13 Exploring the Political, Economic, and Social Implications of the Digital Silk Road into East Africa

The Case of Ethiopia

Sanne van der Lugt

Abstract
Chapter 13 analyses various causal relations through which Ethiopian and Chinese actors interact in the context of the Digital Silk Road initiative. What is playing out in Africa is part of a larger contest between the West and China for dominance over technology and global influence. From a Chinese perspective, the Digital Silk Road is an attempt to narrow the gap between underdeveloped and developed countries through capacity building. From a Western perspective (Freedom House, Human Rights Watch, etc.), Chinese investments in the Digital Silk Road provide unethical support to authoritarian leaders. The chapter moves beyond this simple dichotomy of good and bad Chinese investments in the digitalization of Africa, instead identifying the actors involved and investigating their motives and levels of influence.

Keywords: Belt and Road Initiative, Digital Silk Road, East Africa, Ethiopia, China, agency

In March 2015, the Chinese government announced plans for a third component of the Belt and Road Initiative (BRI): the Digital Silk Road. The plans for the Digital Silk Road included the construction of cross-border optical cables, transcontinental submarine optical cables, and spatial and satellite information passageways. These would be created to expand information exchanges and cooperation (NDRC 2015). The decision of the

Schneider, Florian (ed.), *Global Perspectives on China's Belt and Road Initiative: Asserting Agency through Regional Connectivity*. Amsterdam, Amsterdam University Press 2021
DOI: 10.5117/9789463727853_CH13

Chinese government to develop the Digital Silk Road could be seen as its reaction to the news that Western spy agencies were tapping submarine cables (see, for example, Goetz et al. 2013). Shen (2018: 2691) suggests that through the Digital Silk Road, the Chinese government aims to create its own 'transnational network infrastructure through submarine, terrestrial, and satellite links, primarily alongside the Belt and Road Initiative countries'.

Ethiopia is one of these Belt and Road Initiative (BRI) countries. The Ethiopian Ministry of Innovation and Technology (MIT)[1] aspires to lead the Ethiopian economy toward tech-led growth. As a result, MIT revised its fifteen-year-old national science, technology, and innovation policy as part of a series of reforms currently taking place in Ethiopia (Ayele 2019).

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 seem to go hand in hand. From an Ethiopian perspective, the transnational network infrastructure that the Chinese government plans to build in the BRI countries is an opportunity to be better connected. Meanwhile, from a Chinese perspective, the Digital Silk Road is an attempt to 'narrow the gap between underdeveloped and developed countries, to remove bottleneck problems holding up the development of relevant countries, and to greatly improve their own production capacity [of these relevant countries]' (Lu 2017). However, the question is whether the cooperation between countries such as Ethiopia and Chinese firms will lead to more or less independence. And who will have control over these technologies?

From a Western perspective (as expressed by organizations such as Freedom House and Human Rights Watch), Chinese investments in the Digital Silk Road are often depicted as the unethical support of authoritarian leaders. This is especially the case when these investments take place in countries with authoritarian regimes. For example, the 'Freedom on the Net 2018' report, an annual country-by-country assessment of Internet freedom published by Freedom House, stated that 'Beijing' took steps to propagate its model abroad by conducting large-scale training of foreign officials and providing technology to authoritarian governments (Freedom House 2018). Perhaps this means that support from the Chinese government leads to more independence for the Ethiopian government, but less independence for the ordinary citizens in Ethiopia.

Western NGOs and the Chinese government use different discourses to convince their audiences that the support of Chinese firms for the digitalization

1 Before 2018 the Ethiopian Ministry of Innovation and Technology (MIT) was called the Ministry of Science and Technology (MoST).

of African countries is either good or bad; that it is either about development or exploitation. With this study, I aim to go beyond the simple dichotomy of good and bad. I will identify the different actors that, with the help of Chinese firms, are involved in the digitalization of East Africa and investigate their motives and levels of influence. Then I will test the dominant propositions that have been made about the social, economic, and political impacts of support from Chinese firms for the digitalization of East African countries. The main question addressed is: In the context of the Digital Silk Road, to what extent does Chinese information and communications technology (ICT) contribute to the Ethiopian government's control over its citizens?

Digital Developments within Ethiopia

Ethiopia is underestimated as a source of digital talent. The country is usually connected with either coffee or drought and drought-related hunger. It might surprise many Western readers, for example, that the Ethiopian software developers of iCog Labs in Addis Ababa developed part of the software for Sophia, a social humanoid robot created by the Hong Kong-based Hanson Robotics (and the only robot in the world with citizenship).

iCog Labs is a 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 (Wuilbercq 2015). The company's core specialty is AI, including machine-learning-based data analysis, computational linguistics, computer vision, mobile robots and cognitive robotics, cognitive architectures, and artificial general intelligence. One of the employees of iCog Labs, Betelhem Dessie, is a good example of the kind of digital talent that exists in Ethiopia. Only 20 years old, she is the founder and CEO of Anyone Can Code, a coding school at iCog Labs that teaches children the skills that are needed for the future job market. Dessie started coding when she was just nine years old (Mella TV 2019). At the age of twelve, she started working as a developer for the Ethiopian Information Network Security Agency (INSA). Aseffa argues that Ethiopian programmers have the same skills as those from China, from the US, and Europe. The only difference is the economic gap and the daily challenges that they face. These challenges include: lack of infrastructure, erratic Internet access, and frequent power cuts (Wuilbercq 2015).

MIT aims to establish Ethiopia as the premier IT hub in Africa. In June 2019, the government approved legislation that would open the telecom market

to competition and provide much needed foreign investment. In September 2019, the process to part-privatize Ethio Telecom, the only provider of telecommunications services in Ethiopia, moved forwards when the company was audited. Meanwhile, it is expected that two licenses will be offered to international operators by the end of 2020 (Lancaster & Lange 2020).

In January 2020, the French company ArianeGroup started to build a satellite manufacturing, assembly, integration, and testing (MAIT) facility in Addis Ababa. The company is using funding from the European Union's European Investment Bank (EIB) (Space in Africa 2019b). After completion, the MAIT facility will be managed by the Ethiopian Space Science and Technology Institute. It is expected to be the centrepiece for Ethiopian satellite technology development and manufacturing. There are currently only two functioning assembly, integration, and testing facilities on the African continent, in Algeria and South Africa. However, Egypt and Nigeria are also building facilities (Ibeh 2019; Ibeh 2020).

State of Research

This section discusses the three main debates examined in this study. These are: 1) the debate about the impact of high technology on development and repression; 2) the debate about the extent to which China-Africa relations pose a threat; and 3) the discussion about the need to include African agency in studies on China-Africa relations.

High-Tech and Development versus Repression

Shen (2018) argues that the Chinese leadership has assigned its Internet companies a central position in the BRI to achieve five major policy objectives: cutting industrial overcapacity, enabling corporate China's global expansion, supporting the internationalization of China's currency, the renminbi (RMB), constructing a China-centred transnational network infrastructure, and promoting an Internet-enabled 'inclusive globalization'. Meanwhile, according to Wang Yiwei, a professor in the School of International Studies at Renmin University, the Digital Silk Road will also offer benefits for participants by efficiently connecting landlocked and developing countries to the global economy through a more inclusive international trade and investment system (Wang in Shen 2018: 2693).

In contrast to the self-interested high-tech discourse's promises about the inherently democratic nature of new information and telecommunication

technologies, Walton (2001) argues that these technologies are embedded in a social context. It is not the technology itself but the way people will use it that leads to either development or repression. However, this does not mean that technology is inherently neutral. Rather, the context in which a new technology is used influences whether the impact of this new technology is perceived as positive or negative.

European development cooperation institutes, such as the German Society for International Cooperation (GIZ), are enthusiastic about the potential of 'digital solutions for sustainable development' (GIZ 2017). However, Western institutes are more critical about the digitalization of African countries when Chinese firms are involved. For example, the 'Freedom on the Net 2018' report by the US-based non-governmental organization Freedom House (2018: 2) states that:

> [Chinese] companies have supplied telecommunications hardware, advanced facial-recognition technology, and data-analytics tools to a variety of governments with poor human rights records, which could benefit Chinese intelligence services as well as repressive local authorities.

China-Africa Relations

In the literature on relations between China and African nations, the main debate has been about whether or not China's growing presence in Africa is a threat to Western or African interests. The blog 'China in Africa: The Real Story' and the associated book *The Dragon's Gift*, both produced by the scholar Deborah Brautigam (2009), have contributed to shifting this debate more in favour of China. Hirono and Suzuki (2014) have suggested that the conclusion that the behaviour of Chinese actors on the African continent is not uniquely immoral is not so surprising. They argue that the idea of a China threat is the result of the heavy influence of Western states' policy interests on the literature on Chinese foreign policy.

Another recurring debate in the literature on Sino-African relations, linked to the idea of a China threat, is the debate about the motives behind Chinese overseas direct investment (ODI) in Africa and the role of the Chinese government in this. Chinese economic cooperation in Africa is seen by some as a 'charm offensive' through which it seeks to win political and economic clout. Buckley et al. (2007) argue that the Chinese government has used ODI to ensure the supply of those natural resources that are scarce in China. This leads to Chinese ODI that is primarily resource seeking. Others have argued that Chinese telecom companies' investments in large

infrastructure networks in Africa are used by the Chinese government for both traditional and economic espionage (Reed 2013).

These theories about the motives behind Chinese ODI all share the assumption that Chinese policymakers have an all-encompassing strategy for Africa. However, as Taylor and Xiao (2009) have rightly pointed out, China is not a centrally controlled, monolithic, unitary actor. There is a multiplicity of Chinese actors operating in Africa. As such, there is a need to go beyond broad studies that look at the motives and practices of Chinese investors in general. Instead, it is necessary to conduct more detailed studies of specific Chinese actors to get a better understanding of the motives of various Chinese players in Africa, as well as their specific practices and the challenges related to these.

Agency

In most analyses of China's engagement with Africa, little consideration is given to the role of African agency (Mohan & Lampert 2012). Brown and Harman (2013) argue that the study of Africa's international relations has for a long time been preoccupied with explaining how the continent has been governed, shaped, and marginalized by external actors. In their book, they ask how far, and in what ways, African political actors are impacting on, and operating within, the international system, instead of looking at how the international system impacts on Africa. Their book attempts to focus on interaction rather than one-way domination.

As a philosophical concept 'agency' refers to the capacity of individuals to act independently and to make their own free choices. The idea of the individual as a 'free agent' – able to make rational choices – was born with the emergence of philosophical individualism in the early Enlightenment. Later, the English philosopher John Locke (1978) rejected the binding power of tradition, affirming the capacity of human beings to shape the circumstances in which they live. According to Emirbayer and Mische, this way of thinking 'embedded agency in an individualistic and calculative conception of action that still underlies many Western accounts of freedom and progress' (1998: 965). Ethiopia is often considered to be a more collectivistic society (Hofstede-insights 2020). It, therefore, makes sense to look at a more relational aspect of agency in this study.

In her research on poverty and citizenship, Lister (2003, 2004) distinguishes between four dimensions of agency and argues that these dimensions interrelate. For example, to act politically, one first requires a sense of personal agency and then acting as a citizen further strengthens that sense

of personal agency. Coulthard (2012) had pointed to how Lister's connection of personal agency with political agency relates to debates from Giddens, Long, and Van der Ploeg about the socially embedded nature of agency. These scholars argue that the capability a person has to act and make a difference to a pre-existing state of affairs or events necessarily involves social relations and can only function through them (Coulthard 2012).

This chapter, therefore, uses a definition of agency that emphasizes the ability to make free choices – either as a group or an individual. How free is the choice made by the Ethiopian government about whether or not to use Chinese ICT? How free are the choices made by groups in Ethiopian society about whether or not to make use of Chinese ICT? Are these actors capable of exercising agency and changing a pre-existing state of affairs?

Methodology

The research question in this chapter is: In the context of the Digital Silk Road, to what extent does Chinese ICT contribute to the control of the Ethiopian government over its citizens? This is a question about both agency and motivation. Currently, most studies of the motives behind Chinese outward direct investment (ODI) are based upon statistical correlation (see, for example, Buckley et al. 2007; Kolstad & Wiig 2012; Ramasamy et al. 2012). However, while such regression analysis can point out the strength of a certain correlation, it cannot prove a causal relationship. For this reason, in the research for this chapter, I have adopted a case study method to answer the research question.

Design

Case studies can make inferences about which causal mechanisms may have been at work by examining intervening variables in individual cases using a method called process tracing. In this way, 'process tracing is a fundamental tool of qualitative analysis' that can contribute decisively to evaluating causal claims (Collier 2011: 823). Process tracing involves a mechanistic understanding of causality. It is the search for intervening variables that link an independent variable with a dependent variable in a process that is commonly referred to as a causal mechanism. When it is possible to theorize a mechanism linking a cause, or several causes, with an outcome, process tracing can be used to test this theory.

To study the impact that the use of Chinese ICT in Africa has on the control that governments have over citizens, a case study is selected which looks at Ethiopia. For this case study, there are various theories which hypothesize causal mechanisms and which we can test. Beach and Pedersen (2016) suggest five steps when using process tracing for theory testing: 1) select typical cases, 2) conceptualize and operationalize the causal mechanism, 3) collect empirical material and evaluate whether there is evidence of the predicted causal mechanism and if we can trust this evidence. When evidence is not found for the whole mechanism, it then becomes necessary to 4) investigate whether the chosen case was idiosyncratic, or when evidence is not found for even a part of the mechanism, it is necessary to 5) engage in theory building to revise the theory.

The following sections will describe how these steps have been carried out in this study of the use of Chinese ICT in Ethiopia. The next section discusses the sampling of data that was performed for this study.

Sample

Ethiopia is an East African country with strong economic relations with China. It is linked to China's BRI via the small neighbouring nation of Djibouti, where Chinese firms have invested heavily in port infrastructure and Africa's first fully electrified transnational railway from Djibouti Port to the Ethiopian capital Addis Ababa (Clemoes 2019). The Ethiopian authorities are focusing on digital economic transformation as part of their Second Growth and Transformation Plan (GTP II). They aim to improve the ICT infrastructure and services in Ethiopia and to enhance the role of the ICT sector in economic, social, and political activities for their country to become a 'low middle-income country by 2025' (National Planning Commission 2016: ix).

This digitization of the Ethiopian economy is being enabled with technology and support from China. The Chinese telecom vendors Huawei and ZTE have dominated the telecom infrastructure market in Ethiopia since 2008, supplying the sole telecom provider in the country, the state-owned Ethio Telecom. This Chinese dominance in the country's digital infrastructure was last year supplemented by the launch of the first Ethiopian remote sensing satellite, which was developed and largely paid for by China and then launched in China (Reuters 2019). It was also increased by recent agreements between China and Ethiopia regarding the joint development of a communication satellite (Space in Africa 2019a) and a new digital trade platform (Gebre 2019).

Ethiopia has long been seen as an authoritarian regime and is still regarded as 'not free' in terms of Internet freedom, political rights, and civil liberties (Freedom House 2020a, 2020b). However, Ethiopia is changing for the better. In February 2018, Hailemariam Desalegn suddenly resigned as the Prime Minister to allow reforms in the country after mass protests led to the loss of life and displacement of thousands of Ethiopians (NTV Kenya 2018). Reports by Freedom House show the progress that is being made in Ethiopia. In 2018, Ethiopia received only 12 out of the maximum 100 points in the Freedom House awards. In 2020, this number increased to 24.

After Hailemariam's resignation, the reform-minded Abiy Ahmed took the position of Prime Minister in a snap election. In the first few months after he came to power, Abiy 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 (Nobel Prize 2019).

However, although Ethiopia is becoming freer it still has a long way to go to be classified as 'free' by Freedom House. A controversial hate speech law, which imposes jail terms for people whose Internet posts stir unrest, was passed in February (Al Jazeera 2020). The question of how the use of Chinese ICT in Ethiopia will impact the government's control over its citizens is therefore highly relevant.

Conceptualization and Operationalization

This study seeks to test whether, and in what ways, the use of Chinese ICT leads to strengthened control of the Ethiopian government over its citizens. To test this, it is necessary to identify the observable manifestations (the potential evidence or 'empirical fingerprints') of the causal mechanisms theorized in the literature. Testing a causal mechanism might be likened to the method of Sherlock Holmes, who looks for evidence that proves or disproves his theories. In the same regard, 'empirical fingerprints' are a kind of evidence that when present can help prove or disprove a causal relation. We, therefore, need to ask: If X causes Y, what do we expect to observe?

Beach and Pedersen (2016) suggest that researchers should first identify as many potential observable manifestations of a causal mechanism as possible. Then they should evaluate the pros and cons of these different observable manifestations systematically, before selecting the most appropriate evidence (empirical fingerprints) of the causal relation to look for

in their data. In this study, one hypothesized causal mechanism is that the use of Chinese ICT in Ethiopia leads to strengthened control of the Ethiopian government over its citizens. We might expect to see the following empirical fingerprints or evidence of this causal mechanism at work:

1 Chinese firms advise the Ethiopian government on a master plan for ICT.
2 Ethiopian firms initiate contact with Chinese firms to acquire hardware and software from them that could be used as surveillance tools.
3 The Ethiopian government requests surveillance tools from China.
4 The Chinese government invites Ethiopian officials for training in China on controlling cyberspace.
5 Chinese firms provide the Ethiopian government with hardware and software that could be used as surveillance tools.
6 Chinese firms provide the Ethiopian government with access to data collected via their technology.
7 Ethiopian officials attend the 2017 World Internet Conference in the Chinese city of Wuzhen.
8 Ethiopian officials attend a Seminar on Cyberspace Management for Officials of Countries along the BRI in China.
9 Ethiopia has an authoritarian regime.
10 The Ethiopian government can legally search and seize personal data at any time.
11 Western firms refuse to deliver surveillance technologies to Ethiopia because of moral objections.
12 The Ethiopian government adopts a cybersecurity law that mimics the Chinese cybersecurity law.
13 The Ethiopian government passes restrictive media laws that mimic Chinese media laws.

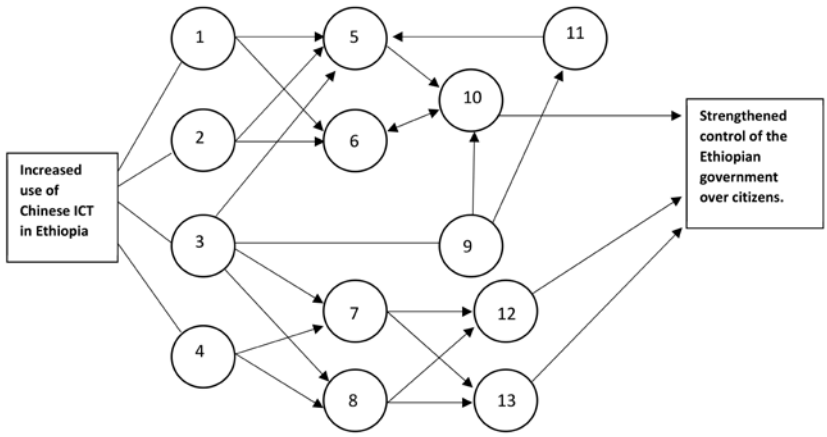
The resulting causal mechanism in figure 13.1 shows how these empirical fingerprints are expected to be linked to each other.

Data Collection

The data for this study consists of both primary and secondary data.[2] I have collected media, academic, government, and company reports dealing with (and either confirming or disconfirming the presence of)

2 I had planned to collect both primary and secondary data. However, due to the COVID-19 pandemic it was not possible to make a field trip to Ethiopia.

Figure 13.1 The causal mechanism



the potential observable manifestations that I identified. Primary data collection was performed using the search engine Google. When this did not yield sufficient, or sufficiently reliable, data about the topic under investigation, I then used my networks in China and on the African continent to supplement this with additional data. The data received from my network in China and on the African continent was always checked for reliability. For example, a Chinese colleague told me that the Ethiopian Minister of Information had attended the World Internet Conference in Wuzhen and sent a link to information about this in Mandarin. On checking the website, the picture of the 'minister' did not match with the actual minister at that time.

The following section will provide an analysis of whether there is evidence to prove the presence of the causal mechanism hypothesized by the literature. To reiterate, this causal mechanism is that the increased use of Chinese ICT in Ethiopia in the context of the BRI is strengthening the control of the Ethiopian government over its citizens.

Analysis

In this section, I test the popular assumption that the Digital Silk Road (and with that the use of Chinese ICT in countries along the Silk Road) benefits repressive local authorities. I do so by carefully studying the case of Chinese ICT support in Ethiopia under the label of BRI.

The previous section discussed the need to identify the evidence of causal mechanisms which analyses should look for, or to ask: 'If X causes Y, what do we expect to observe?' Before we can ask this, however, we need to find out whether X and Y themselves are true, or merely assumptions. Let us first look at X, which in this case is the use of Chinese ICT technology in Ethiopia. It should be asked whether Chinese ICT (surveillance) technology is being used in Ethiopia and whether its use has increased since the announcement of the Digital Silk Road.

From 2008 to 2013, the Chinese firm ZTE was the only telecom vendor building telecom infrastructure in Ethiopia. Since 2013, ZTE has shared this market with the large Chinese company Huawei. These two Chinese firms have each gained a 50% 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 (Maasho 2013). In 2014, the Swedish company Ericsson took over part of ZTE's share in this project because the Ethiopian government had disagreed with ZTE about the costs of upgrading an existing network (Reuters 2014).[3] However, in 2016 Huawei took over a 3G project that was part of Ericsson's share (Fikade 2016). Huawei and ZTE, therefore, continue to dominate the telecom infrastructure market in Ethiopia.

The digital infrastructure over land in Ethiopia is supplemented with digital infrastructure in space. In December 2019, Ethiopia launched its first remote sensing satellite into space. This satellite was developed by Chinese and Ethiopian engineers, largely paid for by the Chinese government, and being launched in China (Reuters 2019). In July 2019, the Chinese and Ethiopian governments also agreed on jointly developing a communication and broadcast satellite (Space in Africa 2019a). In November 2019, another digital connection between China and Ethiopia was created when the Ethiopian government agreed with Jack Ma, the co-founder and former executive chairman of the Alibaba Group, to connect Ethiopia to Alibaba's electronic world trade platform (eWTP) (ENA 2019). Then 2020 started with talks between China and Ethiopia about jointly building a continental satellite data receiver station in Ethiopia (Ibeh 2020). To conclude, Chinese ICT use in Ethiopia has increased since the Digital Silk Road was announced.

Having established that X is true and that Chinese ICT is being used in Ethiopia, it is then also necessary to look at Y. Does the Ethiopian government

3 However, it is important to note that ZTE's strategy for entering into a new market is to initially make an underpriced offer to build a network with the aim of then earning money through the maintenance and upgrading of the project (interviews with ZTE employees in Africa, January 2016).

use technology to exercise control over its citizens and in what ways? According to Freedom House the Ethiopian government still has strict control over its citizens:

> Despite the recent improvements, Ethiopia still has a nationwide Internet blocking and filtering system that can be redeployed at any time for political reasons.
> Anonymous communication is compromised by strict SIM card registration requirements. Upon purchase of a SIM card through Ethio Telecom or an authorized reseller, individuals must provide their full name, address, government-issued identification number, and a passport-sized photograph. Ethio Telecom's database of SIM registrants enables the government to terminate individuals' SIM cards and restrict them from registering for new ones. Internet subscribers are also required to register their personal details, including their home address, with the government. (Freedom House 2019)

It can therefore be concluded that the Ethiopian government has strict control over its citizens that is partly accomplished through technology.

Four players potentially have a key role in the increased use of Chinese ICT in Ethiopia. These are: the Ethiopian government, Ethiopian firms, the Chinese government, and Chinese firms. These are therefore the four potential starting points of the presented causal mechanism.

The remainder of this section tests whether we see the hypothesized causal mechanism at work in the case. To recap, this is a causal mechanism that shows how the use of Chinese ICT in Ethiopia (X) could contribute to the control of the Ethiopian government over its citizens (Y). The section tests for this causal mechanism by looking to see whether those empirical fingerprints that I have previously identified as key indicators of this causal mechanism are present.

Empirical Fingerprint 1: Chinese firms advise the Ethiopian government on a master plan for ICT

The Shenzhen Outbound Alliance (SOA) set up its first African branch in Ethiopia in 2017. According to the SOA, it is responding to the aims of the BRI and is helping Chinese companies to go global. It represents Shenzhen-based companies abroad. According to Sun Tianlu, vice chairman and secretary of SOA, Shenzhen is well-placed to share best practice with other global cities as this is the city where global tech firms like Huawei and ZTE are based (Mamabolo 2017). On its website, SOA claims to have good relations with the Ethiopian government (SOA n.d.).

From this information about SOA, we cannot conclude that Chinese firms necessarily have such a level of influence over the Ethiopian government that they can advise on a master plan for ICT. However, this information does show that Chinese firms often have the means, as well as the contacts, to carry out lobbying. Therefore, while *Empirical Fingerprint 1* can be observed to some degree in the data, the evidence to suggest that Chinese firms advise the Ethiopian government on a master plan is less clear than expected.

Empirical Fingerprint 2: Ethiopian firms initiate contact with Chinese firms to acquire hardware and software from them that could be used as surveillance tools

Ethio Telecom issues the tenders for telecom infrastructure (HRW 2014; Maasho 2015). Ethio Telecom is a state-owned company (HRW 2014). This means that any choice to use Chinese technology is a choice made by the Ethiopian government and not by independent Ethiopian firms.

The project to build and launch Ethiopia's first remote sensing satellite is being run by the Ethiopian government. The Ethiopian Space Science and Technology Institute (ESSTI) is affiliated with the Ministry of Innovation and Technology. It was also ESSTI that signed the Framework Agreement with China for a communication satellite (Space in Africa 2019a).

In other words, the initiative for using Chinese ICT seems to mainly come from the Ethiopian government and not from private firms. Therefore, there is no evidence that Ethiopian firms initiated contact with Chinese firms and so *Empirical Fingerprint 2* has not been observed.

Empirical Fingerprint 3: The Ethiopian government requests surveillance tools from China

As discussed above, when looking for *Empirical Fingerprint 2*, the evidence showed that Ethiopian government agencies have initiated most of the cooperation with Chinese agencies in the realm of digital technology. For example, the communication satellite that will be developed with support from the Chinese government will be fully owned by the government (Space in Africa 2019b). It is too early to judge whether the Ethiopian government will use this communication satellite as a surveillance tool. No public sources are showing that the Ethiopian government has made requests for Chinese technology to use it for surveillance. However, the communication satellite will increase the surveillance capabilities of the Ethiopian government.

Furthermore, the evidence looked at for *Empirical Fingerprint 2* also showed that the Ethiopian government chose ZTE to build the national

backbone. ZTE offers its customers the ability to make use of surveillance software, presenting this software as a tool to manage a customer database (see the discussion of *Empirical Fingerprint 5* for more information about this software). The international non-governmental organization Human Rights Watch (HRW 2014) found that the Ethiopian government has been making use of this software for surveillance. However, this is not conclusive proof that the Ethiopian government requested the surveillance tools from China. Theoretically, it could be that the surveillance tools were an advantage that came with the Chinese technology. To conclude, there is some, limited evidence that the Ethiopian government might request surveillance technology from China and so *Empirical Fingerprint 3* has been partly observed.

Empirical Fingerprint 4: The Chinese government invites Ethiopian officials for training in China on controlling cyberspace

There is information available online describing the training of Ethiopian engineers in China. However, this training seems to be focused on building and maintaining satellites (Space in Africa 2019b). It would be more interesting to know whether Ethiopian government officials have also been sent to China for training in controlling cyberspace. Such training would be more likely to involve the control of information. However, Freedom House (2018) does not mention Ethiopia specifically as one of the countries whose government officials have received Chinese training on controlling cyberspace.

It might be telling, however, that during his 2018 visit to Ethiopia the chairman of the Standing Committee of the National People's Congress of China (NPC), Li Zhanshu, said China will work with the Ethiopian parliament to improve the country's legal environment (Bo 2018). Muferiat Kamil (speaker of the Ethiopian House of People's Representatives) and Keria Ibrahim (speaker of the Ethiopian House of Federation) replied to say that Ethiopia valued cooperation with the NPC. They said that Ethiopia was ready to learn from China's development experience. During his stay, Li also visited the data centre of the Ethiopian Ministry of Science and Technology.

From this information, we cannot conclude that the Chinese government invited Ethiopian officials for training focused on controlling cyberspace. However, such training was likely included in the broader training that the Chinese government has offered to Ethiopian officials. Therefore, *Empirical Fingerprint 4* has not been observed. No evidence has been found that the Chinese government invited Ethiopian officials for training in controlling cyberspace, but it has also not been shown that this definitely has not occurred.

Empirical Fingerprint 5: Chinese firms provide the Ethiopian government with hardware and software that could be used as surveillance tools
In 2008, the Chinese firm ZTE won a deal with Ethio Telecom to exclusively develop Ethiopia's nationwide network to cover fourteen major cities in Ethiopia. In 2009, ZTE's video surveillance solution won the bidding for a city security surveillance project in Ethiopia. This project involved placing more than 200 cameras on the roads of the Ethiopian capital, Addis Ababa (ZTE n.d.). In 2013, ZTE and Huawei together won a new deal to introduce 4G in Addis Ababa and expand 3G services around the country. As mentioned previously, the Swedish company Ericsson took over a part of ZTE's share in this project in 2014. However, in 2016 Huawei again took over part of Ericsson's share. As a result, the Chinese firms Huawei and ZTE are still the main providers of telecom infrastructure for Ethio Telecom, which is Ethiopia's sole telecom provider.

According to Human Rights Watch (HRW 2014), information on all phone calls and text messages in Ethiopia is stored and easily accessed through Ethio Telecom's customer management system, called ZSmart. The customer management software was developed by ZTE. It should be noted that this software is rather common and has not been specially developed for the Ethiopian government. It is also in use in the Netherlands and Germany (Dutch IT-channel 2014), for example. Human Rights Watch suggests that, unlike democratic countries, Ethiopia also makes use of the software's potential to record phone calls and text messages, as well as ZTE's centralized monitoring system, called ZXMT. Human Rights Watch quotes Eric King from Privacy International, one of the world's leading researchers on surveillance technology, who states that:

> One of the things that sets ZTE apart is that when it enters a telecom market it often packages all of its products together as part of its contract, so you get the 'lawful' interception products unless you specifically request to opt out of it. Not too many governments that ZTE does business with are likely to do this. (HRW 2014)[4]

In March 2019, Ethio Telecom and ZTE agreed to establish a joint innovation centre. As part of this agreement, ZTE donated and deployed new technologies worth more than US$3 million to help build the innovation

4 HRW emphasizes that the term 'lawful intercept' is used by equipment makers as an industry label for systems that enable surveillance and does not necessarily mean surveillance practices are legal under national or international law.

centre (Ethio Telecom 2019). The agreement to establish the centre dates back to the middle of 2017 when the two institutions decided to further develop their cooperation and collaborative engagement. In 2017, Ericsson was close to bankruptcy. The timing of the initial agreement could therefore have been an attempt by ZTE to regain some of its market share in Ethiopia after losing business to Ericsson and Huawei.

From this information, we can conclude that Chinese firms have provided the Ethiopian government with hardware and software that could be used for surveillance. Therefore, *Empirical Fingerprint 5* has been observed.

Empirical Fingerprint 6: Chinese firms provide the Ethiopian government with access to data collected via their technology

The Ethiopian government also has a Safe City agreement with Huawei. Safe City initiatives are Huawei's flagship public safety solution for providing local authorities with a wide range of modern products intended to improve policing efforts. When asked if Huawei implemented any safeguards to ensure the technology would not violate human rights, Adam Lane, senior director of public affairs for Huawei's Southern Africa division, said:

> Huawei does not manage, use or have access to any of our systems – we only sell them to the customer and train them how to use it. It is up to individual countries to set their own policies, regulations and laws to govern how such systems are used, and for their legal systems to ensure implementation. (Lane in Woodhams 2020)

From this information, we can conclude that Chinese firms provide the Ethiopian government with access to data collected via their technology. To conclude: *Empirical Fingerprint 6* has been observed.

Empirical Fingerprint 7: Ethiopian officials attend the 2017 World Internet Conference in the Chinese city of Wuzhen

On the official website for the 2017 World Internet Conference, a list of important guests with their photos indicates that the Ethiopian Minister of Information attended. However, the picture of the minister on the site does not match the description given. The man in the picture is not the former Ethiopian Minister of Communication and Information Technology Debretsion Michael.

From this information, we cannot conclude anything. No evidence could be found that Ethiopian government officials attended the conference and

so *Empirical Fingerprint 7* could not be observed. However, it could not be proven that such officials did not attend the conference either.

Empirical Fingerprint 8: Ethiopian officials attend a Seminar on Cyberspace Management for Officials of Countries along the BRI in China
It was not possible to find any information on the attendance of this seminar. However, this does not necessarily mean that Ethiopian officials did not attend this seminar.

Again, from this limited information, we cannot conclude anything. Therefore, *Empirical Fingerprint 8* could not be observed, however, it was also not possible to show that some Ethiopian officials did not attend the seminar.

Empirical Fingerprint 9: Ethiopia has an authoritarian regime
Although Ethiopia is reforming, it is still regarded as 'not free' (the lowest category) in terms of Internet freedom, political rights, and civil liberties (Freedom House 2020a, 2020b). In February 2020, a controversial hate speech law that imposes jail terms for people whose Internet posts stir unrest was passed (Al Jazeera 2020). Therefore, there is evidence that Ethiopia has an authoritarian regime and so *Empirical Fingerprint 9* can be observed.

Empirical Fingerprint 10: The Ethiopian government can legally search and seize personal data at any time
The 1995 Ethiopian Constitution introduced a range of privacy safeguards, which were informed by the privacy provisions found in international human rights instruments to which Ethiopia is party. However, the right to privacy is not absolute in Ethiopia. It can be limited to protect other competing interests (such as national security or the public peace, the prevention of crimes or the protection of health, public morality, or the rights and freedoms of others) provided in subsidiary laws if the necessary conditions are met (Taye & Teshome 2018). These limitations to privacy and data protection are actually similar to those that are found in the European Union (EDPS 2020). It is the way government officials use this space that determines how protected citizens feel.

The Ethiopian government collects personal data. For instance, the Registration of Vital Events and National Identity Card Proclamation allows the collection of personal data, as well as the transfer of this data to various institutions, including intelligence authorities, without consent (Federal Negarit Gazeta 2012). Again, the same applies to European Union countries. However, one main difference seems to be the lack of adequate legal, regulatory, and policy frameworks in Ethiopia (Taye & Teshome 2018).

Another important difference between Ethiopia and EU countries in this respect is the fact that Ethiopia has only one telecommunication service provider: the state-owned Ethio Telecom. Ethio Telecom requires a lot of personal information from users when they register SIM cards. It has access to all phone calls and text messages sent via its networks. It is more than likely that the 'not free' Ethiopian government collects and monitors this data. Ethiopian refugees interviewed by Human Rights Watch (HRW 2014) have stated that the Ethiopian government has access to their call histories and messages. However, the revelations made by Edward Snowden in 2013 have shown that this is not unique for so-called authoritarian states and that the US government also conducts mass surveillance of its citizens.

To conclude, evidence that the Ethiopian government collects data on its citizens has been found and so *Empirical Fingerprint 10* has been observed. However, it may be noted that this finding is not unique for Ethiopia.

Empirical Fingerprint 11: Western firms refuse to deliver surveillance technologies to Ethiopia because of moral objections

A report by Human Rights Watch (HRW 2014) on telecom surveillance in Ethiopia stated that in 2012 a FinSpy command and control server had been discovered in Ethiopia. FinSpy is an example of a type of remote monitoring tool (often referred to as spyware or malware). In 2012, the FinSpy software was still owned by a UK-headquartered company called Gamma International, which said it sold this software exclusively to governments (the software is now owned by the German company FinFisher). The Human Rights Watch report argued that the presence of a command and control server in Ethiopia did not by itself mean that the Ethiopian government was deploying FinSpy. However, the report also said that 'given the high costs of these tools and the fact that Gamma states it only sells to governments, it is unlikely that a nongovernmental party would have purchased and used the tool in Ethiopia' (HRW 2014). The software has been found in the devices of Ethiopian citizens who are living overseas and who have links to Ethiopia's opposition party.

Human Rights Watch has also reported the use of spyware from the Italian company Hacking Team. It reported that this spyware was employed in an attempt to hack into the Ethiopian Satellite Television Service (ESAT) – a diaspora-run satellite television station. Hacking Team offers a product called 'Remote Control System', which allows the user to take control of infected computers or mobile phones. Like the FinSpy software, the Remote Control System is very expensive software and Hacking Team has stated that it only sells this software to governments,

particularly to law enforcement or intelligence agencies. According to its publicly available customer policy, Hacking Team does not sell products to governments or countries blacklisted by the US, EU, UN, NATO, or ASEAN. However, Ethiopia is not on any of these sanctions lists. Human Rights Watch asked Hacking Team about whether it had discovered any 'red flags' during its review process in Ethiopia. In response, Hacking Team said that it 'expect[s its] clients to behave responsibly and within the law as it applies to them'.

From this information, we can conclude that not all Western firms have refused to deliver surveillance technologies to Ethiopia. Therefore, the evidence does not show that Western firms refuse to provide technologies to Ethiopia and so *Empirical Fingerprint 11* has not been observed.

Empirical Fingerprint 12: The Ethiopian government adopts a cybersecurity law that mimics the Chinese cybersecurity law

In this case, mimicking implies that the Ethiopian government actively and consciously followed the example given by China's laws. This seems to be the case. However, Fourie (2015) has argued that this mimicking is more likely to be the result of an Ethiopian tradition than the result of efforts made by the Chinese government to export its model. She has described how for decades Ethiopian elites have looked at 'frontrunner' countries to draw lessons. These elites not only looked to the models offered by European countries such as France and the UK but also looked to Japan and other nations for models. In the 1970s and 1980s, the repressive Derg government looked at the Soviet Union as a model.

Fourie (2015) explained that when the Ethiopian People's Revolutionary Democratic Front (EPRDF) ousted the Derg in 1991, it found itself at a critical juncture. The various rebel groups that comprised the EPRDF had all been founded and run on communist principles, yet the ideology had now become unpopular both globally and within the country. As a result, there was a period of relative ideological uncertainty in Ethiopia.

The desire shown by Prime Minister Meles Zenawi, as well as other members of the EPRDF, to learn from China is in line with these historical processes. In 2005, Ethiopia's most democratic elections to date ended in chaos and contestation. Some believed that the electoral violence was a result of Ethiopia having tried to liberalize too much and too soon. This belief led to arguments that Ethiopia should adopt a model that would allow it to reap the rewards of the global market while keeping control firmly in the hands of a strong and authoritarian ruling party. The model for this was found in China.

Gagliardone (2014) has argued that the Chinese government has aided Ethiopia both indirectly, by offering legitimation for alternative models of media engagement, and also directly, through the provision of essential technical and financial support. The Chinese government's offer of a US$1.9 billion loan in 2006 was a critical factor in the Ethiopian government's ability to expand mobile services and Internet connectivity while keeping the state-owned Ethio Telecom as the only player in the market.

However, we have to keep in mind the agency that the Ethiopian government has in choosing its own development path. As Fourie (2015) has also explained, the initiative to adopt elements of the China model came from the Ethiopian elite, who were looking for examples abroad of how to manage economic development while resisting neoliberalism. Political stability is one of the core aims of the governments in both Ethiopia and China. As Gagliardone (2014) has noted: 'Even the increasingly popular "Africa rising" narrative is placing greater emphasis on stability, as a precondition for investments, over rights.'

At the moment, the Chinese government is putting more effort into promoting its cybersecurity model abroad. In the International Strategy of Cooperation on Cyberspace (Ministry of Foreign Affairs of the PRC 2017), Chinese Internet firms were encouraged to go global and to help developing countries with such things as distance learning, remote health care, and e-business to contribute to their social development. The promotion of Chinese technology exports seems to still focus on serving the main goal of the Chinese government, namely maintaining political stability. China's 2017 International Cyberspace Cooperation Strategy emphasizes Internet sovereignty. With the export of Chinese technology, the Chinese government makes it possible for developing countries to claim Internet sovereignty and experience its benefits. This then means that these developing countries will likely support this Chinese concept in international institutions.

From this information, we can conclude that the Ethiopian government actively and consciously mimics the Chinese cybersecurity law. Therefore, evidence of *Empirical Fingerprint 12* has been observed.

Empirical Fingerprint 13: The Ethiopian government passes restrictive media laws that mimic Chinese media laws

When Prime Minister Abiy Ahmed was awarded the Nobel Peace Prize in October 2019, the Nobel committee praised his 'discontinuing media censorship' among a series of achievements made during his first hundred days in power in 2018. Ethiopia jumped 40 places in the 2019 World Press

Freedom Index compiled by Reporters Without Borders – from 150 to 110 out of 180. This is the largest leap that has been made by any country.

At the same time, Freedom House has criticized the current Ethiopian government for repressing media and repeating the authoritarian ways of previous governments. In particular, it has criticized the ongoing implementation of a controversial Anti-Terrorism Proclamation to stifle dissent. One reason for the restrictions that is given by Prime Minister Abiy is that Ethiopian media are 'fomenting unrest'. In this respect, Abel Wabella, the managing editor of the Addis Ababa-based newspaper *Addis Zebye*, has said in an interview with the German news organization Deutsche Welle that:

> The problem now is that so many individuals are mixing up the roles of activist and media when they shouldn't go together – media is meant to have its own ethics and rules. You have people running media who are calling for protests – it's totally absurd. (Jeffrey 2019)

Eskinder Nega, a prominent Ethiopian journalist and blogger who was released from prison under Abiy's reforms in early 2018, admits that journalists double as activists 'as a necessity':

> We have found out as Ethiopian journalists that to be a journalist you have to have a liberal democratic order, but if you live in an authoritarian setting, it's not going to work. So, whether you like it or not, to be a journalist here, you have to struggle for democracy, you have to double as an activist. (Jeffrey 2019)

Kiya Tsegaye, an Addis Ababa-based lawyer, argues that Ethiopia is a fragile society and therefore that a Western, liberal-style, free media is not possible. He argues that Ethiopia is in a transitional time and that the government needs to intervene to keep the country stable.

Some Ethiopian journalists have noticed a trend that has occurred after every regime change since the fall of Haile Selassie in 1974. Initially, new media flourish with the lifting of restrictions, but within a few years, the new government once again begins cracking down and attempting to put the lid back on what it opened.

Abiy Ahmed may be following this trend, or he may be really working on long-term reforms for the media in Ethiopia and just being careful in doing so. Regardless of which of these is true, Ethiopian media law seems to reflect the national situation at different times. For example, in the middle of June 2020, Ethiopia's state-owned telecommunications monopoly, Ethio

Telecom, suspended the country's Internet service for more than a week. It is suspected that they did this because the government was trying to block the leak of national exam answers (Mbah 2019). Then again, on June 22, there was another Internet shutdown enforced across Ethiopia, after a group of soldiers staged a failed coup in Amhara state.

In other words, Ethiopian media law does not appear to have been mimicking China's media law but instead following its own path. Therefore, *Empirical Fingerprint 13* could not be observed.

Conclusion

This study found that the empirical evidence partly supports the hypothesis and popular belief that increased use of Chinese ICT in Ethiopia leads to strengthened control of the Ethiopian government over its citizens (see figure 13.2). The 'fingerprints' that are coloured green are the fingerprints where I found evidence to suggest that the causal mechanism was present. The 'fingerprints' that are coloured red are the fingerprints for which I found evidence that challenged the idea that this causal mechanism was present. The fingerprints that are coloured grey, are the fingerprints for which I did not find confirming or disconfirming evidence. The fingerprints with the green stripes are the fingerprints for which I found some, but limited, evidence to support the presence of this causal mechanism.

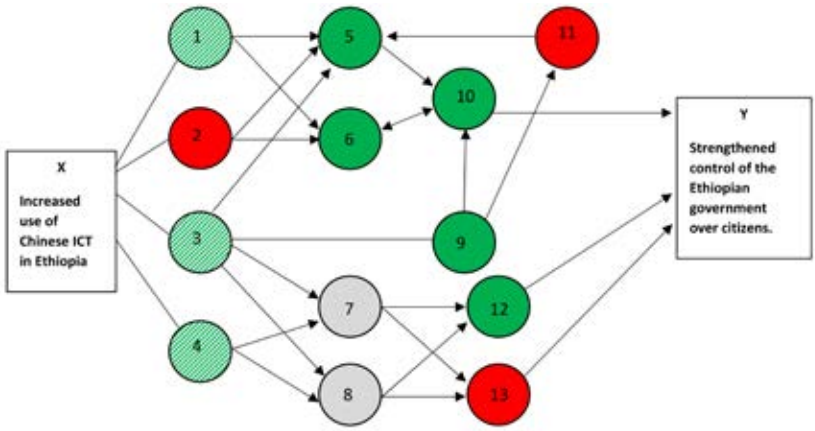
When we look at figure 13.2 we see that there are two most plausible routes:

Route 1:
X (3) 5 + 9 10 Y

Route 2:
X (1) 5 + 6 10 Y

To begin, let us follow the first set of causal links that can occur in this causal mechanism (Route 1), shown by the first green path in figure 13.2. One example of the increased use of Chinese ICT technology in Ethiopia (X) that has been partially observed in this study is that the Ethiopian government requested surveillance tools (3) and has received Chinese technologies that could be used as surveillance tools (5). The findings show that the Ethiopian government initiated most of the cooperation with Chinese agencies in the realm of digital technology. The combination of the fact that the Ethiopian

Figure 13.2 The resulting causal mechanism



government classifies as an authoritarian regime (9), has access to surveillance tools (5) and can legally search and seize personal data at any time (10) leads to the fact that the Ethiopian government strengthened its control over its citizens (Y).

However, the findings for *Empirical Fingerprint 11*, or the fact that Western companies did not appear to be refusing to supply the Ethiopian government with software on moral grounds, suggests that this causal process does not only occur for Chinese ICT support to Ethiopia. Despite the fact that many Western countries have criticized the export of Chinese surveillance tools to authoritarian states, Human Rights Watch has demonstrated that European companies also sell surveillance tools to the Ethiopian government. The Chinese company ZTE appears to offer more ways for the Ethiopian government to monitor the users of its network than either Huawei or the European companies Ericsson and Nokia. However, with the software provided by European companies such as FinTech and Hacking Team, the Ethiopian government can collect similar information to that which it collects with the ZTE software ZSmart. This means that the outcome would not be so different if the Ethiopian government did not use Chinese ICT and instead made use of other foreign ICT.

Now let us follow the second set of causal links that can occur in this causal mechanism (Route 2), also shown as a green path in figure 13.2. The fact that Chinese firms have the means and contacts to advise the Ethiopian government on a master plan for ICT (1) is another potential example of the increased use of Chinese ICT technology in Ethiopia (X) that has been partially observed in this study. It has then been found

that Chinese firms provide the Ethiopian government with hardware and software that can be used as surveillance tools (5) and that they also provide the Ethiopian government with the data that these tools collect (6). Furthermore, this study has found that the Ethiopian government can legally search and seize personal data at any time (10). This means that Chinese ICT strengthens the control of the Ethiopian government over its citizens (Y).

It appears that on the Chinese side it is the commercial interests of Chinese firms, rather than the geopolitical interests of the Chinese government, that is driving involvement in Ethiopia and the supply of technology to the Ethiopian government. On the Ethiopian side, the government's desire to enhance its control appears to be the reason why it has chosen to work with ZTE instead of with European companies such as Ericsson or Nokia, and also the reason why it has chosen to develop satellites together with China. The Ethiopian government has only been able to maintain its monopoly over the telecoms industry, held by the state-owned telecom provider Ethio Telecom because it has been able to borrow money from the Chinese government to build an advanced telecom network. The Ethiopian government also may have decided to develop its own satellites in cooperation with the Chinese government to break from its dependence on foreign satellites for which the costs were considered too high.

To answer the main research question: This study has found that in the context of the Digital Silk Road, the use of Chinese ICT does contribute to the control of the Ethiopian government over its citizens. However, it should be noted that the main Chinese actor involved in the digitization of Ethiopia does not seem to be the Chinese Communist Party (CCP) or the central state, but commercial and state-owned enterprises. This does not preclude 'Chinese influence' (i.e. state influence) but points to the complexity of the reality on the ground.

The main Ethiopian actor that is actively bringing in Chinese ICT is the Ethiopian government. However, this study has found that the Ethiopian government also acquires ICT from German, French, Italian, and British companies.

The focus in Western media on China's export of surveillance technology to Ethiopia attributes most of the agency to Chinese firms and the Chinese state. However, this study has found that the Ethiopian government has the agency to independently choose what technology it acquires and from where. By cooperating with China as well as Europe to develop its own space technology, the Ethiopian government safeguards its negotiation position and capacity to act independently.

At the same time, this study has also found that non-state actors in Ethiopia (like iCog Labs) are putting much effort into developing home-grown and state-of-the-art technologies. With these efforts, they are perhaps helping to make their country more independent from foreign technologies.

From a European perspective, it would have been more desirable if Ethiopia had to open up its telecom market to improve its network and if the Ethiopian government remained dependent on Western-made satellites. However, the Chinese government has increasingly offered an alternative to these options and as a result, the tables have now turned. The Ethiopian government is increasingly leaning on Chinese ICT. This has made it of greater interest for Europe to promote the technological self-sufficiency of Ethiopia as a way of ensuring it does not become too dependent on China. The European funding for a satellite MAIT facility in Ethiopia is a step in that direction.

As Gagliardone (2014) rightly points out at the end of his article on new media and the developmental state of Ethiopia:

> The Ethiopian government is unlikely to radically revise its media strategy in response to donor criticism. But it may evolve a more open and responsive system over time if it is encouraged to reform from within, in a way that is consistent with the principles on which the state has been founded.

Throughout history, the Ethiopian leadership has striven to leapfrog by learning from other states while keeping a focus on maintaining stability in the country. This is how the impact of the use of Chinese ICT on the control of the Ethiopian government over its citizens should be interpreted.

References

Al Jazeera (2020, February 13). 'Ethiopia Passes Controversial Law Curbing "Hate Speech"'. *Al Jazeera*. Retrieved 19 March 2020 from https://www.aljazeera.com/news/2020/02/ethiopia-passes-controversial-law-curbing-hate-speech-200213132808083.html.

Ayele, Behailu (2019, January 21). 'Ethiopia: Ministry Manoeuvres toward Digital Economy'. *Tralac*. Retrieved 20 March 2020 from https://www.tralac.org/news/article/13847-ethiopia-ministry-manoeuvres-toward-digital-economy.html.

Beach, Derek & Pedersen, Rasmus B. (2016). *Causal Case Study Methods: Foundations and Guidelines for Comparing, Matching, and Tracing*. Ann Arbor: University of Michigan Press.

Bo, Xiang (2018, May 12). 'China's Top Legislator Visits Ethiopia to Boost Bilateral Ties'. *Xinhua*. Retrieved 20 March 2020 from http://www.xinhuanet.com/english/2018-05/12/c_137173731.htm.

Brautigam, Deborah (2009). *The Dragon's Gift: The Real Story of China in Africa*. Oxford: Oxford University Press.

Brown, William & Harman, Sophie (2013). *African Agency in International Politics*. London: Routledge.

Buckley, Peter J., Clegg, Jeremy L., Cross, Adam R., Liu, Xin, Voss, Hinrich & Zheng, Ping (2007). 'The Determinants of Chinese Outward Foreign Direct Investment'. *Journal of International Business Studies*, 38, 499-518.

Clemoes, Charlie (2019, March 6). 'Cities on the New Silk Road: Djibouti City'. *Topos*. Retrieved 20 March 2019 from https://www.toposmagazine.com/cities-on-the-new-silk-road-djibouti/.

Collier, David (2011). 'Understanding Process Tracing'. *Political Science and Politics*, 44(4), 823-830.

Coulthard, Sarah (2012). 'Can We Be Both Resilient and Well, and What Choices Do People Have? Incorporating Agency into the Resilience Debate from a Fisheries Perspective'. *Ecology and Society*, 17(1), 4.

Dutch IT-channel (2014). 'ZTEsoft Introduceert ZSmart Application Programming Interface (API) Beheeroplossing' [ZTEsoft introduces ZSmart Application Programming Interface (API) management solution]. Retrieved 30 April 2020 from https://dutchitchannel.nl/516712/ztesoft-introduceert-zsmart-application-programming-interface-api-beheeroplossing.html.

EDPS (2020). 'Data Protection'. European Data Protection Supervisor. Retrieved 20 March 2020 from https://edps.europa.eu/data-protection/data-protection_en.

Emirbayer, Mustafa & Mische, Ann (1998). What Is Agency? *American Journal of Sociology*, 103(4), 962-1023.

ENA (2019, November 25). 'Ethiopia Launches Electronic World Trade Platform'. Ethiopian News Agency. Retrieved 20 March 2020 from https://www.ena.et/en/?p=10924.

Ethio Telecom (2019). 'Ethio Telecom – ZTE Joint Innovation Center Inaugurated'. Retrieved 7 April 2020 from https://www.ethiotelecom.et/ethio-zte-joint-innovation-center/.

Federal Negarit Gazeta (2012, August). 'Registration of Vital Events and National Identity Card Proclamation'. Federal Democratic Republic of Ethiopia. Retrieved 20 February 2020 from https://chilot.files.wordpress.com/2013/04/proclamation-no-760-2012-registration-of-vital-events-and-national-identity-card-proclamation.pdf.

Fikade, Birhanu (2016, July 2). 'Huawei Takes over Ericsson's Portion of Network Project'. *The Reporter*. Retrieved 13 March 2020 from https://www.thereporterethiopia.com/content/huawei-takes-over-ericsson%E2%80%99s-portion-network-project.

Fourie, Elsje (2015). 'A New Map for Africa? Ethiopian and Kenyan Responses to the "Chinese Model" of Development'. *Afrique contemporaine*, 1(253), 87-103.

Freedom House (2016). 'Financial Statements'. Retrieved 20 March 2020 from https://freedomhouse.org/sites/default/files/FINAL_Basic_Financial_Statements_2016.pdf.

Freedom House (2018). 'Freedom on the Net 2018: The Rise of Digital Authoritarianism'. Retrieved 20 February 2020 from https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

Freedom House (2020a). 'Countries'. Retrieved 20 March 2020 from https://freedomhouse.org/countries/freedom-net/scores?sort=asc&order=Total%20Score%20and%20Status.

Freedom House (2020b). 'Freedom in the World: Ethiopia'. Retrieved 20 March 2020 from https://freedomhouse.org/country/ethiopia/freedom-world/2020.

Gagliardone, Iginio (2014). 'New Media and the Developmental State in Ethiopia'. *African Affairs*, 451, 279-299.

Gebre, Samuel (2019, November 27). 'Ethiopia's Digitization Drive Attracts Global Tech Giants'. *Bloomberg*. Retrieved 9 March 2020 from https://www.bloomberg.com/news/articles/2019-11-27/two-tech-giants-named-jack-are-in-ethiopia-this-week.

GIZ (2017). 'Digital Solutions for Sustainable Development (DSSD)'. Deutsche Gesellschaft für Internationale Zusammenarbeit (German Society for International Cooperation). Retrieved 15 April 2019 from https://www.giz.de/en/worldwide/73176.html.

Goetz, John, Leyendecker, Hans & Obermaier, Frederik (2013, August 28). 'Britischer Geheimdienst zapft Daten aus Deutschland ab' [British secret service taps data from Germany]. *Süddeutsche Zeitung*. Retrieved 3 June 2020 from https://www.sueddeutsche.de/politik/internet-ueberwachung-britischer-geheimdienst-zapft-daten-aus-deutschland-ab-1.1757068.

Hofstede-insights (2020). 'Country Comparison'. Retrieved 11 June 2020 from https://www.hofstede-insights.com/country-comparison/ethiopia,the-netherlands/.

Hirono, Miwa & Suzuki, Shogo (2014). 'Why Do We Need "Myth-Busting" in the Study of Sino-African Relations?' *Journal of Contemporary China*, 23(87), 443-461.

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

Ibeh, Joseph (2019, October 14). 'Ethiopia to Commence Construction of Satellite Manufacturing, AIT Centre'. *Space in Africa*. Retrieved 13 March 2020 from https://africanews.space/ethiopia-to-commence-construction-of-satellite-manufacturing-ait-centre/.

Ibeh, Joseph (2020, March 13). 'Egypt to Launch Two Experimental Satellites Ahead of a Planned NGEO Constellation'. *Space in Africa*. Retrieved 13 March 2020 from https://africanews.space/egypt-to-launch-two-experimental-satellites-ahead-of-a-planned-ngeo-constellation/.

Jeffrey, James (2019, November 16). 'Press Freedom under Siege Again in the New Ethiopia'. *Deutsche Welle*. Retrieved 20 February 2020 from https://www.dw.com/en/press-freedom-under-siege-again-in-the-new-ethiopia/a-51276791.

Kolstad, Ivar & Wiig, Arne (2012). 'What Determines Chinese Outward FDI?' *Journal of World Business*, 47, 26-34.

Lancaster, Henry & Lange, Peter (2020). 'Ethiopia – Telecoms, Mobile and Broadband – Statistics and Analyses'. BuddeComm. Retrieved 19 March 2020 from https://www.budde.com.au/Research/Ethiopia-Telecoms-Mobile-and-Broadband-Statistics-and-Analyses.

Lister, Ruth (2003). *Citizenship: Feminist Perspectives*. 2nd ed. New York: New York University Press.

Lister, Ruth (2004). *Poverty*. Cambridge: Polity.

Locke, John (1978). *Two Treatises of Government*. New York: E.P. Dutton.

Lu, Youqing (2017, May 11). 'Tanzania – the Belt and Road Initiative and China-Tanzania Relations'. *All Africa*. Retrieved 13 March 2020 from https://allafrica.com/stories/201705110195.html.

Maasho, Aaron (2013, August 18). 'Ethiopia Signs $800 Million Mobile Network Deal with China's ZTE'. *Reuters*. Retrieved 9 March 2020 from https://www.reuters.com/article/us-ethiopia-china-telecom/ethiopia-signs-800-million-mobile-network-deal-with-chinas-zte-idUSBRE97H0AZ20130818.

Maasho, Aaron (2015, October 28). 'Ethiopia to Open Bids for Telecoms Expansion in Dec or Jan – CEO'. *Reuters*. Retrieved 19 March 2020 from https://www.reuters.com/article/ethiopia-telecoms/ethiopia-to-open-bids-for-telecoms-expansion-in-dec-or-jan-ceo-idUSL8N12S3U620151028.

Mamabolo, Matshelane (2017, November 27). 'Ethiopia Links up with China's Shenzhen Province to Bolster ICT'. *ITWeb Africa*. Retrieved 20 February 2020 from https://itweb.africa/content/01Jr5Mx9rabqKdWL.

Mbah, Fidelis (2019, June 25). 'Outrage over Ethiopia's Continuing Internet Blackout'. *Al Jazeera*. Retrieved 9 March 2020 from https://www.aljazeera.com/news/2019/06/outrage-ethiopia-continuing-internet-blackout-190625105401629.html.

Ministry of Foreign Affairs of the PRC (2017). *International Strategy of Cooperation on Cyberspace*. Retrieved 11 November 2020 from https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/kjlc_665236/qtwt_665250/t1442390.shtml.

Mella TV (2019, May 25). 'Mella Monthly Episode 19: Betelhem Dessie, CEO of iCog – Anyone Can Code'. Retrieved 20 February 2020 from https://www.youtube.com/watch?v=hdg7EICnyoc.

Mohan, Giles & Lampert, Ben (2012). 'Negotiating China: Reinserting African Agency into China-Africa Relations'. *African Affairs*, 112(446), 92-110.

National Planning Commission (2016, May). 'Growth and Transformation Plan II (GTP II) (2015/16-2019/20): Vol. I: Main Text'. Federal Democratic Republic of Ethiopia. Retrieved 9 March 2020 from https://www.greengrowthknowledge.org/sites/default/files/downloads/policy-database/ETHIOPIA%29%20Growth%20and%20Transformation%20Plan%20II%2C%20Vol%20I.%20%20%282015%2C16-2019%2C20%29.pdf.

NDRC (2015, March). 'Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road'. National Development and Reform Commission, Ministry of Foreign Affairs and Ministry of Commerce, People's Republic of China. Retrieved 25 October 2020 from https://web.archive.org/web/20181127225143/http://en.ndrc.gov.cn/newsrelease/201503/t20150330_669367.html.

Nobel Prize (2019). 'Abiy Ahmed Ali'. Retrieved 3 April 2019 from https://www.nobelprize.org/prizes/peace/2019/abiy/facts/.

NTV Kenya (2018). 'Ethiopia Prime Minister Hailemariam Desalegn Resigns: Says Move Is to Aid Reforms in the Country'. Retrieved 12 January 2020 from https://www.youtube.com/watch?v=fCOuatOOj1g.

Patrick, Stewart P. (2018, July 2). Belt and Router: China Aims for Tighter Internet Controls with Digital Silk Road. *The Internationalist.* Retrieved 9 March 2020 from https://www.cfr.org/blog/belt-and-router-china-aims-tighter-internet-controls-digital-silk-road.

Ramasamy, Bala, Yeung, Matthew & Laforet, Sylvie (2012). 'China's Outward Foreign Direct Investment: Location Choice and Firm Ownership'. *Journal of World Business*, 47(1), 17-25.

Reed, John (2013, August 4). 'Is Tech Firm a Front for China to Spy?' *IOL*. Retrieved 11 April 2019 from http://www.iol.co.za/scitech/technology/security/is-tech-firm-a-front-for-china-to-spy1.1556887#.UvQBwmJ5Pcw.

Reuters (2014, December 11). 'Ethiopia Says Ericsson to Take Part of Telecom Deal after ZTE Row'. *Reuters*. Retrieved 19 May 2020 from https://www.reuters.com/article/ethiopia-telecomunications/ethiopia-says-ericsson-to-take-part-of-telecom-deal-after-zte-row-idUSL6N0TV2KO20141211.

Reuters (2019, December 20). 'Ethiopia Launches First Satellite into Space'. *Reuters*. Retrieved 9 March 2020 from https://www.reuters.com/article/us-ethiopia-satellite/ethiopia-launches-first-satellite-into-space-idUSKBN1YO0IU.

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

SOA (n.d.). 'Africa Branch of Shenzhen Outbound Alliance'. Shenzhen Outbound Alliance. Retrieved 20 March 2020 from http://www.szsoa.org/html/1/156/168/index.html.

Space in Africa (2019a, May 28). 'Ethiopia Signs Communications Satellite Development Agreement with China'. *Space in Africa*. Retrieved 9 March 2020 from https://africanews.space/ethiopia-signs-communication-satellite-development-agreement-with-china/.

Space in Africa (2019b, August 23). 'Ethiopian Space Science and Technology Institute Director General Sheds Light on Ethiopia's Direction In Space Strategy'. *Space in Africa*. Retrieved 20 March 2020 from https://africanews.space/ethiopian-space-science-and-technology-institute-director-general-sheds-light-on-ethiopias-direction-in-space-strategy/.

Spacewatch Africa (2019, October). 'Ethiopia to Begin Work on Satellite MAIT Facility with European Funding'. *Spacewatch Africa*. Retrieved 20 March 2020 from https://spacewatch.global/2019/10/ethiopia-to-begin-work-on-satellite-mait-facility-with-european-funding/.

Taye, Berhan & Teshome, Roman (2018, September). 'Privacy and Personal Data Protection in Ethiopia'. Collaboration on International ICT Policy in East and Southern Africa (CIPESA). Retrieved 20 March 2020 from https://cipesa.org/?wpfb_dl=301.

Taylor, Ian & Xiao, Yuhua (2009). 'A Case of Mistaken Identity: "China Inc." and Its "Imperialism" in Sub-Saharan Africa'. *Asian Politics & Policy*, 1(4), 709-725.

Walton, Greg (2001). *China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China.* Montreal: International Centre for Human Rights and Democratic Development.

Woodhams, Samuel (2020, March 20). 'Huawei Says Its Surveillance Tech Will Keep African Cities Safe but Activists Worry It'll Be Misused'. *Quartz Africa*. Retrieved 20 March 2020 from https://qz.com/africa/1822312/huaweis-surveillance-tech-in-africa-worries-activists/.

Wuilbercq, Emeline (2015 November 19). 'Des geeks éthiopiens veulent fabriquer les robots de demain' [Ethiopian geeks want to build the robots of tomorrow]. *Le Monde*. Retrieved 19 May 2020 from https://www.lemonde.fr/afrique/article/2015/11/19/des-geeks-ethiopiens-veulent-fabriquer-les-robots-de-demain_4813340_3212.html.

ZTE (n.d.). 'ZTE Build a High-Tech National Public Safety System for Ethiopia'. Retrieved 20 February 2020 from https://usa.ingrammicro.com/media/Documents/vendors/z/zte/docs/zte_build_a_high_tech_national_public_safety.pdf.

About the Author

Dr. Sanne van der Lugt is an Associate Fellow with LeidenAsiaCentre and Clingendael Institute. Her research is aimed at the consequences of China's re-emergence as a global power for Europe, with a special focus on China's economic activities in Africa and China's position in the fourth industrial revolution. Prior to joining the LeidenAsiaCentre she worked for (among others) the Centre for Chinese Studies at Stellenbosch University and Profundo, a Dutch not-for-profit research centre on sustainability. She conducted fieldwork in various African countries for projects commissioned by Oxfam, the WWF, and the European Commission regarding the social and environmental impacts of Chinese investments.