, but does not want to connect to Beijing too closely. Instead, it sees a degree of competition between technological powers as being in its interest. Iran, in contrast, has sought to strengthen its partnership with China in response to greater tensions with the US, which emerged under the Trump administration. There is also considerable cooperation between Tehran and China on technological, security and intelligence affairs. In Cambodia, Chinese technology investment has become part of domestic politics, which entails a pursuit of economic development that sees China as an attractive, but
not exclusive provider of aid and investment. It also involves efforts by the ruling Party to strengthen its hold on power. India, for its part, is experiencing increasing geopolitical tensions with China and is seeking support from the United States. However, Chinese consumer devices and services have grown popular within India in recent year, particularly among the less wealthy. This limits India’s options, particularly as the emergence of its own technology sector has not met the expectations purported a few years ago.

These conclusions have important implications for observers and policymakers. First and foremost, they should move away from the Beijing-centric model that has dominated the debates so far, and take the agency and interests of affected countries into greater consideration. This local knowledge will provide a more accurate picture of potential risks and opportunities, tasks and circumstances than the extant literature does. Second, they should take note that the DSR is not simply a competition between the US and China fought out in neutral territories. Indeed, the DSR as a concept itself may well be far less useful than often thought. Instead, they need to develop a more nuanced picture that moves away from the DSR as a monolithic policy initiative, and includes the multiplicity of Chinese and local actors, interests and processes that are involved in China’s growing digital technology footprint. Third, even though the DSR may well be less of a national strategy than advertised, it nevertheless is the case that China’s digital footprint does pose competitive challenges to Western governments, for local governments’ favour, and for Western businesses, for their markets. Observers and policymakers would do well to meet this challenge head-on, and use it as a stimulus to increase the quality and competitiveness of their offering and approach. The attractiveness of Chinese digital technology, infrastructure and investment in recipient countries should not be underestimated or belittled.

1 In 2017, the Chinese government did attempt to convince countries to sign a framework agreement for BRI-related cooperation on digital economic issues. However, only six did: Laos, Saudi Arabia, Serbia, Thailand, Turkey and the United Arab Emirates. Little reference has been made to this document subsequently. https://chinacopyrightandmedia.wordpress.com/2017/12/03/proposal-for-international-cooperation-on-the-one-belt-one-road-digital-economy/
I. Introduction

Cambodia is a developing economy notionally poised to leapfrog in industrial development and technological adaption, yet nonetheless mired in the recovery from its tumultuous 20th century history. As such, Cambodia has actively implemented policies of openness—favouring most, if not all, opportunities for economic and technological connectivity with international partners. China’s Digital Silk Road (DSR) represents one such opportunity, and challenge, to Cambodia.

Chinese overseas direct investment (CODI) in Cambodia has accelerated in recent years: in 2014, China rose to become Cambodia’s largest foreign investor and development partner. In 2019, the Council for the Development of Cambodia (CDC) approved a subset of CODI projects valued at USD 3.7 billion for investment incentives.¹ That year, registered and incentive-eligible CODI constituted thirteen percent of Cambodia’s Gross Domestic Product (GDP) and 78 percent of inbound FDI.² By early 2020, CODI accounted for over 56 percent of all cumulative FDI in Cambodia since 1993.³ The most visible concentrations of CODI in Cambodia are the garment sector, public infrastructure construction, luxury real-estate construction and tourism-related investment, including casino gambling operations, which, in 2019, drew hundreds of thousands Chinese nationals.⁴

Numerous studies have investigated the benefits and costs associated with this influx, as well as concomitant Cambodian public opinion toward CODI. Despite the rising significance of internet access to political and economic inclusion, especially following the covid-19 pandemic, fewer studies have focused on the significance and reception of the DSR specifically.

What has the DSR meant and what could it mean for Cambodia? Compared to the large-scale economic and infrastructural changes introduced by BRI projects, has the more targeted DSR similarly disrupted telecommunications, data governance, internet access, education, and online citizenship? How do Cambodian thought-leaders, those who will play a role in determining the extent to which Cambodia continues to absorb CODI, conceive of the costs and benefits of the DSR?

Based on interviews with industry leaders, prominent academics, senior officials, government advisors, and civil society actors in Cambodia, as well as a review of Cambodian scholarship and media reports, this section finds that the DSR has a limited footprint and conceptual traction in Cambodia. However, Chinese actors play a crucial,
market-leading role in providing Cambodian consumers and institutions with hard digital and telecommunications infrastructure, which lays the foundation for digital development and broader connectivity. Beyond hard infrastructure, Chinese firms have played a less prominent role in capacity-building efforts—from developing STEM education in Cambodia to public-private partnerships aimed to digitize, formalize, and streamline government services. These areas represent an area for potential growth and a more diverse array of actors, including foreign development agencies, multinationals, and indigenous start-ups, among which China is just one.

Cambodian perceptions of China’s involvement and influence are complex: all segments of society enthusiastically welcome investment in high-quality infrastructure investment, including internet and telecommunications infrastructure, regardless of its origin. It is broadly recognized that CODI drove economic growth of 7.7 percent over the last decade and generated undeniable value for rural and urban Cambodian households, which are more able to access the internet and, therefore, basic services and socioeconomic opportunity.

Nevertheless, this enthusiasm is coupled with an undercurrent of opposition to infrastructure investment that supports officials within the incumbent Cambodian People’s Party (CPP) regime, as opposed to the Royal Government of Cambodia (RGC) and the country’s development generally. Interviewees across academia, journalism, civil society, the business community, and even government expressed this anxiety. Specifically, they expressed concern that Chinese institutions are responsible for selling equipment and undisclosed services to the CPP, facilitating the CPP’s growing ability to control the country’s internet, undermine democracy and rule of law, and perpetuate the party’s oligarchic power. Cambodian resistance to the DSR focuses on the initiative’s potential to expand the Cambodian regime’s capacities, exacerbating pre-existing governance issues and authoritarian tendencies. The concerns do not relate to the exposure of Cambodian citizens to direct privacy and security risks involving Chinese corporations or the Chinese government.

The sections that follow describe the extent and nature of the DSR in Cambodia as the initiative stands today, summarizing dimensions of Cambodian perceptions of the DSR. For the purpose of this report, “DSR” is employed as a shorthand to refer to CODI in internet and telecommunications goods and services, despite the relatively low frequency with which the formal DSR designation is attached to ongoing projects in the Cambodian context.
II. Footprint of the Digital Silk Road in Cambodia

Formal Agreements

No bilateral Sino-Cambodian agreements refer to the DSR explicitly, although some bilateral BRI agreements and MoUs mention digital, telecommunications, and internet development.

At the Belt and Road Forum in Beijing, on May 16, 2017, Cambodian Prime Minister Hun Sen and Chinese President Xi Jinping signed the Outline of Bilateral Cooperation Plan to Jointly Build the Silk Road Economic Belt and the 21st Century Maritime Silk Road. In relevant part, the Outline states intentions (1) to “encourage Chinese enterprises to participate in export[ing] telecommunications equipment”; (2) to “encourage Chinese enterprises to invest in Cambodian digital Television broadcasting network construction” and “to accelerate popularization of digital television in Cambodia”; (3) to “promote the Belt and Road spatial information corridor” and “[e]ncourage Chinese enterprises to take part in enhanc[ing the] network of Cambodian Beidou navigation and spatial information service”; and, finally, (4) to “boost bilateral cooperation in the area of innovation and application of information communication technology, information security, and data protection.” As of this writing, only the first two areas of cooperation appear to be economically feasible and underway.

Beyond the Outline, China and Cambodia signed 55 bilateral agreements between 2016 and 2018. Only two of those agreements related to executing discrete DSR-related projects: a 2018 MoU on establishing a research institution, the Cambodia-China Technology Transfer Center; and a 2018 “Cooperative Agreement on the Field of Technical Vocational Education and Training.” Whether and how they are implemented remains unclear. The vast majority of bilateral MoUs outlined terms for classic infrastructure projects, e.g., roads, dams, other energy infrastructure, and even a hospital.

In 2019, the DSR came closer to the forefront of the governments’ priority areas for bilateral cooperation. At that year’s Belt and Road Forum, Prime Minister Hun Sen and Huawei Vice President Li Jin’ge signed an agreement granting Huawei rights to provide 5G infrastructure across Cambodia. In January 2020, an implementing agreement sign by Cambodia’s Ministry of Posts and Telecommunications (MPTC) and Huawei’s CEO stated Huawei’s intention to sell ICT equipment to Cambodian carriers and to “provid[e]” the MPTC with “a data centre facility, video conference system,” fibre-optic connectivity for their office, and “Huawei laptops for central and provincial government offices,” although the terms and conditions—and, therefore, the market implications for competitors in the 5G space—have not been made public. Interviewees representing parties to the deal commented that Huawei’s business in Cambodia predates the BRI and was unaffected by the agreement. Other interviews articulated that formal BRI agreements in Cambodia are largely epiphenomenal, serving mostly
as signifiers of bilateral political support for continued commercial activity of a specific nature and, hence, offering would-be investors greater assurances. Since then, publicized official bilateral agreements have centered on covid-19 recovery efforts and, more recently, a trade deal (finalized as the European Union withdrew the application of its EBA preferential trading scheme from Cambodia in response to the regime’s violations of human rights.)

The actual state of ICT development and commercial activity of Chinese firms in Cambodia does not neatly match the patchwork of Sino-Cambodian BRI agreements, whose primary function is perceived to be signalling investment opportunity. Many sectors of DSR cooperation enumerated in the agreements remain aspirational, such as Sino-Cambodian cooperation in space, and even 5G service, which is not operational and, according to interviewees, will not be fully operational for several years. In other arenas—such as device proliferation, the expansion of earlier generation networks, digital government initiatives, and application development and proliferation—the industry outpaces and dictates government planning. CODI leads in several, but not all, of these areas.

Getting Online: Networks and Devices
Foundational to Cambodia’s digital development is the proliferation of networks, devices, and IT knowledge, which enable basic connectivity. However, the deficiencies of telecommunications and educational infrastructure have stymied the country’s potential. Below two percent of the population has access to fixed line internet, but 70 percent own smartphones. Although state-linked media and telecommunications companies frequently announce imminent 5G network development, 5G is still a number of years from deployment, and many, particularly rural, areas in the country still lack 3G and 4G service. The country’s leadership and industry heads are eager to leapfrog in the space of network connectivity, and hope that when rural areas are brought online, it will be done using 5G.

Huawei is Cambodia’s top supplier of network equipment, including cell towers, data centres, and base stations, by a significant and widening margin. ZTE is the second largest supplier. Although Vietnamese state-owned enterprise Viettel was an early investor, entering the market and building 2G networks across rural Cambodia in the mid-2000s, the sales of Viettel, Nokia (Finland), and Ericsson (Sweden) have declined subsequently. Interviewed telecommunications professionals explained that non-Chinese firms cannot compete with the price and quality of Huawei and ZTE’s technology. Additionally, firms are looking to replace their existing networks and buy ZTE and Huawei’s cheaper and superior quality equipment, especially for the rollout of 5G.
Despite the openness of the market and possibility for competing firms to build out these networks, several interviewees representing various stakeholders explained Huawei’s market dominance in 3G, 4G, and 5G is owed to undisclosed subsidies from Chinese state institutions, such as the Silk Road Investment Fund and the Bank of China. This would compensate for the prima facie lack of profitability in the Cambodian market, as local consumers’ willingness and ability to pay is low. One interviewee also suggested Huawei could have been re-allocating profits from their once-thriving European business to fund business in developing economies, where current purchasing power cannot sustain development.

Nevertheless, all interviewees emphasized telecommunications infrastructure investment empowers communities. For instance, Cellcard, one of the major telecommunications service providers and the only wholly Cambodian-owned one, reports that its 2017 expansion of 4G LTE sites from 300 to 3,000 resulted in 36% more connections and a 500% increase in mobile data traffic, as well as “an injection of $610 million to the local economy.”

Chinese firms are also active in existing and planned cable construction, connecting Cambodia internally and to servers abroad through fiber-optic and submarine cables. This investment is seen as urgent: the limited number of entry points carrying the vast majority of internet traffic has created a speed bottleneck that will hamper reliable internet access even when 5G networks become operational, unless further submarine cables are constructed. The Telecommunications Regulator of Cambodia (TRC) has only issued three fiber-optic licenses: to Viettel, Cambodian state-owned Telecom Cambodia, and a subsidiary of the Chinese firm Hyalroute. As of May 2021, Cambodia’s ability to access foreign-hosted sites relies on two submarine cables in Sihanoukville port. Both became operational in 2017: the USD 100 million Malaysia-Cambodia-Thailand (MCT) cable, built by Huawei Marine and the Asia Africa Europe-I (AAE-1) cable, built by a Hong Kong-based multinational consortium and connecting to Cambodia’s fiber optic network through Hyalroute’s landing station. In 2019, the Asian Infrastructure Investment Bank approved 75 million USD for Hyalroute to expand fiber optic connectivity in Cambodia. In June 2019, Huawei and China Communications Construction Co. (CCCC) announced plans to build a submarine cable between Hong Kong and Sihanoukville. This move followed statements of interest in similar projects by the Beijing-based China Road and Bridge Corporation earlier that year.

Recent growth in mobile networks and smartphone penetration demonstrates Cambodia’s leapfrogging potential: its ability to bypass legacy technology such as fixed-line networks and (eventually) directly invest in and adapt newer-stage technology such as 5G. Fixed-line internet, priced at approximately USD 70 per month, remains inaccessible to most Cambodian households. In a country of approximately 17 million
people, there are approximately 200,000 fixed-line internet subscriptions.\textsuperscript{23} Meanwhile, by 2019, the number of smartphone subscriptions rose to 21.42 million, surpassing the population.\textsuperscript{24} This growth is impressive, but uneven: Only 70 percent of the adult population have smartphones, as many have multiple subscriptions across different networks.\textsuperscript{25}

Interviewees expressed this expansion would not have been possible without competitive pricing by Chinese manufacturers, particularly Oppo and Vivo, whose bright green and blue stalls dot the Cambodian countryside. Oppo smartphones are sold for USD 60 to 200. The average price for other brands, such as Samsung, stood at USD 296 in 2017 and USD 347 in 2017.\textsuperscript{26} Collectively, Chinese firms take at least 54 percent of the market.\textsuperscript{27} Oppo sells the most mobile devices in Cambodia, holding 26 percent of the market as of 2020, followed by Apple (20 percent), Samsung (19 percent), Vivo (13 percent) and Huawei (9 percent). Chinese firms Xiaomi and Realme also have minor stakes in the market, holding four and two percent respectively.\textsuperscript{28}

One missing element of foundational infrastructure is human resources availability and development.\textsuperscript{29} Cambodia is still building back its educational institutions and professional classes following the Khmer Rouge period, during which educated individuals faced targeted persecution. Universities remain under-resourced, with few specialized programs in computer science and information technology.\textsuperscript{30} As a result, many firms in Cambodia hire foreign employees or Cambodians who have self-taught using online resources, studied abroad, or received prior on-the-job training at another firm.\textsuperscript{31} Cambodian students are increasingly studying abroad in China, and Chinese universities have established several joint degree programs in Cambodia, although educational partnerships remain diverse.\textsuperscript{32}

To summarize, although educational infrastructure remains deficient in addressing the population and industry’s appetite, Cambodia’s leading market players in other foundational infrastructure are Chinese vendors offering lower prices that have allowed for extensive mobile phone adoption in both rural and urban area, creating immense socioeconomic opportunity.

**Delivering Services Online**

A secondary element of Cambodia’s digital development involves migrating a cash-based, informal economy online and improving the value of internet-based goods and services. Indigenous innovation and policy play increasingly large roles in the development of applications for the public and private sector is underway, while CODI is less prominent.
Facebook, Cambodia’s most downloaded and utilized application, is the fabric of Cambodian social media and e-commerce. As of September 2020, 11.28 million Cambodian individuals, or 66 percent of the population, had Facebook accounts. In 2016, Facebook surpassed television as Cambodians’ primary source of news. Facebook has taken on greater commercial significance in Cambodia than in the other parts of the world, as businesses and even government institutions forego establishing up-to-date interfaces on standalone websites, to engage with the public through Facebook pages and Messenger. Despite Facebook’s ubiquity, Tiktok became Cambodia’s fastest growing app, reaching eight million in-country users in the span of a two years. Beyond social media, lockdowns during the ongoing covid-19 pandemic and shuttering of wet markets drove a growth in e-commerce and use of app-based services. A number of Southeast Asian start-ups in ride hailing, food delivery, bus and train booking and other services became more popular in cities and have inspired competition from indigenous start-ups in the same space.

The RGC’s operations lag behind the market’s digitization, a state of affairs which facilitates graft, thwarts social service provision and accountability efforts, and hinders economic growth, along with Cambodian individuals’ and enterprises’ abilities to transact in the formal domestic and transnational economies. Cambodia’s 28 ministries and central agencies still rely upon over 50 different IT systems. Several agencies continue to forego keeping centralized digital records and hosting online services. Others retain redundant digital registration processes, requiring in-person repetition. Digitization and integration within, let alone across, ministries will take years.

Recognizing the transformative value of tech-enabled governance, the Prime Minister has articulated ambitious plans to transform Cambodia into an information-driven economy and to digitize government, consciously emulating elements of other governments’ technological adaption. Interviewees cited Cambodia’s aspiration to implement adapted versions of Estonia’s X-Road program, which has migrated approximately 90 percent of all government services online; Rwanda’s Digital ID system, which uses biometrics to locate citizen records; and China’s use of internet controls and facial recognition street cameras in policing.

Within the past year, the RGC introduced two indigenously developed initiatives that signal a step in this direction. Launched in June 2020, the Cambodian Data Exchange (CamDX), an online platform, aims to galvanize business registration and erase inefficiency and graft in quotidian interactions between business and government. Another public-private-partnership, the National Bank of Cambodia’s Bakong uses blockchain technology to facilitate currency exchanges across financial institutions, including e-wallets. Bakong significantly promotes financial inclusion, as only 17 percent of Cambodians had bank accounts as of 2017, relying instead on e-wallets, like
In a country with a dollarized economy and one of the highest domestic remittances rates in the world (40 percent), Bakong could inject more capital into rural communities, and reinvigorate the use of the Cambodian riel. Despite these heralds of improvement in governance quality and accountability, both applications are limited in scope and face uphill battles empowering and incentivizing both government entities and citizens to adapt to the formal economy.

International partnerships, which could assist Cambodia’s leapfrogging efforts, currently play a smaller role in digital capacity-building initiatives. Japan, Korea, and the United States’ aid agencies have engaged in some studies for technological capacity building efforts, but not systemic digitizing overhauls of the RGC’s operations. Interviewees noted the majority of disclosed public-private partnership tend to involve Cambodian firms, as foreign firms can be reluctant to provide tools to the CPP regime. Although multinational firms could operate intelligent applications for public services with profound social value, from covid-19 tracing to land registration apps, multinational firms do not typically reach out to the government. On the other hand, unless urged by the Prime Minister, the RGC remains “intransigent” and disincentivized from innovating. As a result, the RGC’s lack of sophisticated digital systems and reliance on applications developed in foreign jurisdictions present compelling security risks, in addition to impeding accountability and quality service provision.

In summary, Chinese firms are less dominant in the application space and in facilitating private and public online services, than Chinese firms are in hardware and equipment provision. The most widely used personal and commercial applications represent diverse sources and are hosted in various jurisdictions. Notably, in this sector, Cambodian start-ups represent legitimate competition for international developers and spearhead the majority of disclosed public-private partnerships. Given the RGC’s ambitions, Chinese firms like Huawei, Baidu, and Alibaba could become more involved in hosting the country’s digital infrastructure.

Governing the Internet: Analog Repression and the National Internet Gateway

A final aspect of Cambodia’s digital development has been the RGC’s regulation of online conduct, another area of public policy commandeered by the CPP. Historically, the incumbent party has operated anti-democratic surveillance efforts using state apparatuses and through analog means, with retaliations resulting only after speech drew official attention by being shared or going viral. Lawmakers and a compromised judiciary have aided this process, with the former implementing legislation, including the Telecommunications Law, the Election Law, the NGO Law, the National Internet Gateway Sub-Decree, and the forthcoming Cybercrime Law, granting the RGC greater legal authority to prosecute opposition figures and demand telecommunication firms comply with ad hoc requests to remove content. Prior to the country’s 2018 general
elections, the RGC pursued criminal charges for tax evasion against independent media in the country, forcing Voice of America, Radio Free Asia, and the Cambodia Daily to close.\textsuperscript{55} The same year, a businessperson close to the Prime Minister purchased the \textit{Phnom Penh Post}. Months later, the courts dissolved the opposition Cambodia National Rescue Party (CNRP), while opposition leaders were placed under house arrest or fled Cambodia. The following year, a social media movement to boycott the 2018 elections involved citizens sharing photos of a clean index finger, in contrast to voters whose thumbs are inked at the polls. The Prime Minister threatened prosecution against those with clean thumbs and claimed an intelligent algorithm could detect boycotters' photos with a low margin of error.\textsuperscript{56} Furthermore, U.S. cybersecurity analysts found evidence that hackers associated with the Chinese government hacked Cambodian opposition party figures and the National Election Commission prior to the 2018 elections.\textsuperscript{57}

In the years since, the RGC has convicted hundreds of individuals, who have expressed criticism of the CPP or support of the CNRP online, under "incitement" charges.\textsuperscript{58} Interviewees noted the growth of self-censorship in Cambodian official, academic, and business culture over the past decade.\textsuperscript{59}

In recent years, the Prime Minister's efforts to undermine free speech, political freedoms, rule of law, and democratic institutions have purportedly become algorithmic.\textsuperscript{60} In 2017, leaked emails demonstrated the Council of Ministers had established a so-called "Cyber War Team" (CWT) and installed the Prime Minister's son Hun Manet, a General in the Royal Cambodian Armed Forces, as its director.\textsuperscript{61} An interviewee in civil society claimed the CWT members' Facebook profiles show they frequently attend trainings in China. The interviewee also believed Chinese institutions, such as Huawei, are equipping the CWT with the hardware and software capacity to censor opposition activity.\textsuperscript{62}

Worsening the state of affairs for internet freedoms is the Prime Minister's February 2021 Sub-Decree on the establishment of a National Internet Gateway (NIG).\textsuperscript{63} Seeking to legalize surveillance, the Sub-Decree mandates all telecommunication companies and internet service providers allow traffic to be re-routed through government-controlled and monitored servers "to prevent and disconnect all network connections that affect national income, security, social order, morality, culture, traditions and customs."\textsuperscript{64} Observers have interpreted the NIG as yet another way the Prime Minister seeks to emulate China's style of governance, instituting cyber-sovereignty in the image of the Great Firewall.\textsuperscript{65} The private sector and civil society collectively pushed back against the NIG's establishment during the period between its initial proposal in July 2020 and its adoption into law in February 2021 to no avail. Even business associations objected to the NIG for its creation of systemic vulnerabilities in introducing another single point of failure into the country's internet access; for the grant of power
to a historically protectionist government to directly and arbitrarily block the operations of inconvenient entities; and for “undermining citizens’ rights to internet access, raising grave concerns about freedom of expression, media censorship, and user privacy.”

Senior government officials defended the project as a method of improving tax regulation, citing Cambodia’s long history of fiscal dependence on development partners, and combatting transnational cybercrime and fake news, especially regarding public health following the covid-19 pandemic.

Since the February announcement, telecommunications service providers and other companies have not heard subsequent details or instructions about the NIG’s implementation plan. Nor has the RGC disclosed the entity with which it is contracting to construct the NIG. No interviewee had any further information on the NIG, and interviewees advising the government claim to know nothing about it.

Multiple interviewees involved in the sector stated their belief that either Huawei or ZTE was building the NIG. They explained, the reasoning behind this assertion involves processes of elimination beginning with those contractors technically capable of building such a system. Sources have confirmed that Huawei has built multiple data centres for Cambodian government institutions, as well as the private sector, most prominently for Cambodia’s banking sector, although this revelation is not inherently implicative.

Interviewees also disclosed that news of the NIG caused many in civil society, prominent academics, and even government officials close to the regime to download VPNs, to exclusively use encrypted chatting apps, and to forgo using traditional phone calls, in anticipation of imminent content removals, restrictions, and heightened surveillance. Two interviewees observed how, practically, no matter how effective or operational the NIG is, the threat of panoptic surveillance has already sent a chill through civil society.

III. Cambodian Perceptions of the Digital Silk Road

In Cambodia, the DSR does not have the conceptual prevalence of the BRI; nor that of Cambodia’s own trademark development initiatives, such as the Digital Government Roadmap and Prime Minister’s trademark Rectangular Strategy, which articulates ambition to leapfrog into the “fourth industrial revolution”; nor that of regional development plans, such as the ASEAN Digital Masterplan 2025.

Interviewees noted this is one demonstration of the RGC exercising its agency over inbound CODI: RGC officials utilize the BRI and the DSR insofar as those programs provide development value. One interviewee explicitly rejected the notion that Cambodia “follows” any other country, including those with advanced digital economies.
and digitized governance; they emphasized that the RGC “creates [its] own” initiatives that align with Cambodian needs and values. This claim is subject to two caveats: First, Cambodian agency is largely exerted by an oligarchic elite who enforce policies and direct development in line with their personal proprietary interests. Second, physical telecommunications infrastructure and the critical operations of Cambodia’s emerging digital ecosystem are increasingly reliant not only on foreign suppliers, but largely on foreign suppliers from one jurisdiction. Nevertheless, given Cambodia’s level of development and present inability to manufacture such infrastructure domestically, such interdependence is somewhat inevitable, and thought leaders in the country, if not the Prime Minister, remain eager for and open to diversified sources of investment.

Generally, Cambodian citizens are enthusiastic about accelerated economic connectivity, whether with China or another development partner, yet anxious about and disturbed by the domestic political implications of CODI’s support for the incumbent regime. The dominant viewpoint is represented by prominent academics and policymakers who echo Cambodian Prime Minister Hun Sen in voicing support for most FDI, particularly the BRI and DSR. This group points to a series of positive results of Cambodia’s recent history of absorbing CODI, namely: (1) broad, if uneven, macroeconomic growth; (2) household economic empowerment in regions hosting foreign employers, particularly garment manufacturers which have offered alternative, steady, wage-based employment to individuals whose livelihood previously consisted only of subsistence farming; and (3) increased internet access for all, including lower and middle-income Cambodians, with Chinese firms offering more affordable telecommunications equipment and mobile devices.

Audiences might be sceptical of some thought-leaders’ apparent lack of scepticism of the outsized influence and power of foreign companies. Responses from Cambodian interlocutors should, to some extent, be contextualized within the incentives created by the CPP’s repressive and economically powerful regime. Yet, these beliefs are genuinely held by many.

The genuineness of Cambodia’s development needs are reflected in the central divergence with the majority position between thought-leaders and the Prime Minister. The Prime Minister exhibits blatant favouritism for CODI above other FDI sources. The Prime Minister not only makes outsized concessions to CODI, but also has consistently and uniformly praised the Belt and Road Initiative, China, as Cambodia’s most “ironclad friend,” and CODI, even where industry-wide, country-agnostic criticisms and oversight would be reasonable. Meanwhile, the majority of interviewees support CODI and believe in its value, but do not refuse to raise constructive criticism where it is merited. This group emphasizes that Cambodia does not discriminate between international partners; they explain that Chinese actors are currently the most active
in seeking out opportunities and investments in Cambodia, but that the landscape is open to others. While this may be theoretically true, practically speaking, certain sets of foreign investors face greater legal constraints in entering opaque markets from their jurisdiction of origin than others: For instance, according to interviews, the U.S. Foreign Corrupt Practices Act operates to discourage American investment opaque environments such as Cambodia. If pressed, senior officials in Cambodia—especially those with contacts to academia, small and medium enterprises, and civil society—qualify their support for concessions given to foreign investors by stating that Cambodia should accept “sustainable” development only, implicitly recognizing that CODI has produced irreparable losses to some communities, along with gains elsewhere.76

The dominant neoliberal logic also has particular salience in developing economies and unique resonance in post-socialist Cambodia. All interviewees emphasized Cambodia’s status as a nation recovering from the Khmer Rouge’s decimation of Cambodia’s population, targeting its educated segments, the property and land ownership system, currency valuation, natural resources, culture, and prior technological adaptation. One interviewee noted the majority of senior policymakers and academics in Cambodia, many of whom lived through the Khmer Rouge and the following decade of unrest, have a deeply felt appreciation for stability and concrete economic measures of wellbeing.77

Looking into the future, interviewees uniformly emphasized the significance of CODI in realizing Cambodia’s leapfrogging potential—the nascent economy’s ability to bypass the adoption of legacy technology and to structure governance and commerce around emerging technology. This potential is made more realizable by the occasional top-down drive to develop a digital society and by Cambodia’s demographics. Cambodia has a median age of 25, which suggests technological adaption, once initiated, will happen rapidly.78

Despite the dominant position, simultaneous concern pervades most circles. When considering CODI generally, Cambodians are concerned about: elite cession of sovereignty and valuable natural resources to foreign nationals; increased illicit expropriation of private property and the resultant economic displacement of marginalized citizens; self-aggrandizement of the CPP; and the CPP’s political mimicry of the Chinese Communist Party.79 With respect to the DSR specifically, the concern most frequently cited by Cambodian scholars and activists is that the CPP regime’s alacritous acceptance of FDI from a jurisdiction with dissimilar constraints on overseas commercial actors risks entrenching and even fuelling these structural issues in Cambodian governance that predate and are independent of CODI.
Although little affirmative data undeniably links Chinese entities to inappropriate support for the incumbent regime, many Cambodians assume behind-the-scenes deal-making occurs given the impunity they have seen noncompliant foreign enterprises enjoy in Cambodia, the prevalence of CODI in the market, and the Prime Minister’s otherwise inexplicable and over-the-top affirmations of the close friendship between the two countries.

Many large-scale Chinese investments in Cambodia have distinguished themselves from other multinational players and directly played into this narrative by employing the majority of their corporate social responsibility resources to cash donations to the Cambodian Red Cross (CRC), a charity led by Prime Minister Hun Sen’s wife, Bun Rany, and internationally criticized for lack of transparency. For instance, Union Development Group (UDG) is a Tianjin-based company that was leased 30 percent of Cambodia’s coastline for an unlawfully lengthy period. It has evicted hundreds of Cambodians from their land and been sanctioned by the United States government. UDG regularly makes multimillion dollar donations to the CRC, as does Hong Kong-listed, Phnom Penh-based casino NagaCorp, which, despite raking in USD 500 million in profits in 2018, has been exempted from corporate tax in Cambodia and subject only to ill-defined “obligation payments.” Huawei donated USD 300,000 in 2011 and between USD 10,000 and 20,000 in the last two years to the CRC, an institution from which other investors seek distance.

Pre-existing governance issues in Cambodia—including the CPP regime’s corrupt expropriation of civilian assets, life-threatening under-regulation of certain industries, repression of and violent retaliation against political opposition—can only be sustained through systems of patronage and surveillance. Regardless of the factual extent of Chinese state-linked entities undisclosed facilitation of the CPP regime, the Chinese state is widely perceived by elites and ordinary Cambodians alike as supporting Prime Minister Hun Sen.

Separately, many are sceptical of the feasibility of promised development, such as the plausibility of leapfrogging, and of the concessions demanded in the meantime to achieve it. Given the inurement of Cambodia’s bureaucracy in longstanding modes of corrupt operation and inaction, the lack of adequate educational resources in STEM and IT, and the reluctance of most multinationals to seek out cooperation with the CPP, the likelihood that Cambodia takes advantage of its leapfrogging potential will depend on the extent to which any given e-Government initiative, like Bakong or CamDX, is endorsed by and receives follow-through attention from the Prime Minister himself.
IV. Conclusion

“The DSR is a less ubiquitous and more subtle concept than the BRI, domestic policy initiatives, and regional efforts—reflecting how sources beyond CODI are driving technological innovation and digital development in Cambodia, even if Chinese infrastructure is supporting that innovation. Overall, Cambodian thought-leaders recognize the value of the DSR, yet remain concerned about any program that, even indirectly, empowers the illiberal incumbent party at a critical point of domestic political development. Cambodian enthusiasm toward CODI is shaped by the host country’s history, development status and domestic manufacturing capacity, as well as its political system. Within Cambodia, there is broad consensus that the DSR brings infrastructure connectivity and opportunity to marginalized, particularly rural, populations; and hence, materially supports the eventual provision of positive or substantive rights in Cambodia—social goods ranging from healthcare and education to improved welfare distribution and law and regulatory enforcement. This receptiveness is complemented by openness to all international partnerships, not just those with Chinese institutions, and by the CPP’s sizable agency in channelling imported resources and initiatives toward domestic policy goals aligned with party leaders’ interests. Simultaneously, many in Cambodia, in both elite and other circles, perceive the DSR to be secondarily responsible for a potentially irreversible rollback in negative rights or political freedoms. Ultimately, Chinese firms do not seem to be dictating the terms of Cambodian digital development or governance, but rather answering the host country’s call.”


5 Copy of Outline in author’s possession.

6 Id.


10 Supra note 9.
11 Interview, March 13, 2021.
16 Interviews, March 13, 2021.
17 Supra note 19.
30 Interview, May 27, 2021.
31 Interview, May 24, 2021.
37 Fieldwork interviews, November 29, 2019 and February 20, 2020. For instance, the court system rarely produces written judicial decisions, but when they are written, opinions are kept in hard copy files only accessible through petty bribes to a clerk, making due diligence on business partners difficult.
39 Interview, May 26, 2021; Interview, May 18, 2021.
41 Interview, May 21, 2021
43 Interview, May 15, 2021; Interview, June 2, 2021.
44 Interview, June 2, 2021.
49 Interview, May 22 #1, 2021.
51 Interview May 27, 2021.
52 As a result, some of the leading multinational firms have launched several of their own public service applications on private platforms and retaining ultimate control of all data. Governmental inertia even slows the RGC’s adoption of indigenously created apps in many compelling cases: For instance, Cellcard built Cambodia’s fist vaccine passport within its popular chat app Pouk Mak to aid the country’s tracing efforts. Although it partners with the Ministry of Health data to verify vaccine and test status, the app is not government controlled. “Cellcard launches covid-19 vault storing vaccination records app,” Phnom Penh Post, May 14, 2021, Accessed June 5, 2021, https://www.phnompenhpost.com/business/cellcard-launches-covid-19-vault-storing-vaccination-records-app


Interview, June 2, 2021.


Interview, June 2, 2021; Interview, May 15, 2021; Networked Authoritarianism.


Interview, June 2, 2021.


Interview #3, May 22, 2021.

Interview, May 15, 2021; Sokphea Article 1; Interview, June 2, 2021.


Interview, May 26, 2021.

Cambodia’s repressive political environment contextualizes some of this elite support: Prominent academics and officials are likely to suffer serious retaliation for speech that threatens the CPP regime’s legitimacy or continued ability to illicitly profit from under-regulated and frequently unsustainable foreign investment projects


Interview, May 18, 2021; Interview, May 22 #2, 2021; Interview, May 26, 2021.

Interview, May 18, 2021; Sokphea Young, Internet, Facebook, competing political narratives, and political control in Cambodia, February 2021, Media Asia 48(2), DOI:10.1080/01296612.2021.1881285

Interview, May 26, 2021.

Supra note 75.


I. Introduction: Iran in the Cyber World

This section aims to shed light on the role of Iran in China’s ‘Digital Silk Road’, which is the digital wing of China’s Belt and Road Initiative (BRI). The story of Sino-Iranian tech cooperation cannot be separated from the larger geopolitical and geo-economic processes that the two countries are involved in, especially as those processes relate to challenging the global and regional hegemony of the US. In fact, the two countries’ stories are so interlinked that the Trump administration’s crackdown on Huawei, and its request for the extradition of Meng Wanzhou, the CFO of Huawei, from Canada to the US, was based on the allegation that Huawei’s ‘unofficial subsidiary’, Skycom, violated the Iran sanctions by doing business with Iran. The $1.2 billion fine that was levied on ZTE in 2018 was also due to its alleged selling of sensitive technology to Iran and North Korea. In short, developments regarding Iran are inseparable from Sino-American relations.

It is first necessary to contextualize the topic in terms of the Sino-Iranian relations, Iranian leaders’ view of the emerging global order, and the place of China and Iran in this order. Iranian leadership, both on the conservative and the reformist fronts, view the contemporary world as one in ‘transition’ towards a ‘post-Western world’. In this view, Asia or ‘the East’ is rising, as ‘the West’ retreats. Along these lines, Javad Zarif, the Iranian Foreign Minister and university professor at Tehran University, has co-authored a book with the title ‘Transition in International Relations of post-Western World’ (2016). The country has accordingly developed a doctrine called ‘Pivoting to the East’.

Iranian foreign policy, including its cyber-related elements, is centered on this transitional, ‘East’-oriented worldview. In this emerging global order, Iranian elites view the rise of China (and other Asian powers such as India) as inevitable. This view dovetails comfortably with the Chinese elite view of the emerging global order. Xi Jinping views the present moment in terms of the world ‘facing a period of major change never seen in a century’. Along the same lines, Wang Yi, the Chinese Foreign Minister, has called for ‘a new type of international Relations’. The basic premise of the Sino-Iranian contemporary worldview can be summarized as follows: Western powers are no longer, or should no longer be, the sole actors who set the agenda for global politics and economics. In the new global order, China aims to be a global power and Iran a regional power.
The two actors have formed ‘a comprehensive strategic partnership’\textsuperscript{5}. It is important to note that the relationship between the two countries is a ‘partnership’ and not an ‘alliance’. As far as partnerships go, it is a multifaceted and deep-rooted one. The two countries have numerous ideational, material, historical, and policy affinities (Forough, 2020). Both push the discourse of being ancient continuous civilizations that have survived the test of time. Both emphasize that they never had a major confrontation with each other in their long history. More recently, the two countries have uplifted their partnership to the strategic level through various means, particularly, the New Silk Road (aka Belt and Road Initiative – BRI), China’s geo-economic initiative to ‘reconfigure global economic geography’ (Forough, 2019). Iran plays a (potentially) integral role in the BRI due to the size of its economy and middle classes, energy resources, security partnership with China, relatively well-developed transport infrastructure, and the centrality of its geography. Iranian vision in the New Silk Road is to make itself a civilizational and economic ‘crossroads’ (Forough, 2021) at the intersection of its multiple neighboring regions and countries, such as Caspian Sea region, Central Asia, Russia, Persian Gulf region, the Indian Ocean, the Levant, and the Mediterranean region. To cut a long story short, Iran and China complete each other’s strategic needs in more ways than one.

It was due to such affinities and complementarities that the two countries have signed a strategic ‘25-year-roadmap’\textsuperscript{6} or cooperation framework (with an estimated worth of US$400 billion), covering most of the major strategic areas of cooperation between the two sides. It involves the energy sector, multimodal infrastructure, investment in Iranian manufacturing base, creation of free economic zones, banking, industrial parks, and security and intelligence-sharing, and more relevant for the purposes of this particular report, cooperation in the field of ‘information technology and communication’.

Just as Iran has embraced the New Silk Road, it has also welcomed its offshoots such as the ‘Health Silk Road’\textsuperscript{7} and the ‘Digital Silk Road’ (henceforth, DSR), the digital offshoot of New Silk Road, introduced ‘with a loose mandate’ in 2015\textsuperscript{8}. In more recent years, DSR has taken a more systematic shape through Chinese investments in information and telecommunications infrastructure of countries across the BRI geography. The stated aim is to create digital connectivity in a way that serves the interests of Chinese and recipient countries. This push intensified in the aftermath of the Trump administration’s attack against Chinese tech giants such as Huawei, ZTE, and others. Through the DSR, China aims to solidify its role in the global technology and also find new growth markets (mainly located in the Global South) for its tech players, some of which are banned from North American and several European markets. It is important to note that viewing Chinese DSR purely on its own term and just as a security and surveillance issue is myopic and will inevitably lead to myopic policy analysis and recommendations. A more comprehensive perspective is needed, which should
view the DSR in the larger context of China’s increasingly influential role in global development. ‘The Digital Silk Road’, in other words, is a development issue⁹.

It is the aim of this report to examine Sino-Iranian digital technology cooperation. The analysis will unfold in the four following sections. Part 2 will discuss three events that serve as moments of awakening for Iranian elites (the Flame malware, the Stuxnet attack, and the use of social media in the 2009 political unrest in Iran). Part 3 will discuss the Iranian efforts, inspired by and in cooperation with China, to develop a national internet. Part 4 discusses the geopolitics of 5G development in Iran and the role of Ericson, Nokia, and Huawei in this dynamic. Part 5 concludes the report by discussing the prospects of a Sino-Iranian ‘united cyber front’.

II. Iran’s Three Moments of Awakening in Cyberspace
To understand the role of Iran in cyberspace, it is important to know what put Iran on the global cyberspace map. There are three moments of awakening that happened towards the end of the 2000s, which jolted the Iranian political leadership into putting their cyber act together. The first event pertains to the political unrest in Iran in 2009. The Green Movement came into being in the aftermath of the disputed Iranian presidential election, which resulted in a controversial second term for the incumbent president, Ahmadinejad. The rival campaign of Mir-Hossein Mousavi effectively used social media in the pre-election campaign as well as during the post-election contestation of the results. This met with unprecedented violent crackdown by the country’s security forces. The protesters used social media networks such as Facebook, Twitter, and YouTube to organize protests and inform the international media of the goings-on in the country. The revolution, for better or worse, came to be known as the Twitter Revolution by some Western media¹⁰. This event and the widespread role of internet in it by protesters shook the Iranian political establishment to the core.

The second moment of awakening was the attack known as Stuxnet. This was the first publicly known case in the world where states used a cyberweapon against another state with kinetic consequences¹¹. The malware infiltrated and wreaked partial physical havoc on Iranian nuclear infrastructure. It was uncovered in 2010. Although neither confirmed or denied officially, the attack, codenamed “Operation Olympic Games”, was attributed to the US and Israel ¹². This operation started during the Bush administration and was finalized during the Obama year, and ‘temporarily took out nearly 1,000 of the 5,000 centrifuges Iran had spinning at the time to purify uranium’¹³. During that time, Iran was under a Western sanctions regime. In response to this attack, Iran carried out a cyberattack against ARAMCO, the Saudi oil company, which wiped out more than two thirds of the Saudi company’s IT infrastructure, bringing it close to collapse¹⁴.
The third moment was the massive and highly sophisticated malware that came to be known as the Flame, which was used against computer systems running on Windows in Middle Eastern countries. The majority of infected systems were in Iran. The malware was detected first by the MAHER Center of the Iranian National Computer Emergency Response Team and Kaspersky Lab. The victims included Iranian governmental organizations and educational institutions. The malware could record the audio from devices, monitor keyboard activity, activate the Bluetooth system to infiltrate nearby Bluetooth-activated systems, and take regular screenshots. It is not clear how long the virus was active in Iran and the rest of the Middle East. All evidence points to the fact that this highly sophisticated malware was produced by a state actor and that the main (but not the sole) target was the Iranian political and scientific establishment.

### III. Iranian Cyber Sovereignty: An Intranet Next to the Internet

These three events/processes drove home the unavoidable lesson that a systematic understanding and control of (national) cyberspace was indispensable to the very survival of the political establishment. This understanding was strategic and came from the top. In March 2012, the Iranian Supreme Leader, Ayatollah Khamenei, personally announced the establishment of the Supreme Council of Cyberspace (SCC), which shows how critical this issue is for the leadership. In this background, the so-called Iranian Cyber Army was formed, which is believed to be affiliated with the Iranian military-political establishment. In this context, the idea of the Iranian ‘national Internet’ or ‘National Information Network’ (NIN), which had been formulated and introduced by the Ministry of Information and Communication Technology in 2005, got a serious start in 2013 following these incidents. From 2013 to 2017, under the Rouhani administration, the cybersecurity budget went up by 1200%.

A significant part of Iranian domestic cyberspace policy has been aimed at controlling and surveilling the domestic political landscape, identifying political adversaries, and organizers of anti-government protests. For this type of surveillance technology, Iran is heavily reliant on its international partners such as China. Chinese companies have reportedly provided Iran with the technological means to surveil the Iranian population’s communications. ZTE, China’s second largest telecom equipment-maker, for instance, provided such ‘networking’ technology, in a 2010 deal, to the Telecommunications Company of Iran (TCI), which is government-controlled, and which has a near complete monopoly over landline telephone services in Iran. A considerable proportion of the Iranian internet traffic is supposed to go through its network. The technology was reported to be able to ‘to locate users, intercept their voice, text messaging ... emails, chat conversations or web access’.

As part of the strategic 25-year cooperation deal, cyber cooperation with the purpose of building the Iranian national internet has been mentioned as a clause in the leaked

---

The Digital Silk Road: Perspectives From Affected Countries 27
text of the deal. In this sense, one can see that Iran has practically adopted the Chinese discourse of ‘cyber sovereignty’ or ‘national internet’. Inspired by China, Iran is creating national apps and online platforms (such as Shad, used in online education) to make the country independent from Western digital technology as much as possible. Ultimately, Iranian leaders want to have a functioning closed intranet system for the day to day running of Iranian society, e-governance, and economy, next to being connected to the internet. Then they can shut the country off the global internet whenever they want while enhancing the digitization of society and economy. This vision is both inspired and facilitated by China, whose major tech player have been involved in this process in one way or another. ZTE, as discussed in the introduction, has been involved in Iran and has been fined for it. Alibaba has a strong presence in the country for instance in online ticket purchasing and hotel reservations, car rentals, and such through its Persian language website, which is connected to the Iranian banking system and online shopping.

IV. The Nuclear Deal and the 5G Infrastructure

Iran’s 5G infrastructure development, like many other things Iranian, has been entangled in global geopolitics. After JCPOA (the Iranian Nuclear Deal) was signed in 2015, Iran was allowed to officially do business with the (Western) world again. To develop its 5G network, Iran developed a policy of relying on both the West and China. MTN Irancell, the second largest mobile operator in Iran, and Ericsson signed an agreement to develop the Iranian 5G network. In Sept 2017, the two companies conducted a trial test of a 5G network in Tehran, in an event which was attended by Jahromi, the Iranian ICT Minister, and Ralph Pichler, Ericsson Director for Iran and Turkey, and the Swedish Ambassador to Iran. In a parallel move, Mobile Communications Company of Iran (MCI), the largest mobile operator in the country and one of the largest in the Middle East, signed a Memorandum of Understanding with Nokia to develop part of its 5G infrastructure. MCI owns 58% of the Iranian mobile network. Vahid Sadouqi, the CEO of MCI, and Amr Karim El-Leithy, Nokia director for Middle East and North Africa, signed the MOU. The Chinese tech giants seem to have been sidelined in the Iranian overenthusiasm for connecting with the West in the aftermath of the sanctions being lifted due to Iran Nuclear deal. This situation very much displeased the Chinese (including one can assume the Chinese tech giants) who felt very much ignored if not betrayed. After Trump reimposed sanctions, one can argue that Chinese tech giants, such as Huawei, became the only solid option for Iran.

The Iranians were optimistic that, with 5G, the delayed introductions of 3G and 4G to the country were a thing of the past. In the new 5G era, Iran was hoping to move abreast of the rest of the world. However, the potential promise of cooperation with Nokia and Ericsson came to a grinding halt with the Trump administration’s unilateral withdrawal from the Iran Nuclear Deal and the re-imposition of American sanctions against Iran, which practically cut off the country from the international banking
system. The American sanctions killed almost all the potential for cooperation with Nokia and Ericsson. The latter informed Americans that it was ‘winding down its business and organization [in Iran] significantly’\textsuperscript{27}.

This opened up the space for China in general and Huawei in particular to increase their presence in the Iranian ICT infrastructure scene. China and Iran have agreed in their 25-year strategic deal on the development of Iranian 5G infrastructure network as one of the short-term objectives of the deal\textsuperscript{28}. Needless to say, Huawei is the most likely candidate to develop this infrastructure in Iran. Officially, the Iranian policy is to not rely exclusively on one ICT infrastructure provider, neither Eastern, nor Western. However, with Nokia and Ericsson retreating almost completely from Iran, it is all but certain that China will be the sole or the dominant actor in Iran’s 5G networks. The pace of Iran’s development of 5G is currently slow due to the American sanctions, but it is moving ahead steadily. MCI has announced that it will launch 5G network in five spots in Tehran in March 2021. With the enforced absence of non-Chinese competitors, Iranian 5G development can progress only with the support of China’s providers such as Huawei\textsuperscript{29}.

\textbf{V. A Sino-Iranian ’United Cyber Front’?}

What is most surprising in the Sino-Iranian digital relations is that despite the commonality of the ‘New Silk Road’ as an expression in the Iranian elite and popular discourses, ‘DSR’ (as a discursive trope) is not used much as an expression to describe the Iranian digital relations with China. This goes against the increasingly deepening relations between the two countries in all strategic sectors, including cyber. Further research is required to determine the causes behind this conspicuous lack in the Iranian discourse.

As was shown in this analysis, the story of Sino-Iranian relations in all fields including the cyberspace percolates into some major global dynamics. A consequence of the American reinstatement of sanctions has been that Iran has had to systematically get closer to and rely on China on the (geo)economic as well as the cyber front. This development happened in the context of the US technological cold war against China and its tech giants such as Huawei and ZTE. Iran and China naturally have common grievances against the US as targets of sanctions and tariffs. Since Stuxnet, Iran considers itself in a hot tech war against the US. Since the Trump administration’s crackdown on Huawei, the Chinese leadership consider China to be in a cold tech war or technological ‘decoupling’ with the US. These common grievances, among others, add to the existing Sino-Iranian repertoire of mutual affinities and create new areas of cooperation. In 2019, for instance, Iran and China (together with Russia) conducted a joint naval exercise\textsuperscript{30} in the aftermath of the Trump administration putting heavy pressure on all three countries through sanctions. The 25-year deal with China is rumoured to include intelligence-sharing between the two countries as well. With the
Biden administration coming into office, Iranian oil is already flowing more publicly than before although technically the US has not yet lifted its unilateral sanctions.

Another new area of cooperation is cryptocurrency mining. To evade international banking sanctions and shoring up its economy, Iran has been systematically mining bitcoin. According to University of Cambridge’s Bitcoin Electricity Consumption Index\textsuperscript{31}, during 2020 Iran contributed nearly 4% of global hash rate. The Chinese miners are also heavily invested in crypto mining. In this area there has been cooperation between the two countries as well. Several Chinese companies have moved their assets to Iran due to the cheap price of electricity in Iran\textsuperscript{32}. For Chinese companies, these processes involve Iranian authorities such as Ministry of Energy, Ministry of Foreign Affairs, and ‘even the army in Iran\textsuperscript{33}, which is also reportedly involved in mining bitcoins.

Against the backdrop of American unilateral policy against Iran and China under Trump, these new and old areas of cooperation were solidified in the 25-year roadmap between the two countries. Such processes have led Iranian ICT Minister, Jahromi, to advocate for a ‘common cyber front’ with China against the US on several occasions. In a 2019 meeting with his Chinese counterpart in Beijing, he claimed that China and Iran are already ‘standing in a united front to confront US unilateralism and hegemony in the field of IT.’\textsuperscript{34} According to Iranian state news agencies, Iran and China agreed to form a ‘joint workgroup to survey and counter those threats\textsuperscript{35}. The ‘threats’ come at a time in global and technological history when the question of technology is almost inseparable from the question of geopolitics and geoeconomics. And the united front that the two countries are discussing, needless to say, will involve the conventional questions of technological development such as 5G infrastructure, AI, e-governance, and the like as well as cyber power as it pertains to the military and security domains. The two countries are not likely to become full ‘cyber allies’; however, the strategic partnership is deepening in all fields including cyber.

\textbf{Bibliography}


Forough, Mohammadbagher (2020): ‘Iran and China: Ideational Nexus Across the Geography of the BRI’ in Forced to Go East (ed. by Azadeh Zamirirad). Stiftung Wissenschaft und Politik. Middle East and Africa Division | WP NR. 01, APRIL 2020 Forced to Go East?
Forough, Mohammadbagher (2021) ‘Geographic Agency: Iran as a ‘Civilizational Crossroads’ in the Belt and Road Geography’, in Florian Schneider (ed) Global Perspectives on China’s Belt and Road Initiative: Asserting Agency through Regional Connectivity, Amsterdam: Amsterdam University Press.

Honari, Ali. (2018). “We will either find a way, or make one”: How Iranian Green Movement online activists perceive and respond to repression. Social Media+ Society, 4(3), 2056305118803886

Zarif, Mohammad Javad (2016). Transition in International Relations of Post-Western World, Tehran: Center for International Research and Education.

5 Full Text of Joint Statement on Comprehensive Strategic Partnership between I.R. Iran, P.R. China, Official Website of the President of the Islamic Republic of Iran, 23 January 2016.
9 Arcesati, R., ‘The Digital Silk Road is a Development Issue’, Merics, 28 April 2020.
12 See the following to articles for more details; https://www.nytimes.com/2019/09/04/magazine/iran-strike-america.html and https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gIQAlnEy6U_story.html
18 ‘Iran’s Supreme Leader Sets up Body to Oversee Internet’, BBC News, 14 March 2012.
22 Alibaba’s Persian-language site: https://www.alibaba.ir/
https://static1.squarespace.com/static/54db7b69e4b00a5e4b11038c/t/5f0a3b017adc097c9945645c/1594506439567/China_Iran_Document.pdf
30 ‘China, Russia and Iran Begin Joint Naval Drills’, Aljazeera, 27 December 2019.
31 ‘Bitcoin Mining Map’, Cambridge Centre for Alternative Finance
35 ‘Iran, China Agree to Jointly Counter Cyber Threats’, Mehrnews, 5 July 2019.
Introduction

India is not a signatory to China’s Belt and Road Initiative (BRI), nor its subset, the Digital Silk Road (DSR). Irrespective, India is a notable receptacle of Chinese investments in the digital domain. Most of these investments focus on consumer technology. Considering that Indian policy, academic, and media communities have copiously discussed and often disparaged the BRI since its inception, there is very little awareness of and debate on the DSR. However, there is ample debate and concern over individual DSR constituents: these communities are concerned about China’s role in the country and the region’s digital infrastructure, economy, and security. In South Asia, DSR impact is relatively ubiquitous—the region digitally connects more with China than India. If stakeholders in The Netherlands and like-minded partners in the EU and South Asia desire to slow this trend, it is advised to pursue close interdisciplinary and multi-stakeholder digital cooperation with India.

I. DSR Impact in India and the Region

This section (I) first presents a brief background on Indian views of China’s Belt and Road Initiative (BRI), after which it examines Digital Silk Road (DSR) impact in India and South Asia. Then, in section II, the paper discusses perceptions of the DSR and Chinese investments in India's digital domain.

Background: India’s Disassociation with and Recurring Critique on the BRI

India’s government and academic communities have been one of the world’s most critical voices on China’s BRI. Since the BRI’s introduction in 2013, they have repeatedly questioned the initiative’s transparency, multilateralism, economic rationale, and geopolitical intentions. Initially, the critique was directed specifically towards the China-Pakistan Economic Corridor (CPEC). Not long thereafter, the entire initiative became subject to scepticism: the Indian government has verbally and non-verbally expressed scepticism: in the latter case, by not sending a single delegate to the two Belt and Road Forums held thus far in Beijing. Neither did India endorse the BRI at the 2018 Shanghai Cooperation Organization (SCO) Ministerial Meeting. India is not a signatory to the initiative, and officially there are no investments or activities in India associated with the BRI or its subsets, such as the Health Silk Road and the Space Silk Road.

Two phases of critique in India on the BRI can be distinguished. In phase I, 2014-2017, the debate centered on the initiative’s geopolitical and developmental implications. In
phase II, early 2018 to the present, BRI developmental implications became more nuanced by moving economic, financial, and ecological sustainability of projects to the center of the debate. Equally in this second phase, the initiative’s ‘mishaps’ have been the subject of much discussion and were used to substantiate claims made in phase I. These alleged mishaps included the ‘economic failure’ of CPEC, the so-called ‘debt-for-equity’ Hambantota port deal in Sri Lanka and general allegations of debt-trap diplomacy in the region. It is important to note that in their analyses of the BRI, Indian observers tend to focus geographically on South Asia, and prioritize short-term analysis over long-term strategic understanding.

Impact
There is no formal DSR investment or activity in India. Since the DSR is a subset of the same BRI that India has rejected, the authorities are not receptive to official DSR investments or activities. However, the DSR, very much like the BRI, has an amorphous nature: i.e., Chinese investments in the digital domain do not need to be officially or labelled as the DSR and can, nonetheless, still fulfil the same purpose.

Indeed, India has become a significant recipient of Chinese investments in its digital domain. The Indian government, in an attempt to upgrade technology and digitalization, has long accepted Chinese technology and related investments. Prior to 2014, the Sino-Indian relationship was mostly focused on trade, with a trade balance tilted heavily in favour of China. After 2014, the Chinese state-led trade and business relationship swiftly became more market- and investment driven through Chinese technology giants. These giants spotted the vast sales potential of and connection with ‘the next billion’ and the sizeable pool of English-speaking IT engineers. Indeed, India is home to the second-largest online population after China and the largest emerging digital economy, if we assume China has already “emerged”. Chinese companies thus arose as prominent players and investors, especially in consumer technology and technology start-ups, and have sought to establish a long-term presence without much involvement of either the Chinese or Indian government. Chinese consumer technology goods have come to dominate the Indian market.

Sales of consumer technology goods and mobile apps have proliferated, particularly laptops and smartphones. India is the biggest overseas market for Chinese mobile phone companies. Chinese brands have 70 percent of the local market share. OPPO, Vivo, Xiaomi, and Huawei are in the top five best-selling smartphone brands in India, and the aggregate turnover of all Chinese mobile phone companies in India passed US$7.2 billion in 2018. Chinese companies have even come to customize management, products and services for the Indian market.

Xiaomi, in particular, has customized: the entire leadership team of its local operations is Indian, all locally sold phones and TVs are made in India, and it employs 50,000
Indians. This aided the image and the sales of the company amidst growing anti-Chinese (products) sentiment following the border clashes in 2020. Xiaomi has also expanded quickly: in 2019, it announced its seventh factory in India, and by 2020 it had about 5000 (affiliate) retail stores. Xiaomi has become a significant technology investor in India, the third-largest after Alibaba and Tencent, whose input has already exceeded US$3 billion. They channelled some of these investments to Indian unicorns: 18 out of 30 of these have significant Chinese investment. Even research and development moved locally in some cases: in 2015, Huawei opened its first centre outside of China in Bangalore.

These investments and expansion fit well in the bigger picture of Chinese investments in India—these have grown considerably across various (non-tech) sectors in the last few years. As a result, the Chinese private sector and associated Chinese provincial governments have emerged as important interest groups in molding China’s diplomacy with India. Apparently, Chinese authorities have largely stopped ‘selling’ the BRI and DSR to India. Perhaps, they have come to understand that India’s leadership refused to deviate from their resolute and consistent stance on the BRI. Alternatively, Beijing may have realized that Chinese tech companies had made enormous headway in India anyhow, outside of large connectivity infrastructure projects, and wished not to imperil them.

As with hardware, Chinese mobile app developers and providers have made remarkable headway in India. They invested in a host of local companies that offer online services. These include e-commerce, taxi, music, social media, news, and education services. Another notable new front in India, and South Asia at large, is in Fintech (financial technology). Alipay has steadily become a large player as an investor in Paytm (India), bKash (Bangladesh), and Easypaisa (Pakistan). In Sri Lanka, Alipay has partnered with Dialog Axiata, and the Commercial Bank of Ceylon, and in 2020, Nepal granted Alipay and WeChat Pay permission to operate in the country.

The line between DSR and non-DSR projects is, as with the BRI, ambiguous and subtle. Still, India’s (extended) neighbours in South Asia do, however, also partake in ‘typical’ DSR digital infrastructure, so-called ‘backbone’ projects. The prime examples of these are in telecom. These examples include the China-Afghanistan Fibre-Optic Cable System that runs through the sliver of land that is the Wakhan Corridor; the China-Pakistan Fibre-Optic project, the Pakistan-East Africa Cable Express (PEACE) project; the Nepal-China Fibre Optic Link project; the Nationwide Submarine Cable Öredoo Maldives (NaScom) project; and if considering Myanmar part of South Asia, the China-Myanmar International Terrestrial Cable System. Pakistan’s military has shifted from GPS to China’s BeiDou global navigation satellite system, and similarly, Sri Lanka is preparing for BeiDou use. A new China-South Asia Technology Transfer Centre (CSTTC) was inaugurated in Islamabad, Pakistan, on 8 July 2017.
South Asia is becoming better connected with China than with India. This development worries New Delhi, as it, in turn, erodes Indo-centrism in the region.

Part of this is apparent contradiction is rooted in the fact that India deliberately followed a policy of insulation and non-connectivity with South Asia until the early 1990s. Since then, and expedited by Chinese foreign policy in the region since BRI introduction, India has picked up the pace to connect with the region—including a regional satellite launched in 2017, GSAT-9. Indian connectivity, however, proceeds comparatively lethargically in terms of both traditional and digital connectivity. The next section examines perceptions in India of the DSR and Chinese investments in the digital domain.

II. Perceptions

Perceptions of and analysis on specifically the DSR has thus far been limited in India. Perhaps this is because the DSR projects that get in the media spotlight are typically large digital backbone projects that comprise submarine and terrestrial fiber-optic cables, next-generation cellular networks such as 5G, and China’s BeiDou. India has its own independent satellite system: the Indian Regional Navigation Satellite System (IRNSS). Occasionally there is a reference to the DSR in the media without probing into it. Consequently, analysis fails to connect the dots and assess larger strategic implications. There are some exceptions, and awareness is slowly rising. In 2020-21, some academic observers flagged the lack of debate and analysis on the DSR. Those who debate the DSR often belong to the academic community and are frequently from the same small pool of authors. The debate on the risks associated with Chinese investments in the digital domain are plentiful, however. Most Indian think tanks have covered China’s technological ingress, the Observer Research Foundation (ORF) and Institute of Chinese Studies (ICS) have been quite prolific.

Nearly every publication examined argues that the risks of using Huawei’s 5G technology outweigh the technological and financial benefits. Risks are divided and examined over the government to government, business to business, and business to consumers’ level. While there is an acknowledgment of 5G benefits and Huawei’s competitive prices, there is fear that Huawei could install ‘trap door’ or ‘back door’ technologies that could facilitate espionage, surveillance, cyberattacks, and propaganda operations in recipient countries. This is very much in line with US/the former President Trump administration’s view(s) on security risks associated with Huawei tech. In dealing with China and the BRI-DSR, India and the US may come to seek closer cooperation. In Indian analyses, there is often mention that Chinese law requires Chinese companies to cooperate with their government to support the country’s national interests. Many observers signposted Chinese mobile apps dominance last year, though a few questioned the government’s ban.
Generally, concerns revolved around controlling stakes and data security. However, a small academic and media cohort in India welcomes Chinese investments, pointing out that these bring know-how and allow local technology start-ups to scale-up. Another, although less discussed, matter, is China’s state-paternalistic view on digital governance. India, at least rhetorically, generally supports a more human-centred, multi-stakeholder internet within a multilateral framework. In practice, nevertheless, particularly when considering local internet-shutdown policies in the interest of domestic order, India has a flexible interpretation of human-centric digital governance. While the Indian perspective does not entirely mirror the EU’s human-centric perspective on digital governance in practice, it is more closely aligned to the EU than to China’s.

Indian media, most notably the Hindustan Times, has covered China’s progress on BeiDou on multiple occasions—without connecting it to the DSR. This is exemplary of piecemeal coverage: flagging Chinese technological advancement without linking it to the DSR explicitly. In general, there is little evidence of connecting the DSR with implications for the global digital order and the unfolding Fourth Industrial Revolution.

Likewise, the Indian authorities have also grown more conscious of China’s economic and technological progress and dominance. Amidst the Covid-19 pandemic and not long after violent skirmishes at disputed borders between India and China, the Indian government decided to lessen its dependence on China. It banned 59 popular Chinese mobile apps in June 2020 on grounds of national security, specifically concerns over the data security of Indian citizens. These apps included the wildly popular PUBG Mobile, AliExpress, WeChat and TikTok. After reviewing responses from the companies in question on compliance and data privacy, India decided to sustain the ban indefinitely. In September that year, another 118 Chinese mobile apps were banned permanently as well. Chinese apps have been very popular in India due to their free-of-use nature, but worries persisted over data (ab)use.

Finally, Indian experts have pointed out that the DSR should not just be seen as a standalone technology endeavour since it also aims to connect with BRI and non-BRI Chinese production centres in South Asia and across the globe. In other words, DSR projects synergize BRI projects, China’s global production supply chains, and a generally more China-centric Asian (and global for the matter) digital order. To India, an aspiring tech power, and the central actor in South Asia this prospect is a serious security challenge.
III. Conclusions

India has declined all DSR projects and activities on its soil, particularly the large digital infrastructure projects usually associated with it. However, considering the scale of Chinese investments and market share in the local digital domain, it can be argued that India has ‘unwittingly’ signed up for the DSR. Irrespective of this when considering the DSR’s objective to expand and improve digital connectivity, the Indian market is indeed a prime example of the spirit of the DSR, even if India is not formally a signatory to it.

Chinese consumer technology and apps overwhelmingly dominate(d) the Indian market. However, in the case of the latter, this has been halted by the authorities’ ban on popular Chinese mobile apps following the 2020 violent border disputes between China and India. In the absence of ample competing Indian digital products and services, South Asia has become a noteworthy market for DSR and Chinese digital products and services. In other words, India, through its domestic consumer base’s preferences and neighbours, is respectively steeped in and increasingly 'enclosed' by Chinese digital products and services.

Observers in India have paid attention to China’s growing technology dominance, although not necessarily tying it to the DSR. There is little awareness, debate, or coverage of Chinese digital investments under the auspices of the DSR. Rather, thus far, observers have focused on the DSR’s individual components. This approach has ignored the broader vision, objective, and progress of the initiative in the region. Much of the policy, academic and media debate has focused on Chinese 5G technology risks and Chinese mobile apps’ popularity. It often refers to debates and policy decisions on 5G in the West, often applauding bans. The prevalent fear in these debates is a loss of autonomy, China setting the standards of the digital sphere, the prospect of breaches in the country’s national security due to the national security law in China, and China’s state-paternalistic/authoritarian view on digital governance.

Clearly, China, through the DSR, is filling a large and essential digital infrastructure gap in South Asia—a market of some two billion users. If leveraged prudently by local stakeholders, this can help digitalize these countries and narrow the economic and technological gap with more advanced economies. This digitalization, and associated economic growth, could benefit Indian and EU exporting and digital products and services businesses too. There may, however, be a flip side to that coin, which requires a better understanding of what will the long-term strategic impact of this be? If stakeholders in The Netherlands and like-minded partners in the EU and South Asia wish to curb undesirable impacts, they should pursue close interdisciplinary and multi-stakeholder cooperation with India on digital affairs. Exact avenues of constructive collaboration require further research. Questions guiding that research include what
the consequences for Dutch and India strategic interests are if China, through investments in the digital domain, further cements its position in South Asia as the primary supplier of digital products and services; the extent to which the DSR’s expansion and impact in South Asia aids China’s position in the global digital order; and how the Netherlands, likely together with EU partners, and India best improve their position as competitive suppliers of digital products and services in South Asia?

---

1 This includes think tanks and research centers.
3 India has a complex and uneasy relationship with Pakistan and this corridor crosses territories claimed by India.
5 Interestingly following the Wuhan Summit in that same year, the tone of official Indian critique on the BRI/CPEC became a bit milder.
12 Ibid.


Chinese and Indian interlocutors in conversation with the author in China and India in 2018-19.


Ananth Krishnan is one such example and should be commended for shedding light on these issues. Interestingly the Konrad Adenauer Stiftung (KAS) and the Institute of Chinese Studies (ICS) held a conference on Digital Silk Road implications in New Delhi in the fall of 2019—the author attended it.


33 This is elaborated on in detail in the upcoming LAC-IPCS policy paper: ‘ Acting on China’s Digital Silk Road: Prospects for EU-India Cooperation’ by Ghiasi, Richard and Krishnamurthy, Rajeshwari.


36 Ibid.


I. Introduction

Ethiopia is a landlocked East African country that is connected to the Belt and Road Initiative (BRI) via the port of Djibouti. The Ethiopian Ministry of Innovation and Technology (MIT) aspires for Ethiopia to become Africa’s next tech hub. As a result, MIT revised its fifteen-year-old national science, technology, and innovation policy in collaboration with the United Nations Conference on Trade and Development (UNCTAD) as part of a series of reforms that recently took place in Ethiopia. While the former policy was more focused on introducing the new sector to the country, the current policy is focusing on how the digital economy can benefit other sectors including agriculture and textiles.

The aim of the Ethiopian government to become Africa’s next tech hub and the plan of the Chinese government to promote the digital silk road (DSR) seem to go hand in hand. There are quite a few DSR-related projects already active in Ethiopia in which Chinese firms are involved. Some of these projects, like for example the 3G and 4G telecom infrastructure built by ZTE and Huawei, had been finished before the announcement of the DSR in 2017. Other projects, like for example the help of the Chinese government with the development and launch of Ethiopia’s first remote sensing satellite, started after the announcement in 2017. At the onset of this study, the main research questions were: Is there a lively debate in the country on the DSR, who are the main participants and what are their standpoints?

However, right from the start of the research, it appeared that the DSR is not mentioned in any discourse in Ethiopia. Instead, it appears that the digitalization process of Ethiopia is a local initiative in which China is just one of the many foreign cooperation partners. Ethiopia has a proud history of investing in its infrastructure and has alternated its relations with big powers to stay sovereign.

This chapter will look at the role of China and other foreign partners in the digitalization process of Ethiopia. It will also look at whether the digitalization process of Ethiopia is seen in Ethiopia as a wider regional effort (in line with, or similar to the DSR) or not.

II. Ethiopian Agency

It is important to realize that the digitalization of the Ethiopian economy is an Ethiopian initiative. Ethiopia missed the 1st and 2nd industrial revolutions (and to a large
extent also the 3rd industrial revolution with a focus on computerization and the internet) and the Ethiopian government is determined to not miss the current and 4th industrial revolution. According to Myriam Said, “[t]his is a critical moment. Failing to transition to the digital economy, will really widening the gap between poor and rich economies.”

In June 2020, the Ethiopian government unveiled its Ten-Year National Development Plan (2020-2030), which reflects the belief of the government that technology development is essential for the country’s development. ‘Technology capability and digital economy’ is also one of the ten strategic pillars of the Ten-Year National Development Plan.

The Digital Ethiopia 2025 Strategy – that was drafted in synchronization with the country’s national development vision, policy goals, and prioritized sectors – was endorsed by the Council of Ministers in the same month. The strategy proposes an inclusive digital economy approach that will catalyse the realization of Ethiopia’s broader development vision, in line with the African Union’s Continental Digital Strategy. Although digitalisation is a local initiative, foreign cooperation is not shunned.

On the contrary, speaking at a diplomatic event organized by MIT, Abraham Belay (Minister of Innovation and Technology) requested Ethiopian diplomats to support the country’s digital economic journey by looking for funds and attracting direct investment to the sector. Minister of Foreign Affairs, Ato Gedu Andargachew, added that priority should be given to diplomacy that entails technology transfer to Ethiopia and aide its overall reform agenda.

Over the course of the history of the country, successive Ethiopian leaders have balanced their relations with the West and East. Ethiopian scholar Aaron Tesfaye argues that the impetus for a closer China-Ethiopia relationship only came about when the Ethiopian government recalibrated its relations with the West beginning ’90s. Nowadays, the Prime Minister of Ethiopia wants to reduce the country’s dependence on Beijing and is re-positioning the country to leverage competition between the West and China. How does this balancing act play out for digitalizing Ethiopia’s economy?

III. What Role Does the DSR Play in the Digitalization of Ethiopia?
Extensive research of online Ethiopian newspapers and government documents (in English), and interviews with Ethiopian experts on China and the BRI, demonstrate that there is no mention of the DSR in the discourses on the digitalization of the Ethiopian economy. From an Ethiopian perspective, cooperation with Chinese actors in
the digital domain is perceived to be bilateral cooperation rather than a regional effort to digitalize and connect.

Some Ethiopian experts explain that there is no regional approach to digitalization (yet) because there is still so much to do on the national level. Before Ethiopia can take the next steps in creating a digital economy, they first need to ensure the fundamentals like a reliable supply of electricity and connection to the internet. Ethiopia does receive support from Chinese (and other foreign) actors in these fundamental sectors, electricity, and telecom infrastructure, and most of the digital domains.

The support the Ethiopian government receives from abroad needs to follow the Ethiopian Ten-Year National Development Plan and the Digital Ethiopia 2025 Strategy. In the Digital Ethiopia 2025 strategy, Ethiopia’s digital readiness is evaluated against a digital economy framework comprising of four pillars, namely: Infrastructure, Enabling systems, Applications, and the broader Ecosystem. The remainder of this section highlights the role of Chinese and other foreign partners for the first three pillars.

IV. The Foundational Platforms

Internet access is the backbone on which a digital economy is built. Creating this access requires basic infrastructure such as electricity and transportation, and core connectivity infrastructure that includes fibre optic cables, mobile phone towers, and affordable devices. According to Ms Said, the role of the government is fundamental for the foundational platforms. If the foundational platforms are in place, the private sector will be able to create and build upon these foundations. What is the status of the foundational platforms in Ethiopia and what role do Chinese actors play in this pillar?

Energy

The country has set an ambitious target to supply 100 per cent of its domestic energy demand through renewable energy by 2030. Ethiopia has many renewable resources covering wind, solar, geothermal, and biomass. However, the biggest potential is in hydropower: with 45,000 MW has Ethiopia the second-highest hydropower potential on the African continent, after the DRC. Over half of this potential is located in the Abbay and Omo river basins, where the nearly completed Grand Ethiopian Renaissance Dam (GERD) (with 6,000 MW the largest hydroelectric dam in Africa) and the recently completed 1,870 MW Gibe III project, are located.

Both the GERD and the Gibe III project are partly financed by Chinese banks. The USD 1.8 billion Gibe III project was 40 per cent financed by the Ethiopian Government, and 60 per cent by the China Exim Bank. The Ethiopian government intended to finance the entire costs of the GERD by itself to avoid the risk that a foreign partner could withdraw under pressure from the Egyptian government.
Ethiopia indeed managed to finance a large part of the GERD through internal fund-raising in the form of selling bonds and persuading employees to contribute a portion of their incomes. The turbines and associated electrical equipment of the hydro-power plants (costing about US$1.8 billion) are reportedly financed by Chinese banks. Ethiopian Electric Power (EEP) also signed an agreement with the Chinese company Voith Hydro Shanghai for the installation and commissioning of six turbine generators at the GERD. China Gezhouba Group Corporation Limited (CGGC) signed an agreement with EEP to invest $40.1m in the project for “pre-power generation activities”. The contract to build the dam was awarded to the Italian company Salini Impregilo, the same company that built Gibe I, Gibe II and Tana Beles hydro-power plants.

The ambitions of Ethiopia in generating power reach further than meeting the national needs. The country has regional ambitions when it aspires to become a power hub and the battery for the Horn of Africa.

Telecom Network
Ethiopia was one of the first African countries to introduce telephone communication, and it was the only one doing this outside of colonial domination. However, Ethiopia’s telecom network was virtually destroyed by the end of the war with Italy in 1936. Acute shortages of money and staff led to a further deterioration of the telecommunications facilities that still existed. By the beginning of the 1950s, there was hardly anything left of Ethiopia’s telecom infrastructure. The World Bank proposed to lend Ethiopia money for reconstructing its telecom infrastructure provided that Ethiopia established an independent telecommunications authority. The Imperial Board of Telecommunications of Ethiopia (IBTE) was established in 1951 to which the World Bank lend in total $12.2 million.

The Swedish company Ericsson was a major supplier of telecom infrastructure to Ethiopia during that time. According to Ericsson, it helped that the head of the Ethiopian equivalent of the PTT was a Swede. However, when the military seized power in Ethiopia in 1974, Ericsson closed its technical office. The military government (also known as the Derg) maintained close ties with Russia.

After a long war, the military regime fell in 1991 and the new government established closer relations with the West and China again. The IMF then tried for many years to coerce the Ethiopian government into liberalising the telecom sector and privatising Ethio-Telecom in return for loans and aid. However, the Ethiopian government did not give in and chose to borrow from China instead, to keep control over the telecom infrastructure. In 2006 the Chinese firm ZTE won a deal with state-owned Ethio-Telecom to exclusively develop Ethiopia’s nationwide telecom network.
However, the Ethiopian government was not content with ZTE’s services and decided to invite a competitor to the market. In 2013, ZTE had to share its new telecom deal with Huawei. These two Chinese firms have each gained a 50 per cent share in the carrying out of a US$1.6 billion project to introduce 4G in Addis Ababa and expand 3G services around the country.\(^{34}\)

In 2014, the Ethiopian government introduced another competitor to the market (the Swedish company Ericsson took over part of ZTE’s share in this project), because the Ethiopian government disagreed with ZTE about the costs of upgrading an existing network.\(^{35}\) However, in 2016 Huawei took over a 3G project that was part of Ericsson’s share.\(^{36}\) Huawei and ZTE, therefore, continue to dominate the telecom infrastructure market in Ethiopia.

Besides telecom infrastructure, Huawei and ZTE both also provide Ethiopia with city security surveillance technology.\(^{37}\)

**Affordable Devices**

Much of the hardware found in Ethiopia has been developed abroad and does not always fit the realities on the ground in Ethiopia. The Ethiopian government realizes that it needs to encourage local manufacturing of hardware devices.\(^{38}\) Therefore, MIT and iCog Labs\(^{39}\) jointly organized Ethiopia’s first electronic and hardware design contest called “designed in Ethiopia” in 2018.\(^{40}\)

To make the products designed by Ethiopian designers, iCog turned to China and found a partner in Shenzhen Open Innovation Lab (SOIL). According to Chinese journalist Isabelle Niu: “Hardware engineers in Shenzhen like to brag that they can make electronics for the price of cabbage.”\(^{41}\) It is this affordability and the open-source culture of Shenzhen that attracts Ethiopians (and many other foreign buyers) to Shenzhen.

Besides the affordability, iCog Labs is also likely to be attracted to the attitude of the founder of SOIL, David Li, towards the Ethiopian designers. David Li says he invests in African talents because of his own experiences in Shenzhen that global brands only looked at China as a factory and not as a resource of talent.\(^{42}\) It is this attitude that is more eye-level approach than what they experience in their relationship with Westerners, that African actors value about their cooperation with their Chinese partners.

This cooperation with SOIL is a good steppingstone for developing electronics that suit the Ethiopian context; however, to become independent in terms of critical electronics it is important to also encourage the manufacturing sector in Ethiopia. Besides the fact that foreign-designed and produced hardware often does not suit the local
conditions, it is also more expensive to use foreign hardware. For example, in the case of using the services of foreign satellites.43

With the support of China, Ethiopia launched its first satellite in December 2019. The satellite was jointly developed with Ethiopian and Chinese engineers and the demand and control centre is based in Ethiopia.44 This will drastically decrease the costs for Ethiopia in the long run and fits the plan to acquire new technological skills and increasing the technological sovereignty of Ethiopia.

V. **Enablers**
Enablers are like an intermediary layer that links infrastructure to applications. They are essential to convert connectivity into usable products and services.45 This technology-backed layer allows for rapid verification and transactions.46 The three key enablers mentioned in the Digital Ethiopia 2025 strategy are digital ID, digital payments and cybersecurity. There does not seem to be any Chinese company involved on this level.

For the digital national identification card (ID), the Ministry of Peace of Ethiopia made a deal with the International Institute for Information Technology of India.47

Although China is strong in digital payments and has (like Ethiopia) experience with having a large number of citizens that are “bankless”48, there are no Chinese firms involved (yet) in developing digital payment systems in Ethiopia. Mobile financial services are only allowed in Ethiopia if they are linked to banks.49 That means that there is no place for Huawei’s hardware wallet for China’s digital currency.50 Instead, the Ethiopian government went for cooperation with the Mastercard Foundation.51

Ethiopia has not yet undergone a cybersecurity assessment. Ethiopia lacks cybersecurity experts and expects (rightfully so) that external support may entail a conflict of interest.52

VI. **Application-Level**
Applications are “the gateways through which end-users (individuals and/ or organizations) participate in a digital economy”.53 Examples include government applications for E-Commerce, E-Governance, and E-learning. And applications for services of private businesses like food delivery and taxi services. Chinese firms are involved in the development of different government applications; however, the market for applications for private businesses are dominated by Ethiopian (diaspora) entrepreneurs.
E-commerce
In November 2019, the Ethiopian government signed an MOU with Alibaba Group to join the Electronic World Trade Platform (eWTP), an Alibaba-led initiative that aims to lower barriers to global trade for small and medium-sized enterprises through e-commerce. \(^54\) China Commodities City International (CCCI) partners with Alibaba in the development of the eWTP Hub. As part of the agreement, the Alibaba Business School implements the capacity building and training portion of the partnership which consists of several programs, including specialized programs for Ethiopian entrepreneurs, business leaders and university lecturers. \(^55\)

Two remarkable statements were made during this ceremony. One was the statement by Jack Ma, the founder of Alibaba, who said that Africa does not lack talent and that the continent is not short on resources or opportunity, either. This is remarkably different from the way the African continent has been portrayed by Western media for many years. \(^56\)

The other statement was made by the Prime Minister of Ethiopia who said: "Taking eWTP as one of the e-commerce platforms, Ethiopia aims to facilitate the development of e-trade and the digital economy through the development of e-trade infrastructure and adoption of best practices." \(^57\) By referring to the eWTP as "one of the e-commerce platforms", the Ethiopian government emphasises its diversification strategy.

E-Governance
At the beginning of 2003, the Ethiopian Ministry of Capacity Building and Planning issued a tender for equipment and services for WoredaNet. WoredaNet, partially funded by the World Bank and the AfDB \(^58\), is an e-government network that allows ministers, civil servants, and trainers in the capital to videoconference with the nearly 600 local administrations ("woreda") and instruct local officials on what they should be doing and how. \(^59\) It is a one direction communication: from the centre to the periphery. WoredaNet was developed with the support of two US companies (Cisco Systems and Hughes Networks) who made use of satellite communication. Satellite communication is expensive and inefficient, therefore, part of the fibre optics laid down by ZTE was used to upgrade WoredaNet. \(^60\)

In 2018, a joint venture of three companies (Africom Technologies (Ethiopia), ISYX Technologies (Dubai) and ALROWAD IT Solution (Abu Dhabi)) signed a contract with the Ethiopian government to digitalize the country’s justice infrastructure. ISYX and ALROWAD develop most of the project while Africom customizes the project and the technology to the local context. \(^61\) The National Integrated Justice Information System project costs USD 14.9 million and is fully funded by the Ethiopian government. Nine international IT firms, including Techno Brain, Huawei, ZTE Corporation,
Tech Mahindra, ISYX Technologies and Asseco Group also participated in the bid but did not make the cut.62

E-Learning
Schoolnet is designed to enable students living in Ethiopia’s remote countryside to have access to the same quality of education as those in major towns and cities. At the same time, it is advantageous for the government to have all students exposed to the same programming. It facilitates their training in the founding principles of the state, similar to the US’ strategy during the mid-19th century.63 Schoolnet is partially funded by the World Bank and the UNDP.64 While Schoolnet was, just like WoredaNet, designed and operational before Chinese government support found its way to the country, it also benefitted from the 2006 ZTE agreement for its upgrade.65

In 2016, Addis Ababa University inaugurated the EthERNet platform, a connectivity platform for the Ethiopian Education and Research Network (EthERNet). It connects 36 public universities in Ethiopia to high-speed internet and each other. The network cost US$50 million and was built by ZTE.66

Private Applications and Ethiopian Software Engineers
Private applications for services like taxi-hailing and food delivery seem to be merely initiatives by locals or Ethiopian diaspora. Chinese and other foreign firms do not play a role in this market. For example, all three taxi apps in Ethiopia (ZayRide, RIDE and ETTA) are Ethiopian and the popular food delivery app Delivery Addis was set up by an Ethiopian man who was born and raised in the US.67

Ethiopian software engineers are also active abroad, in China and other foreign countries. For example, Apposit, an Ethiopian software engineering company built, maintained, and is currently supporting Nigeria’s fintech firm Paga (which is within the investment portfolio of American billionaire Tim Draper).68

iCog Labs serves customers in the US, China, Germany and Hong Kong with research activities related to artificial intelligence. Ethiopian developers are in charge of improving image recognition software and other items to improve robot intelligence. For example, software developers at iCog-Labs have developed software for the famous humanoid Sophia from Hong Kong.69 iCog-Lab is also collaborating with a Chinese client to develop a genetic data analysing software to support medicinal and chemistry experimentations. The genetic data project dubbed “Mozi” is sought to assist medical experiments determined to find a cure for cancer.70 On behalf of Californian companies, other lab employees are working on genetic mapping of human genes related to ageing in an attempt to unravel the mysteries of longevity.71
VII. Conclusion

Based on extensive document analysis and interviews with Ethiopian experts on the BRI and China, I conclude that the DSR is not a subject brought up in conversations in Ethiopia. The various projects associated with the DSR are considered to be separate projects and the Ethiopian government has a strong interest in not leaning too much towards one foreign partner and instead diversify its foreign cooperation partners.

Ethiopia is following its own development plan and takes pride in that. The fact that the ITU World Telecommunication Development Conference is hosted in Africa for the first time is seen as a recognition of the digital developments in Africa and Ethiopia specifically.72

Furthermore, Ethiopia focuses much on African agency. To make sure that the ITU WTDC conference will reflect African values, the Ethiopian government has invited all African countries to actively participate in the preparation process of the WTDC.73 This focus on African agency is typical for the country that hosts the AU headquarters and that has managed to resist pressure from the West to liberalize its telecom market when they were not ready to compete with foreign companies yet.

At the moment, Ethiopia is opening up again for investment from the West, investments in general and in the telecom sector, which will be privatized soon. However, the Ethiopian government will ensure that the country does not become too dependent on a specific foreign partner by diversifying its cooperation with various foreign partners. They will avoid becoming a pawn in either the Chinese BRI project or the liberalization project of the West.

European actors can therefore expect to be played-off against other foreign actors and will have to have something interesting to offer to Ethiopia. In the case of satellites, Ethiopia has long been dependent on the expensive services of foreign satellites. Since December 2019, Ethiopia has its own remote sensing satellite in orbit. This satellite was developed together with China and in a way Ethiopia has become a bit more dependent on Chinese technology during this process. However, the satellite was developed with Ethiopian and Chinese engineers together and the control and command centre is in Ethiopia. In other words, much technological spill-over took place and Ethiopia has moved further up the ladder to develop its own satellite technology.

Therefore, if Europe wants to do something about the increased use of Chinese technology on the African continent, it has to offer something else than just the use of European technology. Europe needs to offer support to African countries in developing indigenous technologies so that they can become independent of both Chinese and Western technology.
In the first few months after he came to power, the reform-minded Prime Minister Abiy Ahmed lifted the state of emergency, ordered the release of political prisoners, allowed exiled dissidents to return home, and unblocked many websites and TV channels. He filled half of his cabinet with women. He also ended the state of war with Eritrea by agreeing to give up disputed border territory, for which he received the Nobel Peace Prize in 2019.


Xinhuanet, ‘Full text of President Xi’s speech at opening of Belt and Road forum’, 14 May 2017.


Previously the Director of the National Digital Transformation Program at the MIT where she led the development of “Digital Ethiopia 2025”, and currently senior advisor on the digital economy at the Office of the Prime Minister.


Ministry of Innovation and Technology Ethiopia, ‘Council of Ministers endorses Digital Ethiopia 2025 strategy’, no date.

On 9 February 2020, the African Union adopted its Digital Transformation Strategy (DTS). The DTS aims to harness digital technologies and innovation to transform Africa’s societies and economies to promote Africa’s integration, generate inclusive economic growth, stimulate job creation, erase the digital divide and eradicate poverty to secure the benefits of digital revolution for socio-economic development. In its strategy, the African Union has set sixteen specific objectives, from building a Digital Single Market by 2030 to digitalizing sectors such as agriculture, health and education.

Ministry of Innovation and Technology Ethiopia, ‘Ministry Of Innovation And Technology Calls On Diplomats To Assist Ethiopia’s Digital Transformation Agenda’, no date.


Marks, S., ‘Ethiopia plays Europe off China in bid to boost investment’, Politico, 8 March 2021.


Siemens Gamesa, ‘Siemens Gamesa seals its first wind farm project in Ethiopia, expanding its leadership in Africa’, no date.


International Hydropower Association, ‘Country Profile: Ethiopia’, no date.

European Union Business Forum Ethiopia, ‘Ethiopia, an attractive destination for European direct investment’, no date.


Siemens Gamesa, ‘Siemens Gamesa seals its first wind farm project in Ethiopia, expanding its leadership in Africa’, no date.


Idem.

Ericsson, ‘Ethiopia’, no date.


In 2009, ZTE’s video surveillance solution won the bidding for a city security surveillance project involving placing more than 200 cameras on the roads of the Ethiopian capital, Addis Ababa (ZTE n.d.). The Ethiopian government also has a Safe City agreement with Huawei.


iCog Labs is an Ethiopian research-and-development company that collaborates with international artificial intelligence (AI) research groups and serves customers around the world. It was established by Getnet Aseffa with the help of American researcher Ben Goertzel.


*Quartz*, ‘How Shenzhen is fueling Ethiopia’s burgeoning startup scene’, 24 January 2020.


Ministry of Innovation and Technology Ethiopia, ‘Ministry Of Innovation And Technology Signs Agreement With Mastercard Foundation’, no date.


Idem.


58 Human Rights Watch, “‘They Know Everything We Do’: Telecom and Internet Surveillance in Ethiopia”, 25 March 2014.
59 Gagliardone, I., ‘Are We Getting China-Africa Media Relations Wrong?’, HuffPost, 23 June 2012.
62 https://www.thereporterethiopia.com/content/justice-information-system-project-freezes
63 http://www.homepages.ucl.ac.uk/~uctpimr/research/CSL.pdf
65 https://books.google.nl/books?id=9-c6CwAAOBJAI&pg=PA49&lpg=PA49&dq=woredanet+china&source=bl&ots=T_bYMtlJPz&sig=ACfU3U1JuNblw6VAYZ02pF4btCCqrMo12A&hl=nl&sa=X&ved=2ahUKEwiNotb1j_PuAhVDiqQKHTNgDIAQ6AEwA-noECAMQAw#v=onepage&q=woredanet%20china&f=false
67 https://www.youtube.com/watch?v=okeWRCrOh1M
69 https://www.thereporterethiopia.com/article/it-devotees-working-bigger-ventures-sophia
70 https://www.thereporterethiopia.com/article/it-devotees-working-bigger-ventures-sophia
71 https://worldcrunch.com/tech-science/the-ethiopian-ai-geeks-building-cutting-edge-robots
72 https://www.itu.int/en/ITU-D/Conferences/WTDC/WTDC21/Documents/Speeches/WTDC_Road_to_Ad-dis_Dr_Ahmedin_Remarks.pdf
73 https://www.itu.int/en/ITU-D/Conferences/WTDC/WTDC21/Documents/Speeches/WTDC_Road_to_Ad-dis_Dr_Ahmedin_Remarks.pdf
This report is published by the LeidenAsiaCentre.

Dr Rogier Creemers is an assistant professor at Leiden University’s China Studies Department. His main focus of research is the development of Chinese policy in the digital sphere, both domestically and at the global level.

Molly Bodurtha is a J.D. Candidate at Columbia Law School, where she is a Public Interest and Public Service Fellow. From 2019 to 2020, she conducted research as a Fulbright scholar in Cambodia on Cambodia’s regulatory environment and the impact of foreign direct investment on rural communities.

Dr Mohammadbagher Forough is a research fellow at the GIGA Institute for Middle East Studies. His specific areas of expertise include the international political economy of China with a focus on the Belt and Road Initiative and the contemporary geopolitics and geo-economics of the Middle East.

Richard Ghiasy is a senior fellow at the LeidenAsiaCentre. He researches Asian geopolitics and geoeconomics revolving around China and India, EU strategic interests in Asia, security and connectivity.

Dr Sanne van der Lugt is an academic researcher and fellow at the LeidenAsiaCentre. Her main research interests are Chinese economic activities in Africa, the digital silk road and China’s position in the fourth industrial revolution.