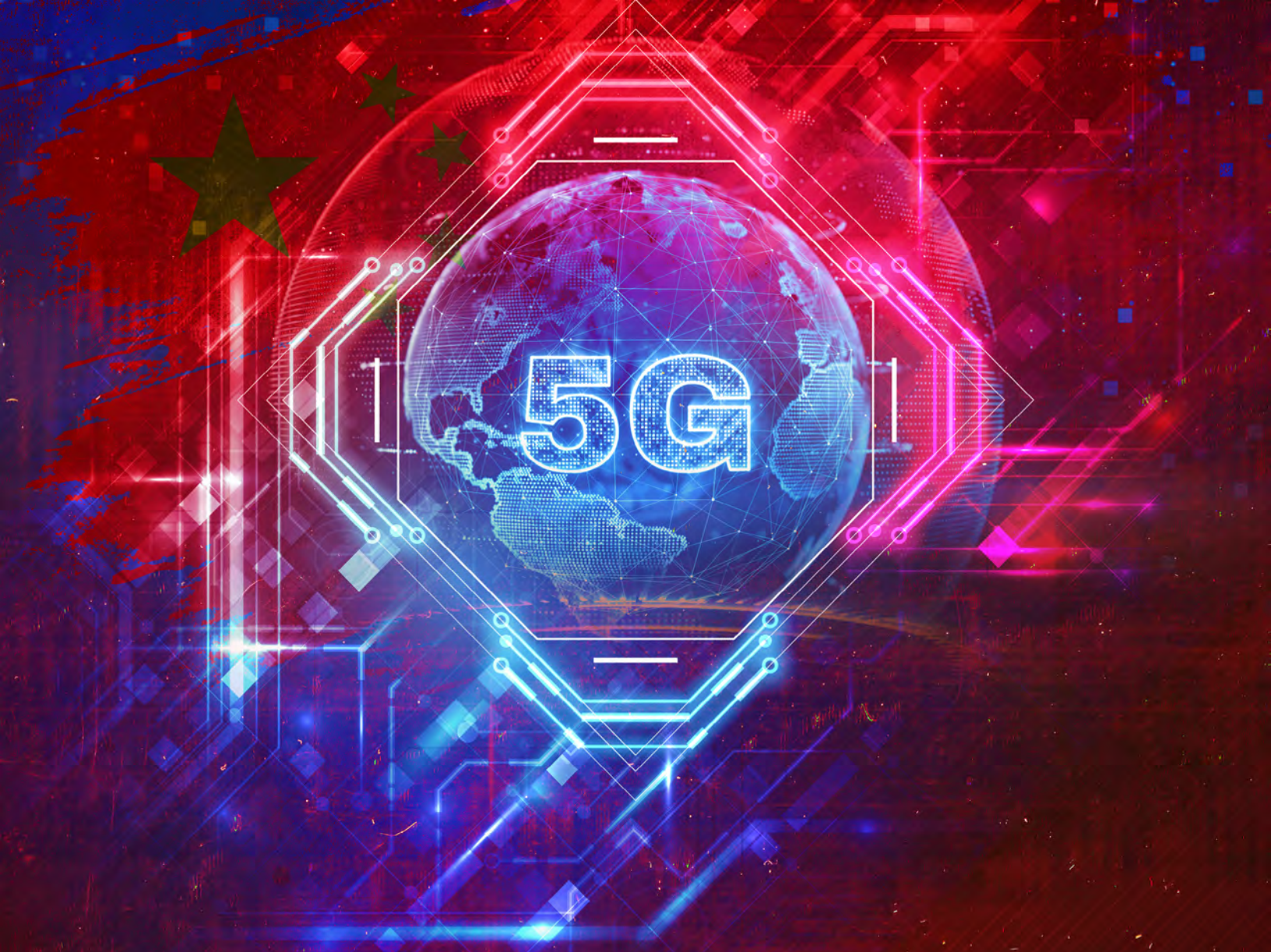


China and the Digital Information Stack in the Global South

By Bryce Barros, Nathan Kohlenberg, and Etienne Soula

JUNE 2022

Ed. Kristine Berzina

alliance for securing democracy
G|M|F

Cover and graphics designed by Kenny Nguyen

Please direct inquiries to
The Alliance for Securing Democracy at
The German Marshall Fund of the United States
1700 18th Street, NW Washington, DC 20009
T 1 202 683 2650
E info@securingdemocracy.org

This publication can be downloaded for free at https://securingdemocracy.gmfus.org/china-digital-stack.

Alliance for Securing Democracy

The Alliance for Securing Democracy (ASD), a nonpartisan initiative housed at the German Marshall Fund of the United States, develops comprehensive strategies to deter, defend against, and raise the costs on autocratic efforts to undermine and interfere in democratic institutions. ASD has staff in Washington, D.C., and Brussels, bringing together experts on disinformation, malign finance, emerging technologies, elections integrity, economic coercion, and cybersecurity, as well as Russia, China, and the Middle East, to collaborate across traditional stovepipes and develop cross-cutting frameworks.

International Republican Institute's Countering Foreign Authoritarian Influence Practice

Over the past four years, the International Republican Institute (IRI) has developed and implemented a framework to build resiliency against growing foreign authoritarian influence and interference through its Countering Foreign Authoritarian Influence (CFAI) practice. IRI's CFAI work uses a three-pronged approach to mitigate the impact of authoritarian influence on developing democracies: 1. Researching malign actors such as the Chinese Communist Party (CCP) and the Kremlin and their impact on vulnerable democracies; 2. Sharing that research through tailored engagements with IRI's global network of partners on the ground; 3. Equipping these stakeholders with tools and resources to bolster democratic resilience to foreign authoritarian influence. By engaging stakeholders across sectors—including government officials, political parties, media, private enterprise, and civil society activists—IRI's work promotes broad awareness of authoritarian tactics and the keys to shoring up vulnerable democratic institutions.

About the Report

This report is the result of a collaboration between ASD and the International Republican Institute's CFAI initiative. Leveraging ASD's research tools and IRI's and ASD's expertise documenting the Chinese Communist Party's (CCP) varied authoritarian influence tactics across countries, the report assesses how the CCP manipulates the information environment to advance its strategic goals. The research presented in this report is part of a growing compendium of case studies on CCP influence and the elements of effective democratic resilience, which directly informs IRI's CFAI programming. We are grateful to the National Endowment for Democracy for its ongoing sponsorship of this report.

Map

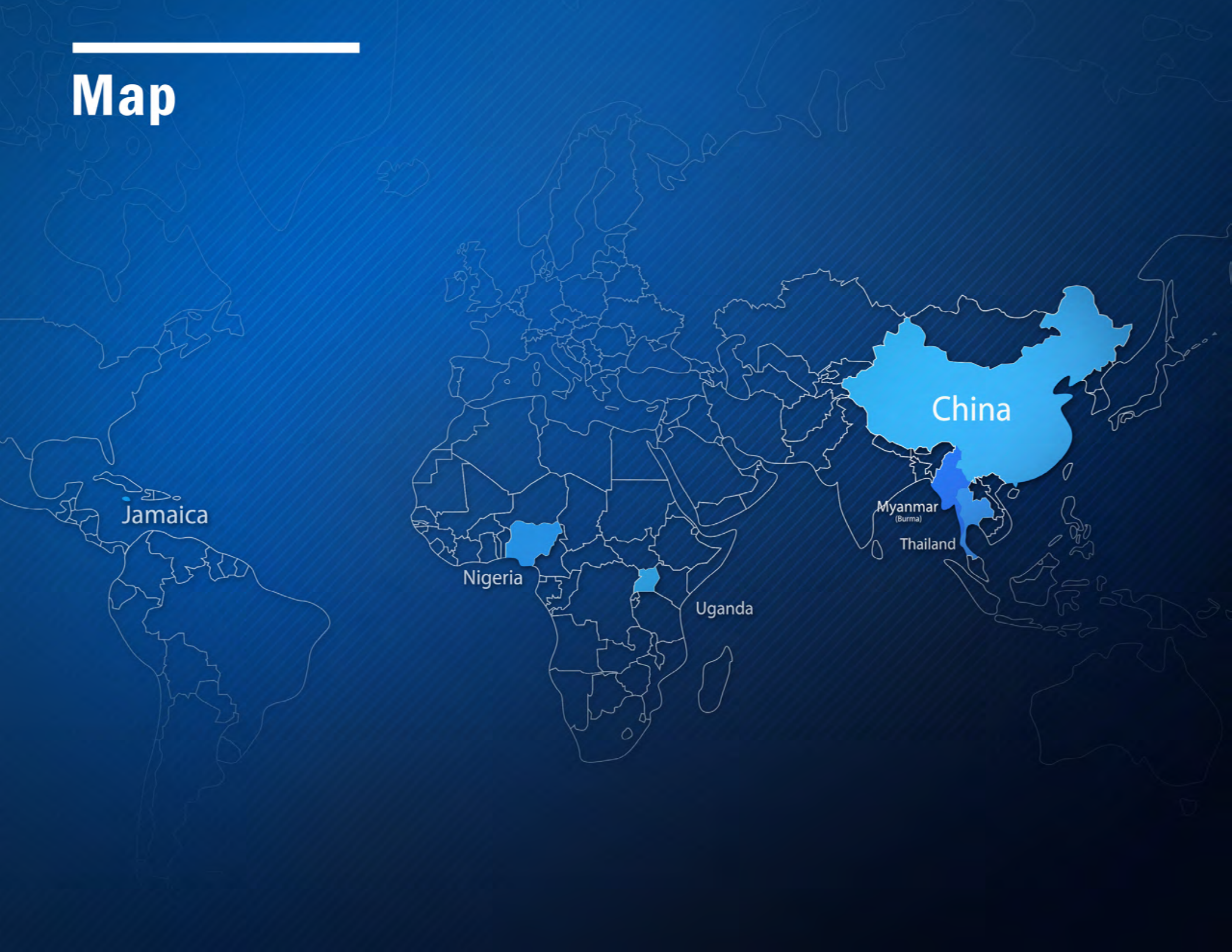


Table of Contents

Introduction 4
The Stack: An Overview 5
The PRC Party-State and the Stack 13
Case Studies and Recommendations 19
- Thailand 24
- Myanmar 32
- Uganda 40
- Nigeria 46
- Jamaica 52

About the Authors 56
Acknowledgements 57
Endnotes 58

Introduction

The 21st Century started with the promise of how technologies can be used to bolster, not undermine, democracies, activism, and human rights. However, the maddening pace at which digital technologies have evolved in recent years means that authoritarians around the world are quickly learning new ways to use telecommunications infrastructure, electronic devices, software applications, information content, and policies and international fora for governing these technologies to suppress advocates for liberal democracy around the world. Among authoritarian regimes pioneering the use of emerging technologies to push back against liberal democracy, the People's Republic of China (PRC) stands out for its aggression in repurposing digital technologies and infrastructure to enable the suppression of civil society.

This collaborative report between the German Marshall Fund of the United States' (GMF) Alliance for Securing Democracy (ASD) program and the International Republican Institute (IRI) examines the diverse ways that the PRC party-state uses its digital information operations to advance its strategic goal of making the world less hospitable for democracy and more welcoming for autocracy. To do so, this report will examine the full digital information "stack" and how the PRC party-state uses it to achieve those goals. Next, this report will provide an overview of the PRC party-state, its digital information environment, and finally, provide five case studies of countries affected by these policies: Thailand, Myanmar, Uganda, Nigeria, and Jamaica. Through a better understanding of the stack, the PRC party-state, and related case studies, this report seeks to illuminate the different ways countries in the Global South can be susceptible to China's influence on the digital information stack.

This report seeks to fill that gap and be a reference for those seeking to push back against the PRC party-state and its autocratic partners. To bolster digital democracy and counter digital authoritarianism, civil society must learn how the PRC party-state uses its influence to shape, influence, control, surveil, and suppress information that is contrary to the PRC and Chinese Communist Party's (CCP) goals or critical of those institutions or other autocrats.

The Stack: An Overview

Digital information ecosystems depend on the digital information stack, which comprises a full suite of five layers and their components bridging the physical and virtual worlds. For this overview, ASD and IRI define the digital information stack as consisting of five distinct, yet mutually reinforcing, layers: network infrastructure, devices, applications, content, and governance. The stack encompasses the technologies, software, hardware, governance standards, and protocols required to control and influence the digital information ecosystem.

Background

This formulation of the five layers of the digital stack is based upon the work of ASD Emerging Technology Fellow Lindsay Gorman, as well as Dr. Samantha Hoffman and Dr. Nathan Attrill of the Australian Strategic Policy Institute. According to Gorman, the stack includes layers for infrastructure, applications, and governance.[1] Dr. Hoffman and Dr. Attrill have divided the stack into four groupings: software applications, storage and software infrastructure, hardware, and carrier infrastructure.[2] ASD and IRI determined the five-layered framework of the stack as defined by this report—network infrastructure, devices, applications, content, and governance—to highlight how China's digital information operations extend beyond devices, applications, and content into intercontinental infrastructure and international technology governance broadly.

The PRC government, and its publicly owned companies, China-registered private companies, and other entities affiliated with the government and the CCP have deployed an integrated approach to dominating the stack. Managing the stack's layers, and the full suite of components that it encompasses, facilitates China's dominance of digital information ecosystems, thus enabling leaders with authoritarian tendencies as well as autocrats the world over to threaten basic human rights.[3]

Digital Information Stack

LAYERS	COMPONENTS
Network Infrastructure	· Digital Silk Road · Submarine/Undersea Cables · Terrestrial Cables · Telecommunications Equipment - Mobile Phone Towers · Data Centers · Cloud Centers
Devices	· Mobile Phones · Tablets · Laptops · Routers · Other “Smart” Internet of Things Devices
Applications	· Social Media Platforms · Software · Digital Payment Platforms · Cloud Services
Content	· Messages · Narratives · “Wolf Warrior“ Diplomacy
Governance	· Proliferation of China’s Cyber Rules, Regulations, and Laws · Technology Standards · Artificial Intelligence · International Organizations · Traineeships/Internships and Talent Cultivation Study Tours

The Network Infrastructure Layer

The network infrastructure layer is key to the control of digital information ecosystems and includes (but is not limited to) satellites, undersea cables, telecommunications equipment, data centers, and other hard infrastructure components that enable China's digital information operations. In addition to these hard infrastructure components, the network infrastructure layer includes the Management Service Provider that maintains those components.[4] If PRC-based companies monopolize the initial build of network infrastructure or the maintenance and upgrade of existing infrastructure, this has the potential to enable autocratic tendencies in the country where this is done if left unchecked.

The Digital Silk Road is a particularly important part of the PRC's efforts to influence this portion of the digital stack. According to the RWR Advisory Group, the total investment in the Belt and Road Initiative's (BRI) Digital Silk Road (DSR) figure is estimated to be US$79 billion, much of which includes network infrastructure-related projects.[5] This initiative focuses on investing in and financing infrastructure related to telecommunications networks and other high-tech areas in recipient countries around the world and supports Chinese companies exporting their telecommunications equipment.[6] Although DSR mostly includes Memoranda of Understanding (MOU) between Chinese public and private companies with telecommunication counterparts and foreign government clientele, other tools such as donations, loans, and sales also fit into its strategy.[7] This is especially noticeable in Africa, where China provides more financing for information and communication technology infrastructure than all democracies and international organizations combined.[8] For example, since 2006 when Huawei signed a US$106 million deal with the Ugandan government to build the country's ICT background infrastructure, Chinese telecommunication companies have maintained a major presence in Uganda, including ZTE's work on Uganda's network infrastructure development.[9]

DSR has been made a foreign policy priority by Chinese leaders, who have promoted the concept at international fora, including the Belt and Road Forum and the fifth World Internet Conference.[10] Projects like China Mobile's Southeast Asia-Japan 2 cable slated for completion in Thailand in 2022 are openly advertised as contributing to BRI.[11] Chinese state-owned and private companies working under the initiative have mostly focused on providing more digital infrastructure, telecommunication carrier services, smart cities, cloud services, and data centers to host countries. Although there are growing negative perceptions of the initiative, many countries are still open to Chinese telecommunication companies providing digital connectivity solutions not offered by counterparts from democracies.[12]

In addition, major Chinese state-owned and private companies like Alibaba, Tencent, China Telecom, Huawei, and Baidu provide cloud centers, the physical infrastructure that hosts cloud services. For example, according to Synergy Research Group, in 2020 Alibaba made up 5 percent of the global cloud market and Tencent made up 2 percent.[13] Cloud centers are a critical component of the network infrastructure layer because they provide the physical infrastructure that artificial intelligence and big data rely on, and in turn, that the societies and governments of many countries require for all aspects of daily life.[14] Of particular concern to the authors of this report is the potential that this infrastructure be used as a foundation for increased surveillance. For instance, a news story announcing the launch of Tencent's latest data center in Bangkok explains that it would support "all ranges of intelligent solutions […] including artificial intelligence [and] facial recognition."[15]

Reasons for countries to use Chinese infrastructure vary. The leaders of some countries desire an affordable infrastructure alternative to the expensive equipment produced by the telecommunications companies of the world's leading democracies, while others may wish to clamp down on domestic opposition, and some wish to replicate China's domestic cyberspace regulations. Regardless of the motivation, there is the potential for host governments to restrict democracy through the telecommunication equipment built and installed by Chinese state-owned and private companies. If used improperly, these network infrastructure projects could enable the leaders of those countries to use their citizens' data in nefarious ways. Understanding the network infrastructure layer in a holistic manner is key for democracy organizations and political opposition leaders around the world combating China's digital information operations or their home governments' efforts to emulate them.

The Device Layer

The device layer refers to the physical devices used by individuals or institutions to access the internet—including mobile phones, tablets, computers, and personal devices like smartwatches—as well as devices comprising the so-called "internet of things" (IoT). The IoT also includes sensors and devices that are components of larger integrated device layer concepts like smart cities.[16] According to Oracle, the suite is defined as, "The network of physical objects—"things"—that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the internet."[17] Reinforcing Oracle's definition of the IoT, IBM defines it as:

> In a nutshell, the Internet of Things is the concept of connecting any device (so long as it has an on/off switch) to the Internet and other connected devices. The IoT is a giant network of connected things and people – all of which collect and share data about the way they are used and about the environment around them.[18]

These IoT devices collectively provide the infrastructure required of concepts like smart cities, which the technology professional association TWI explains as follows: "A smart city uses information and communication technology (ICT) to improve operational efficiency, share information with the public and provide a better quality of government service and citizen welfare."[19]

The IoT allows for physical items like personal devices to "share and collect data with minimal human intervention." The suite includes everything from smart microwaves to self-driving cars to wearable fitness devices to even sports equipment and balls, which can become more efficient and precise.[20] For China, the IoT provides an opportunity to integrate with critical infrastructure like electricity, water, and emergency services, which could be misused by Chinese telecommunication firms. Smart cities seek to optimize the functions of day-to-day life in urban municipalities by using the data gathered from the IoT to make governance more efficient, which in turn promotes economic growth and quality of life for residents.[21]

The device layer also includes industrial control systems (ICS) used to manage sophisticated manufacturing and resource extraction operations. As industries like oil and minerals have becoming more technologically demanding, many states, including Nigeria and Uganda, have invested in industrial hardware produced by Huawei or other Chinese firms in the hopes of improving productivity. Such tools can yield dividends but can also be used to make firms in lower development countries more dependent on Chinese expertise, maintenance, and support to continue their operations, giving Chinese firms a direct point of leverage over major industries in other countries.

For many countries in the Global South, Chinese brands like Xiaomi, Huawei, and others are commonplace because of their affordability when compared with brands like Sony, Samsung, Apple, etc.[22] The dominance of Chinese mobile brands in the Global South provides the PRC government potential backdoors to siphon off data, influence which applications and software can be installed, and therefore influence which digital information is consumed by the user.[23] Additionally, devices that are not produced by Chinese mobile brands can also be targeted by attempts to collect data via spyware.[24]

The dominance of these brands can be potentially problematic for a country's democracy. An agency at the Lithuanian Defense Ministry warned in August 2021 that Huawei and Xiaomi phones posed "cybersecurity risks" and that Xiaomi phones, in particular, had dormant censorship functionalities.[25] In some countries, at least, the population is aware of the risks associated with Chinese handsets. In Myanmar, as citizens sought to escape the junta's repression in the aftermath of the February 2021 coup, Apple sales significantly gained ground vis-à-vis their Chinese competitors.[26]

To amplify the reach of the device layer, China has used the donation of devices not only to promote its goodwill globally but to promote content that favors its geostrategic goals.[2728] For example, Chinese SOE China Electronics Technology Taiji Group Company Limited donated 10 computers for the University of Zambia to help the Zambian government "embrace digital transformation."[29] And by January 2021, Huawei had donated a total of 6,500 electronic devices to the Jamaican government Ministry of Education in addition 300 tablets donated to the University of the West Indies and University of Technology, Jamaica.[30] These examples show how the PRC government works with state-owned and private companies alike to provide device donations that build strong relationships, which in turn can be capitalized on later. Several of the case studies examined in this report discuss how the donations of various electronic devices have become a key component to China's digital information stack and thus the ability to control the flows of information.

The Application Layer

The application layer encompasses social media platforms like TikTok and WeChat, as well as the software that manages big data suite services and IoT components. WeChat and TikTok are currently the Chinese apps most successful outside of China but present slightly different challenges. WeChat is China's "super-app," as it is ubiquitous inside China and is nearly essential for anyone looking to communicate with people behind the Great Firewall. This means that communities like Thailand's significant Chinese diaspora or the many Myanmar traders who conduct business with Chinese partners are de facto reliant on an app that is explicitly subject to the CCP's drastic information control within China. On the other hand, the app has limited appeal and growth potential outside of those communities.

TikTok is in a different position. Although the app's ultimate owner is Beijing-based ByteDance, TikTok is not available in China and, as such, claims not to be subjected to the CCP's censorship regime. However, the Chinese state is one of ByteDance's shareholders and several media reports document TikTok's history of enforcing the CCP's censorship policies.[31] In addition, TikTok has a record of being slow to rein in authoritarian disinformation on its platform. For instance, in Myanmar, at the height of anti-coup protests in February 2021, the military was able to use the platform to circumvent its ban from Facebook and threaten protesters.[32] Most recently, TikTok has failed to rein in Russian state media's disinformation related to the war in Ukraine, despite the company's own policies.[33] The app's meteoric rise around the world, most notably with young users, should be a cause for concern. In countries like Thailand, where the app is already so popular that both civil society and government

see it as a key venue for winning over public opinion, TikTok's track record suggests that it is not on pro-democracy activists' side. Globally, it is an application with a huge and growing presence. Cloud services also fall in the application layer. Cloud services provided by Chinese telecommunication companies host software for clients' networks as well as virtual storage services and file management.[34]

Moreover, Chinese payment providers Alipay, WeChat Pay, and others (which are owned by companies that are also involved in cloud services e.g. Alibaba, Tencent, etc.) are gaining more prominence globally within e-pay and financial technology markets as Chinese tourism and the presence of Chinese companies grows.[35] The growing market share of Chinese e-payment apps in Thailand—or in pre-coup Myanmar—is another avenue through which the Chinese state could potentially surveil users. Chinese investment mechanisms like DSR also could lead to an increase of e-pay platforms. Digital payment platforms and other financial technology applications are one of the fastest-growing areas of the application layer.

The Content Layer

The content layer consists of the messages and narratives that are promoted by the PRC government, CCP, and state-affiliated and state-backed media to burnish the image of China globally while silencing democratic voices that critique the PRC party-state. In recent years, social media platforms, especially Twitter, have become the go-to platform for Chinese diplomats to utilize "wolf warrior" diplomacy to aggressively defend China on the world stage through confrontational rhetoric.[36] The phrase "wolf warrior" refers to a jingoist blockbuster Chinese film franchise that features a protagonist defending Chinese nationals in an unnamed African nation.[37] Echoing the tagline of the film—"whoever attacks China will be killed no matter how far the target is [犯我中华者虽远必诛]"—Chinese wolf warrior diplomats use Twitter to berate critics of China and the Party, promote conspiracy theories, deepen social cleavages by highlighting controversial and sensitive topics, and leverage the networks and messages of other autocrats with whom there is a common interest.[38] Chinese state-affiliated and state-backed media outlets, officials, and personalities amplify the messages and narratives of wolf warrior diplomats.

Through the Hamilton 2.0 Dashboard, ASD tracks these wolf warrior diplomatic narratives and other content that is promoted abroad by the PRC government and party officials as well as state-affiliated and state-backed media outlets. These narratives and messages are wide in scope and include criticizing democracies and democratically elected officials that seek deeper engagement with Taiwan (e.g. the fallout from blossoming Lithuania-Taiwan relations); promoting the belief in the superiority of the CCP's definition of democracy (i.e. the "people's democracy" of Marxism-Leninism); degrading attempts to promote democracy (pushback against the U.S. Summit for Democracy); berating foreign governments and private citizens that seek to critique the actions of the PRC government and the Party as well as its officials (e.g. Chinese tennis star Peng Shuai's sexual harassment allegations); and nourishing anti-Americanism globally with other autocracies. For instance, during the December 2021 U.S. Summit for Democracy, the PRC was actively promoting its own definition of "democracy."[39]

Chinese influence in the content layer is not always so transparent. In Nigeria, China has sought to use the country's developed media industry as a foothold from which to spread pro-CCP narratives across Anglophone Africa. By providing news and entertainment content focused on an African audience, the CCP leverages a genuine market demand to assertively push its own narrative and worldview through films, TV, and news programming aimed at improving China's image, discouraging democratic reform, and other global priorities.

The Governance Layer

Lastly, the governance layer of the stack provides China with a tool to carry out its repression and influence abroad by shaping global technology governance to be more hospitable to its authoritarian digital model. Unfortunately, the United States and like-minded democracies are struggling to produce a regulatory framework that balances freedom of expression with security and data privacy concerns. By contrast, authoritarian states like China see the lack of common policies to protect security and data privacy concerns as an opportunity to find new ways to exploit data to preserve their own political stability domestically while exporting their regulatory frameworks to other authoritarians abroad.[40]

China's impact on the governance of digital information ecosystems has manifested in four major ways:

- First, countries around the world, including the majority of those studied in this report, draw inspiration from China's digital norms and governance model.
- Second, the promotion of technology standards in 5G and now 6G is most significant because of the advantage it provides to Chinese state-owned and private companies in the other layers of the digital information stack.
- Third, China's co-opting of international organizations like the United Nations' International Telecommunication Union (ITU) has the goal of reshaping internet governance to encourage other countries to heed their example concerning cyberspace and internet sovereignty.
- Lastly, China's influence on the governance layer has extended to training public security personnel in other countries across the world, tying in elements of surveillance and other nefarious activities.

First, countries around the world draw inspiration from China's digital norms and governance model. This ranges from Nigerian officials seeking an internet firewall like China's to Senegal (one of the most successful liberal democracies in Francophone Africa) modeling its "digital sovereignty" initiative on China's laws.[41] In the case of Nigeria, local officials reached out to the Cyberspace Administration of China to learn best practices for the creation of an international firewall that will provide the government control over citizens' access to Western social media platforms like Facebook, Twitter, and Instagram.[42] In Jamaica, following China's governance lessons, Jamaican government officials have expressed interest in learning from Huawei how to improve government efficiency, fight crime, and maintain public order.[43] In both Thailand and Myanmar, autocratic governments have passed cybersecurity legislation reminiscent of "the vague and broad nature of China's 2017 cybersecurity law."[44] Beyond legislative convergence, in Myanmar, media reports suggest that, in February 2021, Beijing provided "technical assistance so the Burmese military can develop a cyber firewall similar to the Great Firewall."[45] China's complete control over its own digital information stack ecosystem is leading governments around the world to try their best to emulate its laws and overall approach towards cyberspace sovereignty.[46]

Second, the promotion of technology standards helps influence the digital information stack. Through the promotion of technology standards, especially in 5G and now 6G, Chinese state-owned and private companies can influence the other layers of the digital information stack. In the wrong hands, this would allow portions of all layers involved in the digital information stack to enable surveillance technology and permit police forces and other domestic security forces to spy on political opponents or suppress human rights and civil liberties more broadly.[47] This is especially pernicious given the importance that global technology standards play in ensuring that electronic components across the world are affordable, interoperable, and easily traded globally. The affordability of many products produced by Chinese companies involved in the digital information stack can further enable suppression in countries that already lack strong civil liberty regimes.

Third, the PRC party-state's co-opting of international organizations reshapes internet governance to have other countries heed their example with respect to cyberspace and internet sovereignty. Chinese private telecommunications company Huawei has introduced 2,000 technology standards to the ITU, which, if enacted, would pave the way for a splinternet (two internets, one for liberal democracies, and another for autocrats) and allow for authoritarians around the world to "undermine the norms, predictability, and security of today's cyberspace" by limiting human rights online.[48]

The ITU study group ITU-T SG13 spearheaded by Huawei and other Chinese stakeholders seeks to "cast[..] aside the existing Internet architecture."[49] Through such avenues, China is advancing a multilateralist (as opposed to multi-stakeholder) approach to internet governance, which elevates the power of national governments over other potential stakeholders and enshrines strict control by national governments over the flow of information within their borders.[50] By contrast, the diverse array of stakeholders in the multi-stakeholder approach includes civil society entities, diluting the influence of the PRC and other national governments, as well as state-backed telecommunication companies.[51] In addition, the work of Huawei in the multilateral ITU study group undermines the work being done at multi-stakeholder standards bodies like the Internet Engineering Task Force (IETF) by duplicating their efforts.[52] Huawei's behavior within these bodies may be a result of its close association with the PRC party-state and could reflect a willingness to act as a proxy for political and ideological priorities in ways that the private sector in democratic countries, which has traditionally played a leading role in such standards-setting bodies, do not.[53]

Lastly, China's influence on the governance layer has extended to training public security personnel in other countries across the world. These training opportunities not only support local governments to suppress their citizens' rights but also can silence opposition to China's geostrategic goals, including the silencing of support for Taiwan.[54] In the Solomon Islands, riots broke out in late 2021 after several years of tension over Prime Minister Manasseh Sogavare's announcement of the establishment diplomatic relations with China in 2019, along with other domestic issues.[55] Prime Minister Sogavare's ties with China have culminated with a possible security pact between China and the Solomon Islands.[56] Beyond police training, China has also sought to influence ICT students through traineeships, internships, and other study tours that introduce the practices of Chinese companies like Huawei.[57]

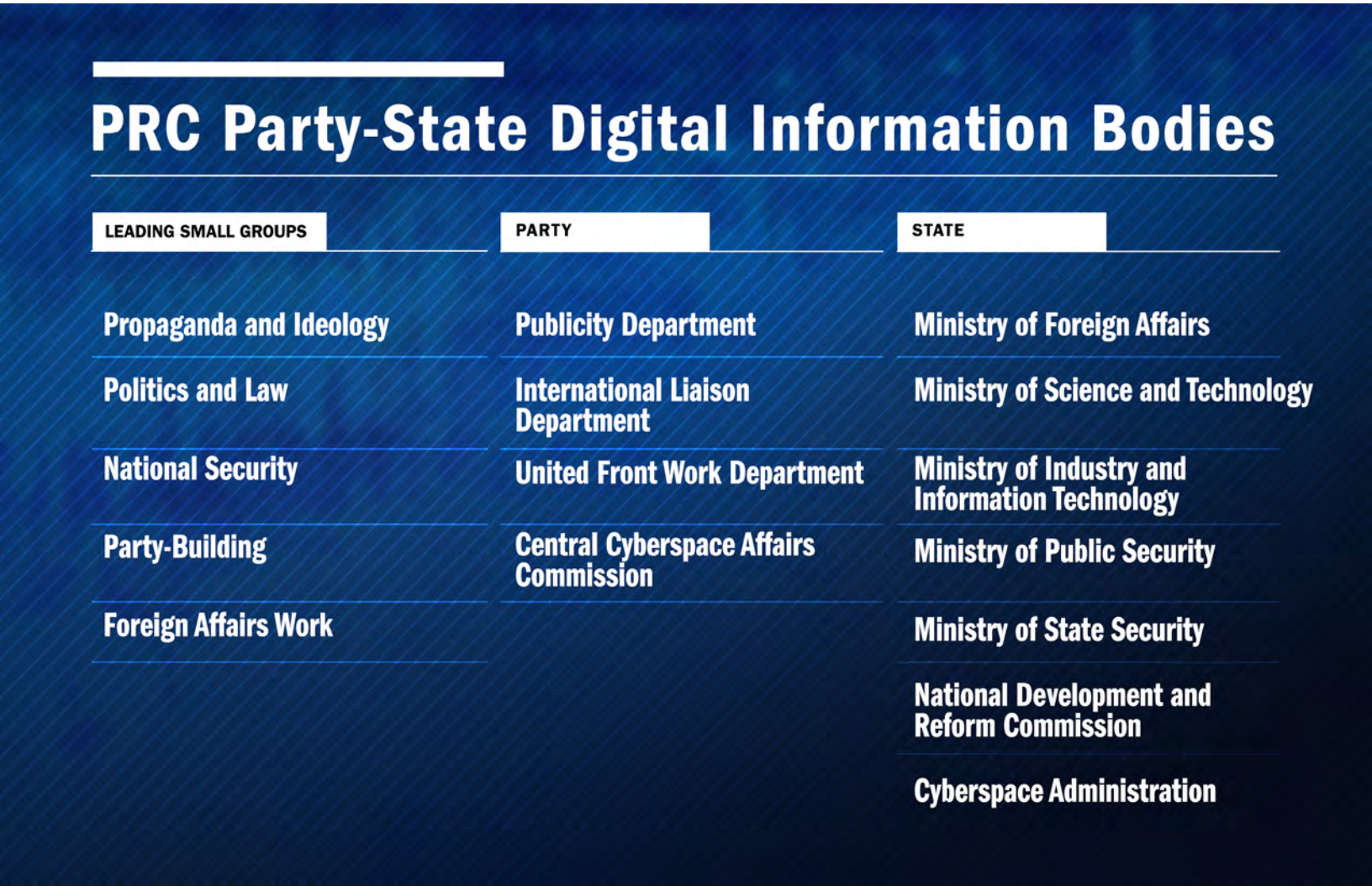
The PRC Party-State and the Stack

PRC Party-State Breakdown

To understand Chinese digital information operations and the digital information stack, one must grasp the nature of the government of the PRC, the CCP, and the differences and overlaps between the two. The party is in command and directs the state. The PRC government is an instrument for the realization of the CCP's goals.

State institutions are central to digital information control, but they are subservient to the party. The party uses ad hoc Leading Small Groups to guide state and party organs that work on a topic area.[58] Groups like Propaganda & Ideology, Politics & Law, and others lead the party's digital information stack policies.[59] Party organs like the Publicity Department, International Liaison Department, United Front Work Department, and the Central Cyberspace Affairs Commission provide more digital information stack guidance.[60] The State Council is responsible for the ministries and commissions that touch on the digital information stack, including the Ministries of Foreign Affairs, Science and Technology, Industry and Information Technology, Public Security, and State Security as well as the National Development and Reform Commission and Party-State hybrid body that the Cyberspace Administration of China.[6162]

Although the party and state are two distinct entities, the party's Leading Small Groups provide the policy and bureaucratic coordination that the state's ministries and other organs require to carry on their work.



Industry and the PRC Party-State

Due to the party's supremacy over everything in the PRC, including the state and the legal system, it is almost impossible for industry to protect itself other than by having ties to the party or the officials of companies to be party members themselves. The importance of the party ensures that companies in China do not act independently from either the party or state in the same way that they would in free-market economies. Both the party and the state require that companies follow their guidance in separate ways, regardless of their ownership. In the case of state-owned companies, the PRC government wholly or partially owns these firms, which can be directed at the discretion of the State Council's State-owned Assets Supervision and Administration Commission (SASAC) and other relevant government organs.[63] For example, major Chinese state-owned companies involved in digital information operations owned by SASAC include China Telecommunications Corporation, China Unicom, and Datang Telecom Group.[64]

Conversely, Chinese private companies like Huawei, Xiaomi, and Lenovo, which are also deeply influential throughout the digital stack, are influenced by the PRC party-state through party cadres at every level of their corporate structures, to ensure they understand, comply with, and promote the party's policy priorities.[65] The relationship between the Chinese government, the party, and private companies is not always harmonious. Legal, regulatory, and financial mechanisms not used with state-owned companies have been used to gain compliance from private companies. This is exemplified by the disputes the party had with the founder and owner of the Chinese e-commerce giant Alibaba Group, Jack Ma, who was the richest man in China until last year.[66] In another instance, Chinese regulators clamped down on the Chinese ride-share company Didi for mishandling sensitive data about users in China.[67]

Regardless of whether a company has public or private ownership, the 2017 National Intelligence Law requires "all organizations and citizens shall support, assist, and cooperate with national intelligence efforts."[68] According to this law, state-owned and private companies alike must assist the Chinese government in intelligence collection when compelled to.[69] This is especially relevant for Huawei, for reasons explained more in the next section.[70] This means that Chinese companies, regardless of ownership, should not be considered equivalent to private companies based in democratic countries.

Export of the Chinese Digital Information Stack

The BRI and, previously, the "Going Out" strategy have served as the two key vectors to enable the export of technologies that are produced by state-owned and private companies under the guidance and policies of the PRC government and the party's doctrine. China announced the Going Out Strategy in 2001, in conjunction with its ascension to the World Trade Organization, to direct outward foreign direct investment and fuel China's rise economically.[71] President Xi announced the BRI in 2013 based on the idea of reinvigorating old land and maritime trade routes to tie China with the rest of Eurasia for geo-economic and strategic reasons.[72]

Within the BRI umbrella, the DSR explicitly bolsters China's engagement in all layers of the digital information stack.[73] This initiative supports companies like Huawei by providing aid and political support to host countries seeking to improve technology including telecommunications, cloud computing, artificial intelligence, surveillance technology, and other components used in the digital information stack.[74] DSR in many cases improved host countries' abilities to surveil domestic political opposition groups, monitor and censor the internet, and use data servers hosted by Chinese state-owned and private companies, both of which require data to be saved back in the PRC.[75]

In addition, Chinese companies involved in the digital information stack are often supported directly by the PRC party-state by other means. For example, in 2019, Huawei announced plans to raise US$1.5 billion from Chinese banks, state-owned and private, to finance its activities within the Chinese market and abroad.[76] This marks the first time that the company did not seek foreign funding due to U.S. trade controls and shows how the U.S. sanctions and export controls regime on Huawei has made the company more reliant on PRC party-state. In other instances, the clients of Huawei and other telecommunication companies have received funding from Chinese state-owned financial institutions. For example, the Wall Street Journal reported in December 2019 that according to annual reports since 2008, Huawei has received more than US$75 billion in financial assistance from the Chinese government through "tax savings, state credit facilities, land purchases, and government grants."[77] Lastly, it is common for PRC diplomatic missions abroad to support Chinese telecommunication companies like Huawei either through informal lobbying, device donations, promoting training programs, or speaking at events hosted by telecommunication companies.[78]

China's Foreign Policy Ambitions

The suite of China's geo-economic programs—BRI, the Going Out Strategy, and the DSR—fit into wider Chinese foreign policy goals of providing a secure environment at home and abroad for the leadership of the PRC party-state.[79] The party fears a collapse like that of the Soviet Union.[80] Thus, China's leaders have invested a large amount of domestic and foreign policy credibility into ensuring that China's economic growth does not produce alternative domestic power centers that could challenge the party's dominant political position. Controlling economic growth and encouraging state-owned and private companies to engage in business abroad not only meet the original intention of the Going Out Strategy by providing more opportunities for those firms to generate revenue to ensure regime stability domestically, but also offer an opportunity to burnish China's image with the popularity of companies like Tencent, Alibaba, and ByteDance outside of China.

Digital Information Control in China and Beyond

Chinese companies are legally required to store their data and provide it to the PRC government under several legal rules and regulations.[81] This has been most notable in the cases of the 2021 Data Security Law, 2017 Cybersecurity Law, 2017 National Intelligence Law, and 2014 Counter-Espionage Law. For example, the 2014 Counter-Espionage Law requires that "when state security organs investigate to learn of espionage conduct or gather relevant evidence, relevant organizations and individuals shall truthfully provide and must not refuse."[82] Additionally, Article 7 of the 2017 National Intelligence Law requires that "any organization or citizen shall support, assist and cooperate with state intelligence work in accordance with the law."[83] Lastly, the 2017 Cybersecurity Law demands that "network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities."[84] This legal regime within China means that when state-owned and private companies operate abroad, they can potentially impart similar laws, regulations, and norms to autocrats the world over and provide a backdoor for China to obtain data globally.

Furthermore, the Hong Kong National Security Law, which was passed in the PRC's National People's Congress and implemented in June 2020, echoed many of the themes of the laws but within the context of the Hong Kong Special Administrative Region.[85] One particularly controversial aspect of the law is its requirement for platform service, hosting service, and/or network service providers to restrict, remove, or block content that violates the law according to authorities.[86] This law's effect is amplified because many foreign technology companies have

moved their services to Hong Kong from the PRC mainland due to the territory's formerly unrestrictive business operating environment. Hong Kong's descent into illiberalism has already affected several companies from democratic countries, especially technology companies Facebook, Google, and Twitter, which have all publicly grappled with compliance with the National Security Law.[87]

Lastly, building upon the 2017 Cybersecurity Law and the 2020 Hong Kong National Security Law, the 2021 Data Security Law provides PRC government authorities more leeway when it comes to data storage, privacy, and protection.[88] This law includes provisions related to China's "collection, storage, use, processing, transmission, provision, and disclosure of data" within the borders of the PRC but also outside.[89] The law also categorizes data in a hierarchical fashion by identifying "important data" and "national core data."[90] Although there is no strict definition of what important data is yet, the Data Security and Cybersecurity Laws encourage a consortium of national-level PRC government agencies to provide more details of which international companies will need to comply.[91] In comparison, the Data Security Law does define national core data information that touches upon national security, public interests, economic issues, and the data of everyday PRC citizens.[92] This law also states that data stored within China is not allowed to be transferred abroad without approval from authorities.[93] Otherwise, information operators could face hefty fines and penalties.[94] This bolstering of the legal regimes of the Cyber Security and Hong Kong National Security Laws through the Data Security Law provides more compliance issues for international companies, especially technology companies, operating across the PRC.

However, these data security laws only scratch the surface of the potential risks that could emerge from China's dominance of the various layers of the digital information stack. For example, Chinese social media platform TikTok creates numerous regulatory issues for other countries' governments including data sovereignty, privacy, disinformation, and content moderation.[95] Even though TikTok's parent company ByteDance stated that the data of users in the United States are stored in-country and backed up in Singapore, the social media platform is still operated in China by machine-learning infrastructure that is shared by all ByteDance platforms.[96] This leaves the platform susceptible to direct manipulation from ByteDance.[97] TikTok was found to suppresses content produced by creators who have disabilities, identify with the LGBT+ community, and other marginalized groups.[98] This is concerning given the popularity of TikTok in the case study countries covered in this report. Additionally, the platform was also criticized in India for suppressing content related to controversial pieces of legislation.[99]

China's engagement in the submarine cable sector is yet another area of potential concern. A submarine cable is usually governed by a consortium of companies that sign an MOU to share the costs of laying, deploying, and operating a submarine cable.[100] As a member of a submarine cable's consortium, a company is entitled access to some of the cable's bandwidth and thus can influence the cable's data flows.[101] Chinese telecommunications companies continue to dominate the submarine cable sector, exposing connected countries to the potential risk that those companies not only control some of their country's data but the bandwidth of the cable itself.[102] In addition to these concerns, one of the top submarine cable laying companies in the world, HMN Technologies (formerly known as Huawei Marine Networks), is a subsidiary of Huawei and the Chinese fiber-optic company Hengtong Group.[103] Its size increases the likelihood that more submarine cables will be laid by HMN Technologies in coming years, with those cables contributing to China's control of the digital information stack.

China's many restrictive laws make it difficult for countries that host Chinese state-owned and private companies involved in the digital information stack to not be affected by them. Regardless of where Chinese companies operate, they can pose problems ranging from data privacy and sovereignty issues, to improper content moderation, to outright not cooperating with local authorities and regulations. Most importantly, Chinese government

and Party authorities can compel local regulators and government officials to heed regulations that are not in the best interest of the local citizens. When combating China's digital information operations and their influence on the stack, civil society and democracy organizations should be aware that the reach of State and Party entities is very wide. Furthermore, there is always a risk that these entities will be acting in the best interests of officials in Beijing instead of local authorities or citizens.

Chinese Enterprise

Regulations/laws

2021 DATA SECURITY LAW
2020 HONG KONG NATIONAL SECURITY LAW
2017 CYBERSECURITY LAW
2017 NATIONAL INTELLIGENCE LAW
2014 COUNTER-ESPIONAGE LAW

Companies

HUAWEI
BYTEDANCE
ALIBABA
ZTE
TENCENT
BAIDU
LENOVO

Case Studies and Recommendations

This section of the report examines five case studies across the Global South in Southeast Asia, Sub-Saharan Africa, and the Caribbean to lay out how Chinese state-owned and private companies are involved in the countries' digital information stacks. The countries examined vary in susceptibility to China's influence on their digital information stacks ranging from the more resilient Jamaica to the most vulnerable Myanmar.

We have provided a selection of overarching recommendations below that can be applied to the countries covered in the case studies. Most recommendations are relevant to civil society, democratic organizations, and political actors on the ground working to stand up for civil liberties and human rights in their countries. Others offer avenues for established democracies to use their influence to support developing democracies resist Chinese domination of their digital stacks.

For each recommendation, we have provided further guidance or examples of how the recommendation can be applied in a local context, highlighting the context of a case study country. This is not intended to be an exhaustive list of country-specific recommendations, but rather to serve as inspiration for the application of the recommendations.

Recommendations

1. Monitor PRC Influence

Civil society actors must be mindful that although the governments featured in this report vary in many ways (levels of press freedom, treatment of political opposition, close relations with the government of the People's Republic of China, and other factors), they all share a desire to work closely with Chinese companies in areas like public safety, government efficiency, or monitoring political opposition. Such cooperation can mean accepting investments and cooperation in the digital information stack. Possible scenarios for cooperation range from outright collaboration between Chinese companies and local public security services to the adoption or adaptation of PRC models of surveillance and technological control.

Democracy organizations should consider monitoring mechanisms to track such collaboration, including technology exchanges, trade arrangements, changes in the security apparatus, surveillance abuses, etc. International donors and organizations can provide support to watchdog organizations through resources, monitoring tools, trainings, and exchanges with global peers.

For example:

- **Track policymakers' efforts to court closer ties with Chinese ICT companies.**

  Jamaica's Prime Minister (PM) Andrew Holness has publicly expressed several times that partnering with the Chinese ICT company Huawei could be beneficial for the development of the island nation's ICT infrastructure. PM Holness visited Huawei's Shenzhen headquarters in 2019 to seek further opportunities for collaboration, and while there, stated that Huawei could play a role in fighting crime, maintaining public order, and improving government efficiency in Jamaica. To ensure that PM Holness and other

leaders fully appreciate the risks of pursuing cooperation that can infringe on rights in Jamaica, activists and advocates on the ground should investigate and publicize policymakers' efforts to establish closer ties with Chinese ICT companies, especially on projects that can limit civil liberties.

2. Build Public Awareness

Civil society, media groups, and political actors should conduct awareness campaigns, drawing from the monitoring described above, to inform the public about the extent and possible impact of PRC cooperation on democratic function. Programming could include communications support to CSOs, training for journalists, and technical assistance to political parties on how to incorporate information on PRC influence operations into their platforms, policies, and constituent outreach.

Awareness efforts should include outreach to business leaders about the possible risks of working with Chinese companies with well-known track records of human rights abuses and by exposing the downsides of projects that compromise civil liberties. Groups can showcase examples of unfavorable financial outcomes for domestic companies through increased Chinese investments and national economic sovereignty losses through certain state trade arrangements.

For example:

- **In Nigeria, highlight the threat posed by compromised undersea cables.**

  Many voters and even policymakers may assume that undersea cables are merely content-neutral "pipes" over which internet is carried, when in fact the firms tasked with building, operating, and maintaining these arteries of information have tremendous power to surveil, censor, and of course, disable the flows of content over their networks.

- **In Uganda, publicize exploitative Chinese trade and investment deals.**

  China is by far the biggest public sector lender on the African continent, and generally imposes harsh terms on borrower governments to ensure that its investments are recouped, and to establish greater leverage over developing countries when they are not. This has led many African policy experts and members of civil society to accuse China of practicing "debt-trap diplomacy" aimed at ultimately exploiting African states, including Uganda, of their natural and human resources. Most recently, this came to a head in Uganda over fears that China sought to take possession of Entebbe International Airport over debts incurred during its renovation. The perception of Chinese "neo-colonialism" in the form of exploitative lending is profoundly concerning and offensive to many Ugandans.

3. Sustain Advocacy

Civic, political, and business groups should develop advocacy efforts to apply pressure on governments and parliaments to be more skeptical of significant investment projects and other arrangements with Chinese firms that would compromise their government's digital information stack. Advocacy campaigns could put forward draft legislation to build defenses but also lean on parliament to carry out its oversight function of executive policies. This advocacy should be aimed at both the local government and other global democracies, including in North America and Europe.

Such efforts should involve extensive research, with the help of international partners, of effective policies and legislation to defend against technological influence. International programming could include training in advocacy techniques, coalition building, and legislative outreach.

For example:

- **Advocate for greater support for financing from established democracies.**

  Local civil society groups should not only publicize the risks of exploitative investment deals but ask richer democracies around the world to increase the availability of fair financing for public development projects and should not by shy about highlighting the exploitation and injustice imposed by Chinese lending terms, when appropriate. This is an animating issue for many societies.

- **In Thailand and beyond, sustain and emulate the tactics and scale of the Milk Tea Alliance.**

  The Milk Tea Alliance was an extraordinary success in both form and substance. On substance, the movement reasserted the universal dimension of democratic values. Youths in places as diverse as Thailand, Taiwan, and Belarus all found they shared certain aspirations and expectations about how their governments should operate. On form, the movement managed to grab global headlines and to raise awareness to these youths' struggle far beyond those places' borders. It is important that the civil society ties birthed in that movement be sustained and reactivated when needed. And the transnational, humor-based, and social media-focused nature of the movement should be emulated in future attempts to push back against autocratic maneuvers in Southeast Asia and beyond.

4. Improve Local and Global Democratic Legislative Oversight

Parliaments can play an essential role in exercising oversight of the executive, and the private sector, in its relations with the PRC. Committees on foreign relations, human rights, defense and security, and technology and trade can all exercise scrutiny provisions to detect and prevent harmful arrangements and conduct. Parliament can also hold the government to account for how taxpayer money is used—purchasing of equipment, trade arrangements, debt—and whether it serves the public's interest. Committees can conduct hearings, inquiries, and question hours as well as create special commissions.

Where political will of the governing party is lacking, and depending on parliamentary rules and procedures, opposition parties could play a critical role in instigating investigations. International organizations could greatly support this process by providing training in the tools of oversight and effective scrutiny measures, such as impact assessments of draft policies and legislation. Parliamentary exchanges, such as the House Democracy Project (HDP), could also lend knowledge and support to legislators. Other democracies around the world, including the United States and the European Union, can enact legislative measures that can also help serve as models or have direct implications in other jurisdictions.

In countries where democratic backsliding has severely limited the powers of legislatures, such as in Myanmar, legislative paths may not be appropriate.

For example:

- **Push democratic governments for stricter sanctions and export controls on Chinese Information and Communications Technology (ICT) companies.**

  In Jamaica, the United States' strict sanctions and export control regime on many well-known Chinese ICT companies has reduced the impact of Chinese companies on Jamaica's digital information stack. The U.S. sanctions and export controls regime has raised the stakes for the Jamaican government and has dissuaded officials from approving the installation of Chinese ICT equipment across the digital information stack, specifically the network infrastructure layer. The U.S. policies have had a more considerable impact due to Jamaica's proximity to the United States, less than 600 miles south of Miami, Florida.

  Activists worldwide concerned about China's involvement in the digital information stack in their respective countries should continue to encourage officials from not only the United States but all democracies to issue more stringent sanctions and export controls on companies like Huawei, ZTE, China Unicom, and others.

5. Increase Transparency from Technology Companies

Civil society actors should seek more transparency from all technology companies involved in the digital information stack. Some governments discussed in this report are skeptical of working with Western technology companies due to legacies of colonialism and foreign interference; however, ensuring more transparency from these companies could also strengthen and empower local governments to be skeptical towards Chinese companies and their investments.

Similarly, civil society groups in countries with restrictive environments should push global democracies and the technology companies themselves to maintain access to these platforms for their countries' citizens.

For example:

- **In Myanmar, pressure the junta to restore access to social media platforms.**

  Until it was banned in the early days of the coup, Facebook was the internet in Myanmar. Over a year later, the country's population can now access a "whitelisted" internet, but Facebook, Twitter, and Instagram are still inaccessible without using a VPN, and the junta is working to make VPN usage illegal in Myanmar.

  Myanmar civil society should ask democracies (who, in turn, interact with Myanmar's current authorities) and Western social media platforms to put pressure on the junta to restore access. The huge market share of those platforms was one of the biggest weaknesses in the PRC's control of Myanmar's digital stack, and democracies should strive to restore that advantage.

6. Develop and Maintain Channels of Protected Communication

Democratic actors on the ground should advocate for the development, institution, and sustainment of protected communications technology due to its significance for vibrant political debate.

In their own operations, democratic actors on the ground should use applications that circumvent state surveillance like those founded by the U.S.'s Open Technology Fund, including Signal, Tor, Ricochet, and others.

In their advocacy with their own governments and democratic governments worldwide, democracy advocates should push for support for open technological alternatives.

For example:

- **In Myanmar, develop an alternative to Huawei's scanning app.**

  Huawei's scan app scans Myanmar citizens' ID cards to translate handwritten information into electronic databases for telecom operators. It is now used by all of Myanmar's major telecom operators whenever someone buys a new SIM card in the country. It allows the Chinese tech giant to build, and likely preserve access to, a database containing the identification information of an ever-growing share of the population. Democracies should sponsor an alternative system that would serve the same purpose without having a PRC tech company act as the middleman.

- **In Uganda, encourage the development and availability of alternative non- Chinese 5G hardware providers.**

  In a market like Uganda's, where nearly all internet access is cellphone-based, having non-PRC party-state providers for both devices and infrastructure hardware is uniquely important. Democracies in North America, Europe, and Asia should make competitiveness in the wireless market a strategic priority not only for the benefit of their own immediate security, but to give developing countries and their consumers more secure options too.

Thailand

Executive Summary

The United States' oldest treaty ally in Asia, Thailand was a key Cold War partner in a critical region. Although Thai-US relations remain solid, the current military government in Bangkok shares Beijing's outlook on governance and seeks to "silence critical voices, centralize policy and power, and privilege big businesses and mega-projects in growing Thailand's economy."[104] Thailand still maintains strong bilateral relations with other democracies, including Japan and the EU.[105] But the values that currently underpin its system of government are making it steadily drift toward China.

This drift is especially visible in the various layers of Thailand's digital information stack:

- In the network infrastructure layer, Chinese tech companies are involved in everything from submarine internet cables and data centers to the rollout of Thailand's 5G network.
- In the device layer, Chinese smartphones, including some with known security vulnerabilities, have a significant market share, and Chinese companies under U.S. sanctions over human rights abuses in Xinjiang are helping the Thai government in set up several smart city projects.
- In the application layer, TikTok is rapidly becoming a key platform for political activism, even as non-Chinese platforms remain the most widely used in the country.
- In the content layer, despite some success with older generations, Chinese diplomats' and state media's efforts to improve their country's perception have largely faltered with younger Thais who were instrumental in the rise of the Milk Tea Alliance, a pan-Asian pro-democracy movement.
- In the governance layer, Thailand's autocratic government is passing cybersecurity laws that resemble Chinese regulations and moving toward a more centrally controlled digital information stack that draws inspiration from the Chinese model.

With Chinese actors well-positioned in the network infrastructure and device layers of the Thai digital information stack, their relative weakness in the application and content layers is compensated by the overall appeal of China's autocratic model for Bangkok.

Overview of Sino-Thai Relations

Since a 2014 military coup, most NGOs consider Thailand to no longer to be a democracy.[106] As a result, while Thai foreign policy officially strives to maintain balanced relationships with competing great powers, ties between the Kingdom and democracies have worsened and its ties to fellow autocrats in Beijing have grown closer. However, in the economic realm, some Thai commentators are concerned about the growing commercial deficit with China, while at the same time, trade relations with the United States remain strong.[107]

A further illustration of Thailand's ambivalent attitude toward China is a history of failed or downsized Belt and Road Initiative (BRI) projects in the country. For instance, a proposed US$ 9.9 billion plan to build 873 km of high-speed railway between Bangkok and Kunming in China, passing through Laos, was announced in 2014. After almost 30 rounds of talks and years of delay, both sides finally agreed in March 2021 to build 251 km of the track between Bangkok and a city in northeastern Thailand.[108] Other stalled projects associated with the BRI in

the Kingdom include a US$960 million coal-fired power plant[109] and the ambitious Kra Canal meant to bypass the Strait of Malacca by cutting through Thailand.[110] Further demonstrating Thailand's reluctance to cede too much to China, these initiatives are at times described as BRI projects, and other times as Thai initiatives.[111]

That may be the key to understanding China and Thailand's slow but steady rapprochement. The current military government in Bangkok shares Beijing's outlook on governance. Just like the Chinese state, Thai authorities seek to "silence critical voices, centralize policy and power, and privilege big businesses and mega-projects in growing Thailand's economy."[112] For instance, the US$45 billion Eastern Economic Corridor (EEC) economic mega-project may be the military government's brainchild, but it could just as easily have been thought of in Beijing. Although Thailand is maintaining strong bilateral relations with the United States, Japan, and even the EU,[113] the values that currently underpin its system of government are making it slowly drift toward China. Recently, the Chinese Ministry of Foreign Affairs quoted the Thai Foreign Minister to delegitimize the United States' Summit for Democracy, to which neither Beijing nor Bangkok were invited. This is emblematic of the broad trajectory of the Thailand-China-United States triangle.[114]

China's growing presence in Thailand is particularly visible in the Kingdom's digital stack. From telecom infrastructure to Chinese-made smartphones, the Chinese state and its private sector proxies are playing a key role in making Thailand's digital information space safe for the military government, and conversely, inhospitable to pro-democracy forces.

The Network Infrastructure Layer

Companies in China's public and nominally private sectors have made great strides in the infrastructure layer of Thailand's digital stack. From internet cables to 5G networks, Chinese actors are involved in all aspects of the Thai telecom infrastructure. While this case study focuses on Chinese companies, it's important to acknowledge that Thai companies and authorities are still intent on keeping other foreign players involved in the deployment of Thailand's infrastructure.

More than half of the eight international submarine cables landing in the country are partly owned by Chinese companies. For instance, Chinese state-owned telecom operator China Unicom was one of the initiators of the Asia-Africa-Europe 1 (AAE-1) submarine cable in 2011.[115] The cable was completed in June 2017 and gets to China through Myanmar, where China Unicom fully funded the AAE-1 landing station.[116] In March 2017, Huawei Marine, the submarine cable-laying arm of the Chinese tech giant, completed the deployment of the Malaysia-Cambodia-Thailand submarine cable. Huawei Marine designed the cable system, as well as the landing station in Cambodia.[117] In these two projects, it is instructive to see how Chinese companies foster connectivity between Thailand and other countries with close ties to Beijing. The geopolitical undertones of Chinese companies' submarine cables activity are sometimes even more overt. State-owned China Mobile, a member of the consortium building the upcoming Southeast Asia-Japan 2 cable, describes the project as part of BRI.[118]

Chinese companies have also made significant inroads in Thailand's 5G infrastructure. In 2014, China Mobile International, a wholly owned subsidiary of the state-run China Mobile Communication Group, acquired 18 percent of Thai mobile operator True.[119] In September 2019, China Mobile and True announced a collaboration on "5G development and network consolidation in Thailand."[120] Chinese telecommunications equipment giant ZTE is expected to build True's 5G network in Thailand.[121] In November 2021, Reuters reported that True was thinking of merging with competitor Dtac to form a telecom giant with over 50 percent of the mobile market in

Thailand.[122] Under this deal, China Mobile could potentially own over 10 percent of Thailand's largest telecom operator.[123] But Thai regulators could still block the merger because of concerns over excessive foreign ownership.[124]

Until the True-Dtac merger goes ahead, the largest Thai telecom operator remains Advanced Info Service (AIS), whose ultimate owner is Singaporean state holding company Temasek. It is unclear who is providing the equipment used by AIS to deploy its 5G network. In August 2019, AIS signed 5G deals with Nokia, Huawei and ZTE to "develop industrial 5G cases."[125] However, a month later, the Bangkok Post reported only on the alliance between AIS and Huawei.[126] When prodded about the bid, AIS' president told Reuters that "U.S. allegations around Huawei were 'not proven.'"[127]

The Thai government itself has collaborated with Chinese tech giants as well. In February 2019, Huawei was one of the companies to launch a "5G test bed" in Chonburi, a province at the center of the military's EEC project. At the time, the Thai Minister of Digital Economy declared that the test bed would allow the Thai government to assess the veracity of the accusations made against Huawei.[128] In September 2020, Thailand's Ministry of Digital Economy announced it would be opening a 5G Ecosystem Innovation Centre in collaboration with Huawei. The Chinese tech giant reportedly invested over US$14 million to fund the installation.[129] The Minister of Digital Economy himself delivered the keynote speech at the Centre's launch, revealing a degree of proximity between the Chinese tech giant and some Thai political elites.

Data centers are another area of concern. Chinese state-owned China Telecom operates three data centers in Bangkok,[130] Tencent Cloud launched its second data center there in June 2021,[131] and Huawei invested US$23 million to build its third data center in Thailand in November 2020.[132] With Chinese companies obligated to hand over any data at their disposal if required to do so by the Chinese government, there are obvious risk to using these data centers. In addition, the news story announcing the launch of Tencent's latest center explains that it would support "all ranges of intelligent solutions […] including artificial intelligence [and] facial recognition."[133]

Chinese tech companies' expertise in telecommunications is giving them a foothold into other sectors. For instance, in 2017, Huawei partnered up with the Thai Provincial Electricity Authority to establish an innovation center that was to act as "a place for the development of innovations for the electricity industry based on advanced information and communications technology."[134]

Huawei's extensive involvement in the Thai infrastructure layer has allowed it to build a close relationship with Thailand's autocratic government. In March 2021, Huawei was awarded "the prime minister's award in the 'Digital International Corporation of the Year'," the only private firm to win this award.[135] In November 2021, the company's CEO attended a virtual meeting with the Thai Prime Minster. During that meeting, the Thai leader praised Huawei's commitment to his country's digital transformation.[136] It is easy to dismiss these events as public relations fluff. But given the extensive powers at the Thai Prime Minister's disposal, his direct endorsement of the Chinese tech giant may influence all other actors in the Thai telecom sector and society more broadly.

The Device Layer

Chinese tech companies have gained market share in Thailand's digital stack in the device layer, where handsets and smart city projects are potentially significant areas for China's influence.

Chinese handsets are potentially problematic for a country's democracy. The Lithuanian Defense Ministry warned in August 2021 that Huawei and Xiaomi phones posed "cybersecurity risks," with the latter possessing dormant censorship functionalities.[137] The Thai press has not relayed those concerns. In July 2020, AIS entered into a partnership with Huawei to sell 5G smartphones in Thailand.[138] While the U.S. campaign to raise awareness about the risks associated to Huawei may have dented its market share in Thailand, other Chinese companies like Oppo, Vivo, and Xiaomi have been the main beneficiaries from Huawei's losses.[139]

Chinese tech companies have facilitated the development of several smart city projects, and the corollary spread of facial recognition technology, in Thailand. The president of Megvii, a Chinese tech firm specialized in image recognition and deep-learning software, met with Thailand's Deputy Prime Minister in November 2018 and explained that his company was helping the Thai Central Bank and Thai Police departments implement facial recognition technology.[140] Megvii was placed under U.S. sanctions in October 2019 over its role in human rights violations against Uyghurs in Xinjiang.[141] In December 2019, Chinese AI company SenseTime, also under U.S. sanctions since October 2019 over its role in human rights abuses in Xinjiang, entered into a joint venture with a major Thai real estate developer to "introduce AI technologies […] that focus on property security."[142] Last but not least, in 2019, Huawei released a 148-page white paper on "Smart City services for Phuket."[143] The Deputy Prime Minster signed the text's foreword. With Phuket one of the world's top tourist destinations, Huawei stands to gain access to very valuable data by deploying its surveillance equipment on the island.

In the device layer, it seems that Thai consumers are not overly persuaded by growing concerns about the safety of Chinese made smartphones. As 5G enables increasing interconnectivity between a whole range of IoT devices, U.S.-sanctioned Chinese companies seem at the forefront of developing surveillance systems that can take advantage of this increased interconnectivity. Under the guise of safety and public order, the likes of Megvii and SenseTime are laying the groundwork for the ever more invasive surveillance of Thai citizens.

The Application Layer

While Chinese tech companies are solidly embedded in Thailand's infrastructure and device layers, they are somewhat lagging in the apps layer. As of January 2022, only two of the fifteen social media platforms most-used by Thai citizens were Chinese.[144] TikTok came in fourth, while WeChat was fourteenth. While 79.6 percent of Thai internet users between 16 and 64 used TikTok, and 11.6 percent of the same demographic used WeChat, 93.3 percent used Facebook and, according to earlier data,[145] 94.2 percent used YouTube, showing the greater reach of U.S. platforms. Tencent's WeChat app seems mostly used by members of the Chinese diaspora and does not have a large user base outside of that community. The percentage of Thai internet users between 16 and 64 who use WeChat actually fell from 24.9 percent in 2021 to 11.6 percent in 2022.

The platform of greatest concern is TikTok. TikTok was the most downloaded app over the whole of 2020 in Thailand.[146] Indeed, the percentage of Thai internet users between 16 and 64 who use TikTok jumped from 54.8 percent in 2021 to 79.6 percent in 2022. This makes it a key platform for political activism. Preliminary analysis of the content that circulates on the platform shows that TikTok allows the spread of anti-government videos, such as short clips of Thai protests.[147] But the government also has a large voice. Thai Prime Minister Prime Minister Prayut Chan-o-cha opened an account on the platform in February 2021 "to connect with younger people."[148] The app also played a key role in the vaccine debate, a highly sensitive issue in Thailand.[149] An app whose ultimate owner is based in Beijing is now inextricably enmeshed in the Thai public debate, among a demographic whose importance will only increase in the short-to medium-term.

Chinese tech companies have also established a foothold in the Thai financial sector. In October 2016, Alipay reached a cooperation deal with ten overseas airports, including Thailand's Suvarnabhumi Airport.[150] WeChat Pay's arrival in the country[151] and Alipay's cooperation with Thailand's Kasikorn Bank[152] were mainly aimed at increasing Chinese tourists' spending. Even though these deals did not target Thai consumers, they built a relationship between Alipay's owner Ant Group and Thai authorities.

In parallel to these efforts to make Chinese payment apps operational in Thailand, Ant Group also bought 20 percent of Ascend Money, the Thai company that runs True Money, the largest e-wallet service in Thailand, in June 2016.[153] Ant Group's ownership in Ascend Money has since risen to somewhere between 25 and 30 percent,[154] with the other major investor being CP Group, a Thai conglomerate with deep ties to the CCP that go back decades.[155] Ant Group has since been caught in the CCP's clampdown on Chinese tech companies and it is difficult to determine the extent to which its stake in Thailand's largest e-wallet service serves China's geopolitical interests. Nevertheless, in February 2021, China chose only Thailand and the United Arab Emirates to participate in a test for cross-border payments of central bank digital currencies.[156] In December 2021, the director of the United Kingdom's signals intelligence agency GCHQ publicly warned that "China's digital renminbi […] risks becoming a tool to surveil users and exert control over global currency transactions."[157]

In Thailand's information space, apps developed by companies based in democratic countries still have the largest market share. However, TikTok's rapid growth, particularly among an important demographic, is already challenging Google, Facebook/Meta, and Line's dominance in the country. Meanwhile, Chinese companies like Ant Group have a solid foothold in Thailand's burgeoning e-payment sector. In this context, China critics and democracy activists could be worried about the implications of electronic payments becoming the new normal in Thailand.

The Content Layer

The Chinese state and media outlets affiliated with it have made strides to amplify narratives conducive to China's interests in Thailand in the content layer, leading to significant backlash from Thai civil society.

A November 2019 article from Thailand's third largest newspaper Khaosod reported that "at least a dozen" Thai language media organizations had signed content sharing agreements with Xinhua, the largest state-run news agency in China.[158] Notably, Khaosod itself had entered into such an agreement with Xinhua in August 2019.[159] Furthermore, Chinese state media firm China Daily is a member of the Asia News Network (ANN), which also includes The Nation, Thailand's largest English-language publication, which regularly picks up China Daily content.[160] The Chinese Ministry of Foreign Affairs has also supported media workshops for Thai journalists.[161] These are only a handful of data points from a broader trend that has seen Chinese state media provide free content to Thai newspapers and TV stations since at least 2014.[162]

In parallel to Chinese state media's effort to promote the CCP's worldview in Thailand, pro-Chinese information manipulation is also taking place online. Pro-CCP content abounds on the most popular social media apps in Thailand, most notably Facebook and Line. Chinese narratives seem to have most traction with older Thai generations. Experts interviewed by RFA argued that Thai citizens, especially older users who overwhelmingly use Facebook and Line, are not familiar with Chinese information manipulation online.[163]

Unlike in many other countries, Chinese diplomats in Thailand have not fully embraced the "wolf warrior" model. The Chinese embassy in Bangkok's Facebook page is the eighth largest of all Chinese diplomatic pages on the social media platform. Top performing posts show messaging that is consistent with the narratives the Chinese state promotes globally: advertising Chinese COVID relief,[164] defending the efficacy of Chinese vaccines,[165] and attacking the United States' definition of democracy.[166]

Younger Thai citizens who have been the engine behind TikTok's spectacular growth in country are far more skeptical of China and use social media for political protest. Beijing's support for Thailand's military government has alienated the country's more reformist youth. As a result, despite China's efforts in Thailand's information space, young Thai netizens joined forces with others in Taiwan, Hong Kong, Myanmar, and beyond to form the "Milk Tea Alliance" in April 2020. Under the guise of their shared appreciation of a popular tea drink, netizens from these regions came together to promote democracy and push back against authoritarian regimes, primarily the Chinese state. Since then, Chinese state media have further alienated Thai youth. Spooked by parallels between Thai protests in 2021 and Hong Kong's pro-democracy movement, Chinese outlets like the Global Times have unconvincingly accused Thai youth of "being used as cannon fodder by the US and its proxies."[167] Through humor, memes, and social media savviness, the loose coalition of young activists outmaneuvered China's clunky attempts to push back[168] and captured global headlines.[169]

As was the case in the apps layer, China's influence in the content layer of Thailand's digital stack is mixed. On the one hand, financial pressures on Thailand's traditional media have given Chinese state media an opportunity to bring pro-CCP narratives to a large section of the Thai public. Online, older generations who predominantly use non-Chinese social media apps are susceptible to pro-Chinese information manipulation attempts. On the other hand, Beijing's support for Thailand's military government has alienated younger Thai citizens who aspire to a more democratic society. The fact that Thailand is at the heart of the Milk Tea Alliance, a pro-democracy movement that has achieved global significance, shows the limitations of the Chinese state's influence over the Thai content layer.

The Governance Layer

Turning to the final layer of the stack, governance, it is important to remember that Thailand is not a democracy in 2022. China may be a technological catalyst to the Thai autocracy, but the authorities in Bangkok are a major driving force behind the legal framework in which liberticidal technologies are deployed. As essential as Thai laws like the draconian lèse-majesté legislation are to the autocratic architecture underpinning Thailand's digital stack, they cannot be ascribed to Chinese interference.

Things are even less certain when it comes to the well-documented conduct of information operations by the Thai security forces.[170] After Twitter removed 926 accounts connected to the Royal Thai Army in October 2020 over their engaging in information manipulation on the platform, the military eventually acknowledged that some of its staff had undergone training "to understand digital media platforms effectively and appropriately."[171]

Who provided the training was never revealed, but there is a reasonable amount of evidence suggesting that Chinese trainings could have contributed to the Thai government's current approach to information operations. Researcher Aim Sinpeng explained in an online event on Thailand's information operations that "Chinese authorities conduct training on different ways to manage information operations for South-East Asian governments."[172] A separate report highlights the fact that military educational exchanges between China and Thailand

have increased significantly since the 2014 coup, although it goes on to add that the United States is still Thai officers' preferred destination.[173] Australian researchers also found that, following instructions from the Chinese Ministry of Public Security, Chinese tech company Meiya Pico provided "digital forensics and cybersecurity" training sessions to Thai police officers.[174]

China's influence over the Thai military government's thinking concerning the governance of Thailand's digital stack was most obvious in the immediate aftermath of the 2014 coup. In September 2015, Thai authorities openly envisaged setting up a "China-like Internet Firewall" to "control all digital traffic in and out of the country."[175] While they eventually backed away from that plan, researcher Valentin Weber recognizes the spirit of "the vague and broad nature of China's 2017 cybersecurity law" in the Cybersecurity Act Thailand passed in February 2019.[176] In some respects, China could even be seen as inadvertently spreading its autocratic approach to digital governance as news reports suggest that part of the reason behind the Thai government's obsession with controlling information within its borders is to prevent the spread of negative stories that would potentially discourage Chinese tourists from visiting Thailand.[177] Inspired by China's successful control over the digital environment within its borders, and perhaps also worried that Thai citizens' freedom of expression might harm economic relations with Beijing, it is clear that Thailand's military government has adopted at least part of the Chinese model of digital governance.

Chinese tech companies also play a role in spreading China's vision of technology. This report has already touched upon Huawei's extraordinary activity in venues like the International Telecommunication Union (ITU) study group on fixed and mobile network protocols. It is notable that the only Thai ministry attending ITU meetings is the Ministry of Digital Economy and Society, whose connections to Huawei have already been described in the infrastructure and device layer sections. In addition, the inclusion of the Chinese tech giant's equipment in Thailand's infrastructure layer and its significant smartphone market share in the country are de facto embedding Chinese technical specifications beyond China's borders. Lastly, when the Huawei OpenLab in Bangkok offers, among other services, to "certif[y] partner products and issu[e] Huawei certification," it is encouraging third parties using this certification service to embrace its set of priorities to integrate into the Huawei ecosystem, and possibly ease their access to China's huge market. It is very unlikely that Huawei's priorities include concerns that matter to democracy's health, such as data privacy or government accountability.

While the Thai military government has its own reasons to embrace high-level of control over the country's digital stack, it is also apparent that through security trainings, the power of example, the implicit threat of economic loss, and the fostering of autocratic synergies in standards-setting, the Chinese state and Chinese companies play a crucial role in the autocratic orientation of Thailand's governance layer.

Conclusion

China's presence in the five layers of Thailand's digital stack has achieved varying levels of success. In the infrastructure and device layers, Chinese companies have made significant inroads. In the application and content layers, Chinese actors' presence seems more contested and sometimes even counterproductive, as shown by the global rise to prominence of the Milk Tea Alliance. In the infrastructure, device, application, and content layers, the significant presence of foreign non-Chinese actors seems consistent with Thailand's tradition of balancing great powers' influence in its territory.

The governance layer is different. Here, the influence of China's overall approach to digital information systems is ubiquitous. As could be expected from an autocratic regime, the Thai military government is clearly drawing inspiration from Beijing when designing the conceptual and legal framework for the Kingdom's digital stack. Chinese involvement in Thailand's "creeping digital authoritarianism" cannot always be proven.[178] But, even absent a Great Firewall of Thailand, the increasingly repressive legal framework regulating the Thai digital information space, the military government's conduct of information operations against its own population, and the AI-enabled surveillance of Muslim groups in the Kingdom's Southern provinces are all too familiar to observers of the Chinese Communist Party's behavior inside of China's borders.[179]

Myanmar

Executive Summary

Myanmar's long land border with China and lengthy coastline on the Indian Ocean make the country strategically important for Beijing. However, the February 2021 military coup has made the situation in Myanmar less predictable. On the one hand, the coup undid many of the investments Chinese companies had made in the country under the democratically elected Suu Kyi government. On the other hand, the junta is militarily and diplomatically dependent on its northern neighbor as its brutal repression of the population has pushed out other investors, including Japan, Singapore, and India. If they can navigate the turbulent political context, the Chinese state and Chinese companies stand to lastingly increase their footprint in Myanmar.

Their involvement in Myanmar's digital information stack reflects this risky calculus:

- In the network infrastructure layer, Chinese companies have been involved in all of Myanmar's submarine internet cables and are central to the deployment of 4G and 5G in the country. A Huawei-developed system collects the ID information of most Myanmar citizens when they buy a SIM card and key government functions like disaster relief depend on Chinese state-run navigation satellite technology.
- In the device layer, Chinese companies manufacture more than half the handsets sold in Myanmar and are collaborating with the government to deploy smart city systems, often including facial recognition technology, in the country's main cities.
- In the application layer, TikTok is making headway with Myanmar's youth and has already become a battleground for pro- and anti-military activists. However, non-Chinese apps like Facebook and Line still dwarf their Chinese competitors, and the coup largely reversed Chinese companies' inroads into Myanmar's digital payment industry.
- In the content layer, China's efforts to place more of its state media's content in local outlets have not been enough to avoid significant backlash over its support to the military government, both real and perceived.
- In the governance layer, the military government has passed a cybersecurity bill with provisions that directly echo those found in the regulatory framework of China's digital information stack, and some media reports indicate that Chinese experts have helped the military increase its control over Myanmar's internet.

The military government hardening stance toward pro-democracy opponents will increase its reliance on China. Underpinned by a cybersecurity bill that echoes Beijing's own digital governance architecture, measures like banning Facebook and pushing Norwegian telecom group Telenor out of the country are paving the way for the Chinese state to further cement its entrenchment in Myanmar's digital information stack.

Overview of Sino-Myanmar Relations

Myanmar and China share a 2,129 km border. In the 21st century, the relationship between the two neighbors has been somewhat turbulent, with an overall upward trajectory. The partial democratization of Myanmar in the 2010s initially led to an improvement in relations with the United States and other democratic countries.[180] However, as Western condemnation of Aung San Suu Kyi's democratically elected government grew ever stronger over the atrocities it committed against the Rohingya minority, Myanmar started shifting closer to China. Ties

between Naypyidaw and Beijing had in fact grown so close that many experts believe that the Chinese authorities were initially dissatisfied with the February 2021 military coup that deposed Suu Kyi's government.[181]

As things currently stand, China is Myanmar's largest trading partner. According to data from 2019, China was the destination for more than a third of Myanmar's exports, as well as the source of more than one third of its imports.[182] Myanmar also occupies a strategic geographical location for China, providing direct access to the Indian Ocean and an alternative route for Chinese energy imports that currently flow through the Malacca Strait, a location Chinese authorities see as vulnerable to potential U.S. blockades.

As a result, China has invested a lot of time and resources to integrate Myanmar into the Belt and Road Initiative (BRI). Given that it was the now-deposed Suu Kyi government that negotiated the China Myanmar Economic Corridor (CMEC), a connectivity scheme tying Myanmar's economy to China's, the coup raised considerable uncertainty over many Chinese-led infrastructure projects.[183] However, it now seems that key projects like the US$2.5 billion Mee Lin Gyiang liquified natural gas generating plant, the US$1.3 billion Kyaukphyu deep sea-port, and the development of several special economic zone are back on track. In fact, with major investors like India, Japan, and Singapore pulling back from the country since the February 2021 coup, China has become an ever more indispensable partner for the Tatmadaw, another name for Myanmar's armed forces.[184]

In addition to being a close economic partner, China is also a key military partner for its southern neighbor. Between 2014 and 2019, China accounted for around 50 percent of the Tatmadaw's major arms imports, with Russia a close second.[185] It was China's voice on the United Nations Security Council that spared the military government from the worst punitive sanctions in the aftermath of the coup. However, Beijing's support for fellow authoritarians in Naypyidaw is not without its risks. Myanmar citizens who took to the streets after the coup are incensed by what they perceive as foreign interference. Chinese-owned factories and a natural gas pipeline between both countries have already been attacked and Beijing is concerned that more could be coming.[186] Growing anti-Chinese sentiment, and the threat it poses to the billions China is pouring into CMEC explains why now, more than ever, control of Myanmar's digital stack, especially its information functions, is a top priority for Beijing.

The Network Infrastructure Layer

Starting with the brick-and-mortar dimension of the digital stack, the infrastructure layer, China's presence in Myanmar is very significant. From internet cables to satellites, virtually every aspect of Myanmar's telecom infrastructure, as well as much of its other critical infrastructure, involves some degree of Chinese participation.

Chinese companies have participated in all three submarine internet cables that land in Myanmar. State-owned China Mobile, China Unicom, and China Telecom are three of the several companies that own the SeaMeWe-5 cable.[187] China Telecom and China Unicom are two of the several companies that own the older SeaMeWe-3 cable.[188] Finally, China Unicom was one of the initiators of the Asia-Africa-Europe 1 (AAE-1) submarine cable in 2011.[189] The cable was completed in June 2017 and gets to China through Myanmar, where China Unicom fully funded the AAE-1 landing station.[190] This project's importance to both countries is highlighted by the fact that China Unicom and Myanmar Posts and Telecommunications (MPT) signed the agreement to build the landing station in the presence of China's Prime Minister and Myanmar's President at the presidential palace in Naypyitaw. In addition, the landing station also connects mainland China to AEE-1 via the terrestrial China Myanmar International (CMI) cable. The CMI cable, entirely funded by China Unicom, runs from Nge Saung Beach,

through Yangon and the capital Naypyidaw, and onward to China via Ruili in Yunnan province.[191] Through AAE-1 and CMI, Myanmar serves as a direct link between Europe and China. Further highlighting the importance of these cables to China's national interests, China's People Daily outlet reported in 2016 that AAE-1 would "facilitate the strategy of China's BRI."[192]

Turning to 4G/5G infrastructure, Myanmar had four telecom operators pre-2021 coup: Myanmar government-run MPT, Norwegian majority state-owned Telenor, joint venture between the Tatmadaw and the Vietnamese military MyTel, and Ooredoo Myanmar, the subsidiary of the Qatari Ooredoo group. Telenor has sought to pull out of Myanmar since the summer of 2021 in response to growing pressure from the military government to cut services and hand over internet and mobile user data. However, the junta wants a local company to acquire at least part of Telenor's Myanmar operations and has been stalling the proposed sale to Lebanese conglomerate M1.[193]

Of these four operators, Ooredoo is most tied to Chinese companies. In 2017, the Qatari-owned operator partnered with part-Chinese state-owned ZTE and Nokia to upgrade its 4G network.[194] However, ZTE was the only company chosen to launch Ooredoo's 5G network in Myanmar, conducting a live demonstration of 5G use-cases in Myanmar in 2019.[195] The partnership further deepened in early 2020 when ZTE took over "the responsibilities for managing the network and customer experience operations of Ooredoo Myanmar."[196] That development is particularly significant as it essentially grants the Chinese company effective control over the network of an operator that services around 15 percent of Myanmar's population.

ZTE is not the only Chinese company active in Myanmar. The presence of nominally private Huawei goes back further and is more extensive than that of ZTE. A 2016 report from the Chinese tech giant explains that it was instrumental in building the country's modern telecom infrastructure and provided coverage to a third of the country's population.[197] More recently, military-owned MyTel announced that it would partner with Huawei for its 5G network services.[198] And in the summer of 2020, the local Huawei CEO said in an interview that his company was working with Myanmar state-owned MPT.[199] Huawei's access to the data of Myanmar's citizens is staggering. Cellphone users must register their ID cards or passports to buy a SIM card. Huawei developed a service that could convert the characters contained in photos into text files, making the registration process much easier. With all the major operators in Myanmar now using the service, some experts claim that Huawei has more information on Myanmar citizens than even the country's own Immigration Department.[200]

Chinese high-tech expertise and services have also given the Chinese state a significant presence in critical sectors beyond telecom. In 2013, the year in which BRI was launched in Beijing, Myanmar adopted the BeiDou Navigation Satellite System (BDS), China's answer to the American-run GPS, "to collect agricultural data."[201] This means that Myanmar's food supply, and a whole range of essential government functions including disaster prevention and climatic resilience, have relied on the Chinese state for the better part of a decade. Myanmar's reliance on BDS is only part of the scientific cooperation between both countries. In November 2018, China and Myanmar inaugurated a joint laboratory on radar and satellite communications.[202]

The Chinese state and Chinese companies have a very significant presence in the infrastructure layer of Myanmar's digital stack. The military government is strengthening China's hand in the country. With Telenor pulling out, all the remaining players are to some extent reliant on Chinese tech companies to develop and, in at least some cases, run their existing 4G and upcoming 5G networks. Similarly, the registration requirement attached to SIM cards is granting Huawei access to the personal information of more and more Myanmar citizens. With

even sectors as critical as food supply at least partly reliant on Chinese technology, the infrastructure layer alone highlights how dependent Myanmar has become on its northern neighbor.

The Device Layer

Chinese tech companies have gained market share in Myanmar's digital stack outside of the infrastructure layer. In the device layer, Chinese companies manufacture most of the handsets sold in Myanmar and are involved in many of the country's smart cities projects.

Chinese companies have a majority market share for smartphones in Myanmar thanks to their lower price point. Huawei was Myanmar's largest smartphone seller between 2013 and 2016, when it positioned itself as a cheap alternative to then reigning champions Apple and Samsung.[203] It started losing ground from 2016 onward as it positioned itself more and more as a premium brand. Since then, Chinese competitors like Xiaomi and, more recently, Oppo have become the top-sellers in Myanmar. As things now stand, these three Chinese brands now hold over 50 percent of the country's mobile market.[204] By comparison, Samsung and Apple hover at around 10 percent each.

While pricing partly explains Huawei's market share losses, the broader geopolitical situation likely also plays a role. The Nikkei reported in 2020 that the U.S. decision to cut the Chinese tech giant's access to the Android OS was one of the factors behind its slipping market share in Myanmar.[205] In addition, documents like Lithuania's August 2021 report explaining that Huawei and Xiaomi phones pose "cybersecurity risks" and that Xiaomi phones have dormant censorship functionalities must resonate with Myanmar's many citizens who are weary of the government's repressive use of technology.[206] In fact, data shows that Apple sales gained ground vis-à-vis their Chinese competitors in the aftermath of the February 2021 coup.[207]

Myanmar's authorities do not seem to share citizens' concern with the growing presence of Chinese companies in the country's device layer. Even before the coup, Huawei was involved in several smart city projects around the country. In 2019, the Mandalay regional government signed a deal with the Chinese tech giant to deploy AI-enabled cameras around the city. Equipped with facial-recognition software, the cameras were meant to lower the high crime rates highlighted in "a survey conducted by district police and Huawei."[208] In December 2020, Huawei provided 335 surveillance cameras for a "Safe City" project in Naypyidaw. While Huawei explained that it did not provide the facial and license plate recognition technology installed on the camera, it is unclear whether the company provided only the cameras or whether it designed an entire system that was then implemented by sub-contractors.[209] Besides Mandalay and Naypyidaw, Myanmar's "Safe City" plan also aimed to deploy a surveillance system in Yangon by mid- 2021. Yangon already uses a traffic management system developed by Chinese state-owned Hikvision.[210] Hikvision was placed under U.S. sanctions in October 2019 over its role in human rights violations in Xinjiang, with additional restrictions imposed in June 2021.[211]

As is the case for the infrastructure layer, Chinese companies play a key role in Myanmar's device layer. Moreover, with smartphones and surveillance cameras being one step closer to consumers than telecom infrastructure, the impact of the Chinese presence in the device layer on the shrinking civil liberties of Myanmar's population is even more apparent. The rapid expansion of Chinese technology-enabled surveillance systems disguised as smart cities was already cause for concern under the Suu-Kyi government. These concerns have heightened now that Myanmar's military runs the country. Since the coup, the authorities have already killed over 1000 people and arrested thousands more, in what Human Rights Watch says amounts to crimes against humanity.[212]

Advanced automated surveillance systems enable the authorities' ruthless repression of Myanmar's citizens. Similarly, the dominance of Chinese smartphones known to have surveillance capabilities opens another avenue through which Myanmar's autocratic authorities can exert control over the population.

The Application Layer

In contrast to China's great success in the infrastructure and device layers of Myanmar's digital stack, Chinese companies are up against stiff competition in the apps layer. WeChat, the mega-app that is ubiquitous in China, has only made limited inroads in Myanmar. By contrast, Facebook was so widespread in the country that reporters could write in February 2021 that "Facebook was the internet in Myanmar."[213]

Facebook is the juggernaut of Myanmar's social media scene, with 22 million users in a country of about 53 million inhabitants. The app has had its fair share of controversy over the years, most notably over the role it played in spreading hate speech that preceded and accompanied the atrocities perpetrated by the Myanmar authorities against the Rohingya minority in 2017.[214] Meta's towering role in Myanmar's digital space was further highlighted when the military cut off access to all its apps, including Facebook, Messenger, and Instagram in the immediate aftermath of the February 2021 coup.[215] Since then, Facebook has taken a strong stance against the military government, taking down all pages belonging to the military and its businesses—including telecom operator MyTel.[216] Myanmar's reliance on foreign apps inimical to the military government is such that in the summer of 2021, the authorities released a whitelist of approved domain names that included Instagram, WhatsApp and YouTube, but kept Facebook and Twitter banned. Despite the ban, it is apparent that many in Myanmar continue to access banned apps through VPNs, with Facebook's usage numbers now almost back to their pre-coup level.[217]

Among the apps white-listed by the military in May 2021 was Tencent's WeChat. In 2015, the app launched in Myanmar in partnership with Huawei.[218] Since then, it often comes preinstalled on Chinese smartphones. While WeChat's reach cannot be compared to Facebook, or even to Japanese app Viber, it still has a large role in the parts of Myanmar that border China. The app's ubiquity in China means that it is a prerequisite for Burmese traders looking to do business with their Chinese counterparts. In addition, the app's good performance in poor network conditions makes it very convenient in areas where internet coverage is still spotty.[219] In Chinese-dominated industries like the jade trade, WeChat has been so widely adopted that it causes significant disruptions for local traders.[220] In addition, civil society groups have used the app to rescue Myanmar women sold to be married to Chinese men on the other side of the border.[221] But what is apparent from stories written about WeChat in Myanmar is that its use is limited to those who interact directly with China one way or the other, with little influence on the country's information space.

In contrast to WeChat, newcomer TikTok has been making rapid progress in Myanmar. Consistently in the top fifteen most downloaded apps in the country, the app has been at the center of the information contest between the military junta and anti-coup protesters.[222] On the one hand, pro-democracy protesters have flocked to the platform, resulting in the anti-junta hashtag #savemymyanmar being used 1.4 billion times on the platform as of April 2021.[223] On the other hand, after Facebook took down military accounts in February 2021, TikTok became something of a safe haven for the junta's propaganda. Throughout February and into early March, videos showing soldiers and policemen threatening protesters proliferated on the app.[224] Although TikTok eventually removed much of this content, reporting by Rest of World shows that parent-company ByteDance was slow to react.[225] The international scrutiny drawn by TikTok in the aftermath of the February coup shows how important a social media platform whose ultimate owner is based in Beijing has become to Myanmar's public debate.

Chinese companies' involvement in Myanmar's digital payments industry is another aspect of China's presence in its neighbor's application layer. Two of Myanmar's most used digital payment apps, KBZPay and Wave Money, have a Chinese connection. KBZPay, a product offered by Myanmar's largest private bank, was developed in partnership with Huawei in 2018.[226] The Chinese tech giant further supported KBZPay with a digital payment cloud in August 2020. The system had 6 million users in the country in October 2020.[227] In May 2020, another very successful digital payment system, Wave Money, received a US$73.5 million investment from Ant Financial, the fintech arm of the Alibaba group.[228] However, these investments took place before the February coup "pushed [Myanmar's] fledgling digital economy to the brink of collapse."[229] The repeated internet shutdowns, combined with people's reluctance to abandon hard cash in times of instability, set the country's digital payments' sector back years. For instance, by August 2021, Wave Money had lost half of its users.[230]

Whereas Chinese companies have a commanding presence in the infrastructure and device layers of Myanmar's digital stack, they are playing catch-up in the apps layer. TikTok is the lone Chinese success story, especially among Myanmar's youth. However, like Facebook before it, TikTok's success in Myanmar also exposed its inadequate content moderation practices. Its temporary transformation into a hub for the military's propaganda showed the risks that come with having a Chinese social media app in an influential position in countries where democracy is under attack.

The Content Layer

Burmese perceptions of China are conflicted. On the one hand, much of the country's economy relies on Chinese trade and ties with Chinese companies. On the other hand, China's support for the military junta in the '90s and its involvement in environmentally damaging projects like the Myitsone dam have bred widespread resentment.[231] This explains why the Chinese state has enrolled its diplomats, officials, and media to improve public perceptions of China in Myanmar.

An October 2019 investigative piece by Myanmar Now explained that "a dozen social media pages and media organizations [are] publishing China-friendly news and programs."[232] The investigation gave precise examples of the many pro-China stories running in Myanmar, most notably a Xinhua-produced advertorial for the BRI that was widely republished but only clearly labelled as an advertorial by a single outlet, and even that one had a content sharing agreement with the ultra-nationalist Chinese tabloid Global Times. It is not only newspapers, as illustrated by Myanmar International, a joint project launched in 2010 by Myanmar's Ministry of Information and Shwe Than Lwin Co. Ltd, a "large enterprise closely linked to the military."[233] In July 2018, the head of China's Propaganda Department personally visited the offices of Shwe Than Lwin Media and Myanmar International's radio offshoot.[234]

Pro-Chinese interest groups also promote pro-CCP narratives on the non-Chinese social media platforms that are dominant in Myanmar. Chinese propaganda articles about Hong Kong protests were reproduced on the Facebook pages of several Burmese media outlets.[235] However, since the February 2021 coup, the military has clamped down hard on the press, including on outlets with which Chinese state media had worked, potentially threatening to undo much of China's efforts in Myanmar's media sector.[236]

In parallel to China's influence on media outlets, the Chinese state has also organized trips and trainings for Myanmar journalists. A December 2019 German report estimated that "hundreds" of Myanmar journalists had visited China on state-sponsored programs.[237] Myanmar Now added that those selecting the reporters ensured

that they would be receptive to their host's message as critical journalists were deemed to be "a waste of money."[238] Indeed, journalists who choose to investigate Chinese investment projects in a critical way run the risk of being arrested, or worse.[239]

Chinese diplomats in Myanmar keep a comparatively low profile. The Chinese ambassador in Naypyidaw does not have a Twitter account. However, the Chinese embassy in Myanmar has the third most followers out of all Chinese representations abroad on Facebook.[240] Many of their posts are boilerplate statements by the embassy or the ambassador in the aftermath of the coup wishing the Myanmar people well and looking forward to a peaceful resolution of the situation in the country.[241] The reactions to these posts are very clear: the dominant emojis are laughter and anger, and the comments range from "SHAME ON CHINA, GET OUT FROM MYANMAR" or "#BoycottChineseGoods" to even coarser expletives.

Despite its significant efforts to coax Myanmar's public opinion, the Chinese state still struggles to find its footing in the country's information space. After the coup, the ambivalent treatment anti-military protesters received in Chinese state media (outward facing coverage cast it as a "cabinet reshuffle" while domestic coverage inside China was far more critical of the Tatmadaw) further damaged Beijing's image with Myanmar's population.[242] Perceptions of China reached such lows that Beijing reportedly pressured the junta to do more to silence anti-Chinese media content.[243] That did not stop angry protesters from torching Chinese factories in Yangon, which Chinese state media promptly attributed to sinister "proxies of the West."[244]

The Chinese state seemed to be making progress in the content layer of Myanmar's digital stack pre-February coup. But, as in other layers, the military's brutal power grab has derailed Chinese plans. Some commentators have speculated that China was to some extent manipulated by the Tatmadaw into siding against the protesters, a position that has objectively hurt its interests in the country.[245] In addition, many of the media outlets the Chinese state worked with in the past are now under threat. Still, Beijing could strengthen its position in Myanmar's content layer should the military succeed in asserting full control over the country's information space.

The Governance Layer

The final dimension of Myanmar's digital stack, the governance layer, is the one where Chinese influence is hardest to assess. The current military government is just as oppressive, if not more so, as the authorities in Beijing. The radical measures passed by the Tatmadaw since February 2021 have largely superseded whatever role the Chinese state and Chinese companies played in defining the framework for Myanmar's information space prior to the coup.

Even before its brutal power grab, the military government laid the groundwork to seize control of Myanmar's entire digital stack. In May 2021, Reuters revealed that, in the months preceding the coup, several officials allied to the military had started pressuring telecom and internet service providers into installing "intercept spyware that would allow the army to eavesdrop on the communications of citizens."[246] After the coup, pressure ramped up with the express passage of a new Cybersecurity Bill that echoed the regulatory framework of China's digital stack. It required online service providers to keep a broad range of personal data on all their users that the authorities could request at any time. This obligation came with data localization requirements, ensuring that nothing could be stored in jurisdictions beyond the Tatmadaw's reach.[247] It contained broad provisions on loosely defined "misinformation and disinformation" that would allow the authorities to censor any content they deemed undesirable, as well as heavy penalties for those who shared that content. It also restricted the creation of

"fake" accounts, removing online anonymity and essentially ending freedom of expression on the internet.[248]

Besides the Cybersecurity Bill, the most damning evidence of the Tatmadaw's imitation of the Chinese model of digital governance comes from February 2021 reports that China was providing "technical assistance so the Burmese military can develop a cyber firewall similar to the Great Firewall."[249] According to these reports, which the Chinese embassy vehemently denied, China provided IT technicians and hardware to help the military stamp out the pro-democracy movement online. Over the summer, Telenor's refusal to abide by new regulations and its reluctance to deploy intercept spyware in its networks was a key factor in the Norwegian telecom operator's decision to pull out of Myanmar.[250] However, Reuters also reported that Ooredoo had not fully complied with the military's requests. Given that part-Chinese state-owned ZTE runs Ooredoo's mobile network since 2020, the operator's reluctance to deploy the Tatmadaw's intercept spyware shows that Chinese technological assistance only goes so far in swaying companies in anti-democratic directions.

As the consequences of the February coup continue to ripple through Myanmar, the governance layer of the country's digital stack has gone down the most autocratic path imaginable. The similarities between the draconian provisions in the Tatmadaw's new Cybersecurity Bill and its Chinese counterpart are undeniable. The reported involvement of Chinese technicians in helping set up Myanmar's version of the Great Firewall provides further evidence of China's role in molding its southern neighbor's autocratic digital stack. All this suggests that the Chinese approach to digital governance will be difficult to turn back in Myanmar.

Conclusion

Each layer of Myanmar's digital stack reveals varying levels of success for the Chinese state and Chinese companies. From Huawei collecting the identification information of anyone with a SIM card, to Chinese companies manufacturing over half the smartphones sold in the country despite many citizens' displeasure with China's perceived support for the coup, Chinese actors are now entrenched in Myanmar's infrastructure and device layers. By contrast, Facebook's towering presence in the country's app layer and the widespread availability of anti-Chinese content in Myanmar's information space are hurdles for China in other parts of Myanmar's digital stack.

The February coup has had mixed effects. On the one hand, the Tatmadaw is pushing non-Chinese rivals out of the telecom sector and its media clampdown could strengthen China's hand in the country's content layer. On the other hand, the coup has wiped out the entire digital payment industry in which Chinese companies were very successful and has provoked violent attacks on Chinese business assets in Myanmar. For now, Beijing is still in touch with the opposition and has not fully embraced the Tatmadaw.[251] However, the Chinese state is helping the military establish complete control over Myanmar's digital stack. Even if the Tatmadaw were to give way to a less overtly autocratic government, the digital architecture set up with China's help will constrain civil liberties and political rights in Myanmar for the foreseeable future.

Uganda

Executive Summary

In recent years Western countries have been very critical of the Ugandan government's crackdown on political opponents and of legislation that targets the country's LGBT+ community. The Chinese government has used these periods of elevated criticism or threat of sanctions as opportunities to provide more loans for infrastructure across Uganda. Often these loans have been used to fund infrastructure built by Huawei, which has helped several Ugandan entities spy on the communications of political opponents and has reportedly established a surveillance network in major cities across the country. Additionally, China's ownership of satellite subscription television services like the Star Times gives the CCP a means to broadcast programming that aligns with its strategic goals.

China's role in developing Uganda's digital information stack provides it with points of leverage at each layer:

- In the network infrastructure layer, Uganda's National Data Transmission Backbone Infrastructure (NBI) and Electronic Government Infrastructure (EGI) were financed by the China Import-Export Bank and constructed by Huawei.
- In the device layer, Huawei has deployed surveillance hardware across Uganda, and aided Ugandan security forces in using it to track political opponents.
- In the application later, Chinese firms have supplied most of the software on which the Ugandan government operates.
- In the content layer, China produces news and entertainment aimed at African audiences, often crafted to support pro-China narratives and elevate authoritarian leaders with whom they work, including Ugandan President Yoweri Museveni.
- In the governance layer, China is investing in the human capital of Uganda through educational programs and scholarships, generally aimed at encouraging both brand and ideological loyalty among Ugandan students, workers, and elites.

Through these five avenues of leverage over Uganda's digital future, China has positioned itself to support one of its favored strongmen, while Museveni makes himself ever more beholden, both financially and practically, to the Chinese government and the firms through which it operates.

Overview of Sino-Ugandan Relations

The People's Republic of China was one of the first countries to establish formal relations with Uganda after its independence from Britain in 1962.[252] Nine years later, Uganda voted in favor of Resolution 2758, which transferred China's representation at the UN from Taipei to Beijing. After President Museveni seized power in 1986, relations between China and Uganda improved further, as Museveni actively courted Chinese investment in infrastructure and industry and encouraged China's growth as a major export market for Ugandan goods. In 2019, bilateral trade reached nearly US$800 million, with China selling US$741 million of goods in Uganda (mostly manufactured goods, including electronics, industrial equipment, and apparel) and Uganda selling US$40 million of goods in China (chiefly agricultural products).[253]

In many ways, China has been a partner of convenience for Museveni's decades-long regime. Once a hero in Western capitals for his armed resistance to the brutal dictatorships of Idi Amin and Milton Obote and his promises to restore democracy to Uganda, Museveni gradually alienated many Western governments through his authoritarian, one-party rule and disregard for human rights, particularly in recent years the persecution of his country's LGBT+ community.

A particularly harsh anti-LGBT+ law in 2014 led many Western governments to review or terminate direct aid to the Ugandan government. Museveni replied confidently that his country would prosper without Western aid,[254] and experts at the time speculated that he would aim to replace Western aid and investment with Chinese projects.[255] Indeed, Chinese FDI in Uganda leapt from US$60.5 million in 2013 and 2014 to US$205.3 million in 2015 and averaged US$145.4 million/year from 2015-2020. Chinese investment has supported a wide range of projects, including two hydroelectric power stations, several major highways, and the Mandela National Stadium outside Kampala.

In 2021, Museveni was inaugurated to his sixth presidential term after elections that were marred by fraud, voter intimidation, and the use of state security forces to prevent political organization by Museveni's opponents. Western governments criticized the conduct of the elections, while Museveni himself accused civil society and aid organizations of conspiring against him and has organized a crackdown on foreign groups operating inside the country.[256] Given how Museveni's regime has responded to tensions with the U.S. and Europe in the past, it is likely that Uganda and China will draw even closer together to offset lost aid and investment opportunities.

Still, relations between Uganda and China are not without their own challenges. Alarm bells went off across the African continent earlier in 2021 when media outlets reported that China might take possession of Entebbe International Airport in response to non-payment of loans from China's Export-Import Bank.[257] Both China and Uganda have downplayed those reports, but the mortgaging of Ugandan infrastructure and natural resources as collateral for Chinese loans remains a political liability for Museveni's government (and many others across the continent), as does the use of Chinese workers to construct many of these projects.[258] The racism and discrimination faced by African immigrants in China constitutes another source of friction between the Ugandan and Chinese governments, one that has grown worse since the start of the COVID-19 pandemic.[259]

The Network Infrastructure Layer

Uganda has relatively low mobile phone access compared with its neighbors and extremely poor wired internet availability.[260] As of 2020, 46 percent of Ugandans were internet users, with mobile handsets accounting for 99.86 percent of connections.[261] This extremely heavy reliance on LTE and other wireless approaches to high-speed internet leaves the country highly dependent on its wireless infrastructure, much of it built by China, for the functioning of its entire society and economy.

China has no full-service data centers in Uganda. Instead, China Unicom maintains a single "point of presence" center in Kampala.[262] This facility serves to connect Uganda's network to China Unicom's global network. But Chinese firms have invested substantially in other aspects of Uganda's network infrastructure, including in fiber optic networks. The first of these major investments came in 2003 when ZTE partnered with African telecoms consortium Comtel to build a fiber optic network linking the Common Market for Eastern and Southern Africa (COMESA), which included installing miles of fiber optic cable across Uganda.[263][264]

Only three years later, in 2006, Huawei signed a US$106 million deal with the Ugandan government to build the country's National Data Transmission Backbone Infrastructure (NBI) and Electronic Government Infrastructure (EGI), comprised of 2,500 miles of fiber optic cables, and financed by a loan from China's Import-Export Bank.[265][266] That project has faced controversy, with Museveni harshly criticizing Huawei in a 2012 letter for using substandard hardware and overcharging the government, and a subsequent government probe ultimately supported the accusation, faulting both Huawei and Ugandan regulators for the mistakes.[267] Nevertheless, the NBI/EGI became operational in 2014 and remains the core of Uganda's national fiber optic infrastructure.[268] Huawei also partnered with Uganda Telecom, the state telecommunications firm, in 2007, to add up to 300 base stations to the latter's network, at a price of US$50 million.[269]

After 15 years of Huawei leading network infrastructure development in Uganda, ZTE announced in 2020 that it would be partnering with MTN Uganda to deploy East Africa's first stand-alone (SA) 5G network.[270] The system is expected to heavily feature ZTE hardware and could make Uganda the third country in Africa with SA 5G, after South Africa and Nigeria.[271]

The Device Layer

Chinese investments in network hardware in Uganda have not been limited to fiber optic cables or 5G broadcast systems—Chinese firms have also secured contracts to invest in security and surveillance hardware for the Museveni government. In 2008, the Ugandan Ministry of Security announced that it was deploying the Tetra Communications System, which facilitates communication between police, army, intelligence, and other security personnel. Though Tetra is manufactured by Motorola, the Ugandan government financed the project with US$5 million from the US$106 million Ex-Im Bank loan for NBI/EGI, under an agreement in which Huawei would implement the technology.[272]

In 2014, Huawei gave 20 security cameras to the Ugandan government,[273] and in 2017, as part of China's Belt and Road Initiative (BRI), augmented its surveillance system by deploying pan/tilt/zoom (PTZ) surveillance cameras along 40 roads in Kampala, along with network video recorders (NVR) to store and process the content.[274] This surveillance system was confirmed by Ugandan police in 2019 to be a fully integrated Huawei Safe City.

Reporting by the Wall Street Journal has since found that the system was used on multiple occasions at least as early as 2017 by Ugandan intelligence officers to spy on opponents of the regime.[275] In one instance, Ugandan police asked Huawei technicians working in Kampala for help decrypting the WhatsApp messages of Ugandan opposition activist Bobi Wine.[276] In 2018, Wine had been dragged from his car and beaten by Ugandan security forces in the lead up to an election; his driver was fatally shot.[277] In the wake of street protests in 2020, Ugandan police have admitted to using the facial recognition tools in Huawei's Safe City surveillance system to track and arrest dissidents and protest leaders.[278] According to Museveni himself, "Kampala Metropolitan alone has 83 monitoring centres, 522 operators under 50 commanders" as of 2020,[279] and Uganda has contracts with Huawei to deploy facial recognition technology throughout the country.[280]

In a country where nearly all internet users use mobile devices to reach it, and where security forces eagerly engage in the surveillance of perceived political threats, the security of consumer devices is particularly important. The Ugandan mobile phone market is relatively fragmented, with the four market leaders—Tecno, Samsung, Infinix, and Apple—capturing only 29.8 percent, 18.9 percent, 11.0 percent, and 6.9 percent of the market respectively.[281] Well known Chinese phone makers Huawei and Xiaomi have 3.1 percent and 2.6 percent of the con-

sumer mobile phone market. Unfortunately, the market leader, Tecno, is a Chinese firm with a history of poor device security. A low-cost phone provider, it has historically used outdated Android operating systems known to be vulnerable to a wide range of exploits.[282] In 2020, the anti-fraud firm Upstream discovered malicious code on tens of thousands of Tecno smartphones sold in countries across Africa (although Uganda was not identified to be among them).[283]

The Application Layer

Like internet users around the world, Ugandan consumers use a wide range of applications produced and licensed by Chinese firms like Alibaba, ByteDance, Tencent, and Baidu. But the Ugandan government also relies on a wide range of Chinese software products, including the surveillance and video processing software provided and maintained by Huawei, as well as the government networks built as part of the EGI contract from 2006. Though the details of the Ugandan government's contracts with Huawei are not known, such arrangements generally involve substantial long-term maintenance and support, without which the products are useless. This gives Chinese firms a substantial hold over regimes like Museveni's that invest heavily in surveillance-based security approaches to maintaining their hold on power.

The Content Layer

As smartphones have proliferated across the country, the demand for content aimed at Ugandans has grown dramatically. Chinese firms have sought to meet this demand, with a particular focus on news and information. This has led to many content-sharing agreements between Chinese firms and Ugandan media groups. Among the most prominent of these has been that between PML Daily, a major Kampala-based news website, and Xinhua News.[284] Such agreements can be mutually beneficial: PML Daily gets unlimited license to republish and distribute Xinhua's stories, providing more content to readers while reducing the burden on its staff, while China dramatically expands its media penetration in Uganda, allowing it to promote narratives favorable to Chinese interests.

China has also worked to expand its presence on Ugandan television. In some cases, it has done this through traditional broadcast agreements that have allowed regionally focused Chinese networks, like CGTN Africa, to garner substantial viewership in Uganda. But another Chinese firm, Star Times, has taken a more novel, two-pronged approach to developing its viewership. In Kampala, Star Times offers paid subscriptions to customers for a wide range of content including not only news, but sports and entertainment. At the same time, they provide free satellite TV to thousands of villages across the region through a Chinese program called Access to Satellite TV for 10,000 African Villages.[285] Through this program, the nominally private Star Times is paid hundreds of millions of dollars by China to create new customers in remote regions of Uganda previously unserved by any TV providers.

Once in place, content distribution networks promote stories and narratives that frame Chinese investment projects in Africa favorably and advance a pro-China worldview with respect to global affairs. Many such stories are fundamentally benign, like a popular Xinhua story about a Ugandan teacher and Chinese construction foreman who married after meeting as a result of the BRI, but are promoted to favorably dispose Ugandan readers to future Chinese projects.[286]

Some information manipulation is much more malevolent, and a major focus of Chinese information manipulation efforts over the past two years has been the global COVID pandemic. Chinese media outlets have pushed back strongly against any suggestion of Chinese responsibility for the pandemic, going as far as to push conspiracy theories blaming American military laboratories.[287] State-backed news agencies, like the China Daily, play up cooperation between China and Uganda on COVID vaccination, using China's "vaccine diplomacy" to frame China as a responsible world leader, and a partner for Uganda's government.[288]

Outside the realm of COVID, Chinese news agencies with readership or viewership in Uganda also push support for the regime since it has been a convenient partner for the CCP. This includes stories by CGTN Africa framing Museveni as a regional leader on economic and political integration.[289] Even more problematically, Chinese news agencies have worked to legitimize Museveni and Uganda's authoritarian political system through stories that validate his election victory and ignore or downplay allegations of fraud and intimidation. Through content sharing agreements, these stories are seen by many Ugandans on Ugandan news websites with few clear indications they come from Chinese media firms.

The Governance Layer

Ultimately, Chinese ambitions in Uganda are much greater than just shaping the media and technology environment favorably to their own narratives. Chinese foreign policy aims to spread a model of digital governance that enshrines state surveillance, censorship, and media control as a global norm. In Uganda, this means training and educating new cohorts of Ugandan police, intelligence officers, civil servants, and technical experts in the way the Chinese government and Chinese firms do business.

Just as in the infrastructure space, Chinese firms represent the tip of the spear when it comes to human capital development abroad. In Uganda, Huawei has established an ICT Academy in partnership with Kampala International University.[290] These institutions train local students in ICT skills, while promoting the use of Huawei's products. This helps build long-term brand loyalty among the country's technical experts, while ensuring an ample supply of technicians trained on Huawei equipment for the company's future maintenance and installation workforce. Huawei has also partnered with Makerere University and pays for Ugandan students to travel to China for specialized ICT training.

But Chinese interest in training young Ugandan professionals goes far beyond the technical realm. China has also begun providing training to Ugandan police and intelligence officers on subjects like "criminal intelligence" and "cybercrime," often with an emphasis on technological solutions.[291] The benefits to such partnerships, carried out both by the Chinese government directly and through private state-backed firms like Huawei, are clear: China enhances the capacity of a state security force that protects a regime that is friendly to Beijing, while making that regime and its security force both grateful and beholden to the Chinese government, all while normalizing the heavy-handed approach to surveillance and political control that China favors.

A third prong of strategic Chinese investment in Ugandan human capital development targets the country's elite and aims to promote attitudes favorable to China, and to close relations between Uganda and China, among the former's future economic, social, and political leaders. The Chinese ambassador in Uganda periodically announces new rounds of scholarships for Ugandan university students to study in China.[292] China opened its first Confucius Institute at Makerere University in 2014, where students can learn Chinese and participate in cultural exchanges, but also where the Chinese government can promote a pro-China worldview and conduct various

forms of public and non-public diplomacy. China also sponsors joint think tanks and regional fora aimed at influencing the attitudes of more senior scholars, journalists, and officials, often bringing them to Beijing for conferences.[293]

Conclusion

The future of Uganda's relations with China, and Uganda's future generally, are uncertain and will depend on the political durability of Museveni's National Resistance Movement, as well as the physical health of Museveni himself. Uganda has a vibrant political opposition, but security and intelligence forces loyal to the regime, now backed by Chinese technology and expertise, have been effective at keeping them away from power. A political transformation in Uganda could substantially alter Uganda's diplomatic orientation towards China and make the country more skeptical of the ownership China is establishing over its physical and digital infrastructure and natural resources. On the other hand, continued one-party rule could allow China to deepen its relationship, including its points of leverage over Uganda, turning the country into an outpost of Chinese influence in East Africa.

Nigeria

Executive Summary

Data and cyber sovereignty have gained significant political salience in Nigeria over recent years as President Muhammadu Buhari and his government seek to silence critics using Western social media platforms like Twitter. The Nigerian government has also expressed concern over the possibility of the United States and other Western governments accessing Nigerian data stored in centers in North America and Europe. Additionally, Nigeria's place in Sub-Saharan Africa as a hub for entertainment and other forms of media make it strategically valuable for Chinese information control. China has invested considerable resources into building up Nigeria's entertainment hub "Nollywood" and several Chinese news outlets maintain bureaus in Lagos and Abuja.

China's role is visible at each level of Nigeria's digital information stack, giving it potent leverage over Nigeria's society and economy:

- In the network infrastructure layer, Nigeria is heavily reliant on undersea cables that run along the West African coast, several of which are partially owned by Chinese firms or were constructed by Huawei Marine.
- In the device layer, China has supplied CCTV cameras, Huawei Safe City hardware, and other surveillance technology to Nigerian police and security forces.
- In the application layer, China has furnished Nigeria with sophisticated oil and gas drilling sensors and management systems, giving Chinese firms leverage over and insight into Nigeria's chief exports to China.
- In the content layer, China has invested in the Nigerian film industry and seeks to use Nigeria as its African hub for cultural exports, including news and entertainment.
- In the governance layer, China has encouraged Nigeria to pursue a path of substantial government control over the internet and over its citizens' data.

Nigeria is by far the most populous country in Africa and one of the most populous democracies in the world. But domestic challenges and democratic backsliding have given China opportunities to encourage and facilitate censorship and surveillance by Buhari's government, while turning Nigeria into an outpost of Chinese cultural influence in the region.

Overview of Sino-Nigerian Relations

Nigeria and China mark 50 years of formal diplomatic relations this year, with Nigeria having switched recognition from Taipei to Beijing in 1971 with UNGA Resolution 2758. Over the past five decades, China has become one of Nigeria's most important economic partners, while Nigeria has become one of the most pro-Beijing countries in the world. The two countries strengthened their relationship particularly during the most authoritarian periods in Nigeria's political history, as Nigeria has faced opprobrium from democratic governments and skepticism from Western companies looking to invest. As of 2019, China and Nigeria have annual bilateral trade of over US$18 billion, including over US$1.1 billion of oil purchased by China that year.[294] The largest single Chinese export to Nigeria is, significantly, telecommunications equipment, which speaks to the dominant feature of China-Nigeria trade today: digital infrastructure for oil.

This partnership is not equal, though, and the enormous economic leverage China possesses can be used to coerce political concessions, as when in 2017 Nigeria asked Taipei to move its representative offices out of the capital, Abuja, one day after Beijing had announced a US$40 billion investment package for the country.[295] Investment is a particularly effective tool of leverage because Nigeria has the largest population in Africa by far, as well as enormous natural resources, which together generate an voracious hunger for capital. This includes major infrastructure investments made through the BRI into at least three railroads and four airports, in addition to other investments in highways, power stations, and other projects essential to the development of the Nigerian economy.[296] But Chinese investments into Nigeria's telecommunications infrastructure have been particularly substantial, and include undersea cables, data centers, wireless and fiber optic data networks, internet exchange points, and even Smart City monitoring and surveillance hardware.[297] Much of this investment takes places under the auspices of the Digital Silk Road as well as the China-Africa Internet Development and Cooperation Forum.[298]

The biggest stumbling blocks for relations between Nigeria and China have concerned the treatment of Nigerians at the hands of Chinese, both in China and Nigeria. During the COVID-19 pandemic, Chinese authorities imposed harsh lockdown protocols on African immigrants living in the country, at times more severe than those imposed on Chinese nationals.[299] In the past, the abuse of African immigrants, many of them Nigerian, by Chinese police, as well as discrimination by Chinese businesses and eviction by housing authorities, have caused tension between the two governments.[300] Nigerians also face abusive labor practices working for Chinese firms in Nigeria, with many allegations of bribes paid to ensure that Nigerian authorities do not enforce the rights of Nigerian workers.[301] Another major source of tension is the disruption that Chinese imports have caused in the Nigerian economy. Cheap textiles and light manufactured goods from China have decimated those domestic industries in Nigeria, with low-quality Chinese goods often pushing out higher quality but more costly domestic or European alternatives.[302] Despite each of these areas of friction, Nigerians remain among the most pro-Chinese population in the world, with one poll finding that as many as 80 percent of Nigerians had a favorable opinion of the country.[303] Pew Research found that Nigerians who lived near major BRI projects had an improved opinion of China.[304]

The Network Infrastructure Layer

Nigeria's internet is primarily reliant on undersea fiber optic cables that carry signal to Europe and North America. China first began investing in these cables with the South Atlantic-3/West African Submarine Cable (SAT-3/WASC), which came online in 2001. China Telecom and PCCW, based in China and Hong Kong, respectively, are both partial owners of the cable.[305] Both companies are also partial owners of the West African Cable System (WACS), which has been in use since 2012.[306] This project was implemented in part by HMN Tech (then known as Huawei Marine), also a Chinese firm. HMN Tech also built an additional cable, the Nigeria Cameroon Submarine Cable System (NCSCS), which became active in 2015.[307]

Though undersea cables can seem like content neutral pipes over which the builder has little lasting control, ongoing involvement including hardware maintenance, traffic management, and other services mean that owners and builders of such infrastructure can have tremendous leverage over users. The threat that this poses has been deemed serious enough that other projects implemented by HMN Tech have been abandoned over security concerns raised by the U.S. In Nigeria's case, three of its six operational submarine cables have Chinese ownership (SAT-3/WASC, WACS, NCSCS) and three do not (MainOne, GLO-1, ACE).[308] Presently, data rates in Nigeria are approximately equal to 1/50th the rates in North America, which means that little excess capacity exists, which in turn means that any interruption to data service along cables with Chinese ownership would have crippling effects on communication and commerce in Nigeria.

To carry the network from the undersea cables' terminals in Lagos to consumers, Nigerians rely on a large terrestrial network of wired data centers and internet exchange points (IXPs), as well as wireless broadcasting systems. Much of this network has been built by two Chinese firms with close ties to the CCP: Huawei and ZTE. The first such project came in 2002, when Huawei and ZTE both took contracts from a US$200 million China Import-Export Bank loan to finance the provision of telephone access to 218 rural communities in Nigeria.[309] The 20 years since have been a race between the two firms. In 2004, Huawei signed an US$80 million contract with VMobile to expand the country's Global System for Mobile Communications (GSM) network.[310] The following year, Huawei signed a US$200 million deal with Nigeria's Ministry of Communication to develop the country's CDMA450 system, a lower frequency cellular network.[311] In 2006, ZTE won a US$100 million contract to implement the third phase of Nigeria's National Rural Telephony Project, as well as the right to complete some unfulfilled obligations of Huawei's 2002 contract. Alcatel-Lucent Shanghai Bell and Huawei also participated in this project.[312] Both firms signed contracts in 2007 to update the country's internet switching capacity, and ZTE signed a further US$5 million deal in 2008 to set up a global trunking architecture (GoTA) in the country.[313]

Over the past decade Huawei has dominated the high-profile network infrastructure projects in Nigeria. Since 2011, Huawei has collaborated with the Emirati telecoms firm Etisalat to expand their data service across 18 countries, including Nigeria, and in 2018 it secured a US$318 million loan to expand broadband across the north of the country.[314][315] The same year, MTN Nigeria and Huawei announced that they had jointly completed the Rural Star 2.0 mobile network, which uses solar powered antennae to carry voice and data to remote Nigerian communities.[316] In 2017, Airtel Nigeria had announced that it would be deploying 4G service in many parts of Nigeria, mostly using equipment supplied by ZTE.[317] Two other Chinese firms, China Telecom and China Unicom, maintain "points of presence" (PoPs) at data centers within Nigeria in order to more directly link their networks to the country's.[318]

The Device Layer

Chinese investment into more visible elements of Nigerian digital infrastructure began in 2010 with an agreement for ZTE to install 2,000 solar-powered CCTV cameras in Abuja and Lagos. The project was funded with a US$470 million loan from China's Import Export Bank and came to include partnerships with the Nigerian ministries of Finance and Police Affairs.[319] Such agreements, which involve the deployment of visible and expensive-to-maintain new tools for law enforcement and intelligence services, often serve as a first foot into the door for Chinese firms with African governments. Cameras require ongoing maintenance and support, ensuring a continued presence for ZTE, while police and other security forces hopefully become brand-loyal advocates for future partnerships.

In 2016, Huawei signed a deal to make Calabar Nigeria's first smart city,[320] and the following year announced a partnership with the Nigerian Ministry of Communications to deploy smart city technology in cities around the country.[321] In 2018, Huawei announced a US$1.5 billion fund to expand smart city deployment across Africa, with Nigeria identified among the markets it sought to develop. These projects promise benefits to efficiency and connectivity but also offer security forces tools for surveillance, and they provide Huawei substantial leverage over local governments that come to depend on the ongoing services required to support them. In the case of Nigeria, a fragile democracy with a history of military dictatorship as well as several active insurgencies, there is a risk that tools acquired under a public safety or counterterrorism framework will be misused for political purposes.

Because nearly all Nigerian internet users reach the internet via mobile devices, the manufacture and distribution of handsets constitutes an additional major vulnerability at the device layer of the stack. Chinese phone makers control nearly half the Nigerian handset market, with Tecno and Infinix controlling 26.2 percent and 23.6 percent of the market, respectively (Samsung and Apple follow with 10.4 percent and 9.8 percent, respectively).[322] Tecno and Infinix have both faced allegations that their devices have shipped with malware pre-installed and are generally considered among the least secure devices available.[323] This leaves Nigerian consumers vulnerable to fraud and exploitation, but also potentially to censorship or surveillance by either the Nigerian or Chinese state.

The Application Layer

Nigerians use many Chinese software platforms for a range of personal, commercial, and industrial purposes, like internet users in nearly every country. This creates a huge range of potential vulnerabilities across Nigeria's society and economy. Among average Nigerians, TikTok has been the runaway success, as it has in many countries, with 31.9 percent of Nigerian internet users using the app as of 2020.[324] This allows ByteDance to gather an enormous amount of data on Nigerian users, which can be used for a wide range of political and social engineering purposes.

Of particular importance to Nigeria have been suites of oil production and distribution management software produced by Huawei.[325] Such platforms can generate substantial efficiency gains by sending petroleum products where they are most needed or will fetch the highest price, cutting off fuel flow in the case of a leak or fire, finding exploitable reserves underground, and many other important services. They can also serve to detect and deter oil and gas theft, a multi-billion-dollar problem in Nigeria.[326]

But reliance on these systems creates a further vulnerability by tying the Nigerian oil industry tightly to Chinese industries closely involved with the CCP. For one, it gives China enormous visibility into the inner workings of the one of its chief suppliers of oil, a market advantage of potentially enormous value. It also carries with it the implicit threat of disruption since Chinese firms hold an unknown degree of power over industrial control systems across Nigeria's oil fields. This makes Chinese digital hardware in the oil industry a point of strategic leverage, just like its involvement in Nigeria's network infrastructure.

The Content Layer

In recent years, China has dramatically increased the amount of content that it produces aimed at African audiences. Nigeria has been key to these efforts because its large population and well-established media industry give it cultural weight across Africa and among the anglophone African diaspora. In recent years, this has included collaboration between the Chinese movie industry and "Nollywood," Nigeria's own filmmaking establishment, and even a joint Nigerian-Chinese feature film, *30 Days in China*.[327] Nigeria also features prominently in China's cultural outreach to Africa because Nigerians broadly approve of China, giving Chinese cultural products a viable market. This offers China opportunities to promote narratives favorable to its own worldview and actions in Nigeria, and among consumers of Nigerian media abroad.

More often than directly collaborating with Nigerian media, Chinese news groups secure content sharing agreements that allow them to run their stories on Nigerian websites, often under the mastheads of Nigerian news outlets. In 2017, Nigeria's Federal Ministry of Information and Culture signed a memorandum of understanding on information exchange with China's State Council Information Office aimed at facilitating media cooperation

between the two countries.[328] This allows Chinese state media to influence Nigerian state media, and through it the entire Nigerian news ecosystem, in ways it finds convenient. China also promotes its own state media through CGTN Africa, which now maintains a Lagos Bureau, and which is available in Nigeria on DSTv, a satellite TV service based in South Africa, and on Star Times, a Chinese multimedia group now available by subscription in dozens of African countries.[329]

China also works to shape the information space and influence narratives through its state-backed social media operations. This is most often content from Chinese diplomats or state-backed news outlets promoting the local benefits of Chinese-backed infrastructure projects.[330] In some cases though, state-backed news agencies will promote a more openly ideological agenda, as when Xinhua invited a political scientist from Nigeria's Center for China Studies onto its program to discuss, essentially, why the CCP represents an ideal model for governance that should be emulated around the world.[331] In recent years, Chinese state-media has generally reported positive stories about Nigerian President Buhari, who has sought to deepen ties with China, which in turn serves to further ingratiate Chinese media with the Nigerian authorities while strengthening the hand of a broadly pro-China leader.[332]

The Governance Layer

China is also deeply invested in shaping the governance of digital spaces in Nigeria, which will have implications for both the political future of Nigeria and for the norms of digital governance around the world. By establishing norms in Nigeria favorable to state control, censorship, and surveillance, China hopes to strengthen authoritarian tendencies within the country and to entrench the power of pro-China politicians and political constituencies into the future. They also hope this will transform Nigeria into an advocate for a permissive global regime when it comes to government control over digital spaces.

It was no doubt a source of great excitement among Chinese authorities, therefore, when earlier this year President Buhari banned Twitter in the country after the company deleted one of his tweets, which appeared to threaten violence against the Igbo people of southeast Nigeria.[333] Since then, Buhari has relented and "conditionally" allowed Twitter back into the country, but the suspension has served to normalize state control over social media spaces, and reflects the approach taken by China to digital fora.[334]

A particular concern for Buhari's government in recent years has been "digital sovereignty," which the regime casts in terms of protecting the rights of Nigerians from foreign governments or corporations. To this end, Nigeria established the Nigeria Data Protection Regulation (NDPR) in 2019, which among other things requires that certain types of data on Nigerians be held in Nigeria.[335] Unfortunately, laws like this that establish major government regulation over privately held data can also be used by the regime to surveil or appropriate that data. China, too, framed its recent Personal Information Protection Law and Data Security Law in terms of protecting users' rights to privacy.[336]

More recently, Buhari's government has sought to establish even greater control over Nigerians' internet access by means of a "Great Firewall" modelled on China's own. Nigerian authorities have met with the Cyberspace Administration of China in 2021 to explore the possibility of using deep packet inspection and other advanced technologies to block entire sections of the internet from Nigerian users, including those using proxies, VPNs, and other workarounds.[337]

Conclusion

Strategic investment by Chinese tech giants into the deep infrastructure of Nigeria's network, especially into wireless transmitters and submarine cables, gives China potentially enormous leverage over the country. Firms like Huawei and ZTE have virtually guaranteed themselves a role in managing and administering the country's hardware networks for years to come, despite their demonstrated subservience to the CCP and its political aims. Because China perceives its interests to be well served by the spread of authoritarianism, this represents a dire threat to Nigeria's faltering democracy. Because Chinese firms are involved in the development of every layer of the digital stack in developing countries like Nigeria, eliminating the threats of Chinese espionage, coercion, and manipulation is no easy challenge. Compromises to hardware and software can both take years to uncover, and Chinese influence in Nigerian training programs, curricula, and exchange programs can be even more insidious.

Unfortunately, Nigeria's government remains cautious about cooperation with liberal democracies and eager to use China as an alternative source of aid, investment, and political support. As the current regime takes steps to undermine freedom of speech and other democratic norms, the risk that Nigeria reverts to dictatorship and falls even more into China's orbit increases.

Jamaica

Executive Summary

Jamaica serves as a staging ground for PRC investments across the Caribbean region. Jamaica is a BRI signatory and has received several infrastructure investments ranging from transportation to its digital information stack. However, U.S. sanction actions targeting Chinese companies have curbed their investment in Jamaica's ICT sector.

The relationship between Jamaica and the PRC is visible in the various layers of Jamaica's digital information stack:

- In the network infrastructure layer, Chinese telecommunication companies are not involved with the undersea cables, but Chinese telecommunication companies Huawei and ZTE provided equipment in Jamaica's 3G and 4G LTE ICT networks. It is unclear whether Chinese companies will be involved in Jamaica's 5G networks.
- The presence of Chinese telecommunication companies in Jamaica's device layer has dramatically tapered since the U.S.'s blacklisting of several PRC companies. The most notable examples of cooperation are ZTE working with Digicel Group, a Caribbean mobile phone company with headquarters in Kingston, Jamaica, to create the world's first low-cost mobile phone in 2009, and Intcomex promoting Huawei's brand across Jamaica to improve device sales.
- In the application layer, TikTok is a popular social media platform in Jamaica and used by politicians to promote their parties and policies, which has garnered some controversy in the country.
- Chinese messaging and narratives in the content layer echo those across the Caribbean, focused on promoting the PRC within the media ecosystems of Taiwan's Caribbean diplomatic allies.
- Lastly, in the governance layer, Jamaica was the first Caribbean country to remove laws that criminalize defamation and have not used ICT equipment from Chinese companies to suppress domestic dissent. Still, Jamaican government officials are courting more opportunities from Chinese companies to make some governance processes more efficient, ranging from fighting crime to maintaining public order.

Despite the ramifications of U.S. sanctions and export regimes and a strong legal framework to protect basic freedoms, some Jamaican government officials continue to entertain the possibility of the PRC's involvement in the country's digital information stack. Civil society actors should be wary of these ties as well as of outreach by Chinese telecommunication companies to promote themselves through donations and training opportunities.

Overview of Sino-Jamaican Relations

Sino-Jamaican relations go back to the 19th Century with the introduction of Chinese laborers to the island.[338] Since Jamaica achieved independence in 1962 and the establishment of formal diplomatic relations between China and Jamaica in 1972, relations between the two countries were primarily defined by shared non-aligned movement values.[339] This changed with the Chinese government's Going Out Strategy in the late-20th Century, which encouraged state and private companies to invest overseas "to promote the export of goods and services," and made Jamaica one of China's primary investment markets in the Caribbean.[340] Jamaica fits into China's broader Caribbean strategy, which is shaped by the region's "good foundation for economic and social growth and huge development potential."[341]

China has emphasized infrastructure cooperation, scientific and technology innovation, infrastructure construction, media cooperation, people-to-people exchanges, and non-traditional security issues as core areas of Sino-Caribbean relations.[342] In Jamaica this has meant US$2.68 billion in investment from China in the tourism, transportation, extractive metals, agriculture, and energy sectors from 2005 to 2020.[343] Furthermore, the Chinese flagship Belt and Road Initiative (BRI) firm China Harbour Engineering Company established its Caribbean headquarters in Kingston, signifying how Jamaica serves as China's staging ground for projects in the region.[344] In short, China's various interests in Jamaica touch upon the digital information stack and the ability of Chinese companies to exert influence over Jamaica's digital ecosystem.

The Network Infrastructure Layer

In September 2009, the Jamaican government issued the final draft of its Vision 2030 plan to map out its network infrastructure layer's national development course. In the plan, the government lays out ICT as a priority sector for Jamaica's infrastructure,[345] and views "ICT as an enabler of all other sectors, including economic, social, environmental and governance sectors."[346] The plan specifically names China an as inspiration for Jamaica's ICT development ambitions, given how this sector has made China a global player.[347] Nonetheless, China did not play a significant role in the initial development of Jamaica's network infrastructure. This is due to the country's British telegraph legacy, proximity to the U.S., and the lack of involvement of Chinese companies in the undersea cable networks connected to Jamaica and its neighbors.[348]

Despite the lack of initial involvement, several Chinese companies, specifically ZTE and Huawei, are active in Jamaica. But Jamaican political and business leaders are torn between adhering to U.S. laws and finding affordable alternatives. In March 2017, Digicel Group announced that ZTE would be involved in the rollout of 4G LTE networks across the island,[349] and according to Digicel, "the planned ZTE-related roll-out in Digicel markets is already complete."[350] This rollout followed a contract that Digicel Jamaica signed with ZTE for the first phase of Jamaica's 2.5GHz mobile WiMAX network in 2009 and the rollout of 3G networks in Guyana and the French overseas department of Guadeloupe that same year.[351] ZTE also was involved in the upgrade of Oceanic Digital Jamaica's CDMA2000 network in 2006,[352] which was later acquired by Digicel. However, ZTE's involvement in future mobile networks in Jamaica, like 5G, have been impeded due to the U.S. government's 2018 export control restrictions.[353]

It is unclear whether Chinese ICT companies will continue to be involved in constructing and deploying Jamaica's 5G networks. Because of Jamaica's proximity to the U.S. and status as a signatory of the U.S. Growth in the Americas Initiative, leaders are concerned about breaking U.S. law by doing further business with Chinese telecommunications companies.[354]

In contrast to ZTE's work directly assisting with Jamaican telecommunication on mobile networks, Huawei has been active in Jamaica's network infrastructure layer by using the island's market as a testing ground for several technologies. In May 2016, Digicel Group and Huawei announced that the companies had successfully tested and deployed 10 Gbps Ultra-Broadband Internet in Kingston, Jamaica.[355] The scale of cooperation is significant. Between 2018 and 2020, Huawei spent about US$27 million on investments and acquisitions in Jamaica.[356] Huawei's presence in Jamaica is not without controversy: former U.S. Ambassador to Jamaica Donald Tapia alleged that Chinese intelligence were listening to his phone calls in Jamaica.[357]

The Device Layer

Unlike the network infrastructure layer, Chinese companies have had more success gaining access to Jamaica's smartphone and mobile markets, although the penetration of Chinese brands is waning.[358] Between January 2019 and November 2021, Chinese smartphone brands including ZTE, Huawei, Alcatel, OnePlus, Xiaomi, Lenovo, Coolpad, LeEco, and Oppo comprised roughly 10 percent of the Jamaican smartphone brands market.[359]

After ZTE's involvement in the deployment of 3G and 4G LTE networks across Jamaica, ZTE remains the most popular Chinese mobile phone brand with 3.6 percent of the market as of November 2021.[360] Yet the penetration of Chinese mobile brands fell by around 2 percent due to sanctions and export restrictions from the U.S. government on Huawei. In November 2021, Huawei made up 1.17 percent of the Jamaican mobile brands market compared to 3.35 percent in November 2019.[361]

ZTE is seeking a prominent role in the Jamaican smartphone market, and Huawei is receiving some success in pushing smartphones. In June 2009, ZTE and the Digicel Group released the Coral-200-Solar which was the world's first low-cost mobile phone powered by solar technology.[362] According to ZTE, this follows Digicel's history of providing "low-cost or free portable solar charges [sic] in many markets."[363] By using proprietary technology from the Netherlands, the Coral-200-Solar provides 15 minutes of talk time for every hour of sunlight.[364] Additionally, in 2016, Huawei worked with Intcomex, a Latin American and Caribbean Information Technology distributor, to promote Huawei's brand across Jamaica.[365] The partnership between the two companies allowed Huawei to strengthen its distribution in Jamaica through the sale of its smartphones and other devices.[366]

Huawei has donated a significant number of devices to educational facilities. In January 2021, Huawei donated 500 computer tablets to the Jamaican Ministry of Education, Youth and Information as a part of the Ministry's "One Laptop or Tablet per Child" initiative, on top of more than 6,000 devices that were donated previously to the initiative. Other donations from Huawei to Jamaican institutions include 200 tablets to University of the West Indies (UWI) students, a Huawei Idea Hub Interactive Classroom System to the same Ministry in November 2021,[367] and 100 tablets to students at the University of Technology, Jamaica (UTech), to "promote ties to students throughout the country."[368] It is notable that these donations have continued as Huawei's share of the Jamaican device layer-relevant markets continue to wane and as Jamaican leaders become more concerned with implications of purchasing devices from Chinese firms targeted by sanctions and export controls.

The Application Layer

Chinese software and applications have little direct impact in Jamaica, but TikTok has gained some popularity on the island. TikTok is popular in Jamaica among influencers and some politicians, mostly notably with the President of the People's National Party and Leader of the Opposition, Member of Parliament Mark Golding. Golding has gained notoriety in the Jamaican press for his attempts to try to go viral on the platform and as of December 21, 2021, has almost 8,000 followers and 40,400 likes.[369] MP Golding has faced criticism for his use of TikTok for viral videos of him dancing and explaining his record of accomplishment as former Jamaican Minister of Justice.[370] Jamaica's Prime Minister and leader of the Jamaica Labour Party, Andrew M. Holness, has 32,700 followers and 137,400 likes.[371] Both politicians have used the platform as a means of conveying policy platforms as well as the work of their political parties and the government. TikTok is also gaining popularity in Jamaica as a place for businesses to advertise and to disseminate public service announcements across the Caribbean, like best practices to prepare for hurricane season.[372]

The Content Layer

Although the content layer of the digital information stack is small in Jamaica compared to other case study countries, the narratives and messages promoted by Chinese officials and state-backed and state-affiliated media fit into wider goals across the Caribbean. When compared with other case study countries, China has not made a large push to highlight the Chinese-made vaccines that have been donated and sold to Jamaica, despite calls from Jamaica to seek out more vaccines from China, India, and Cuba once vaccines were available.[373] The total number of vaccines provided to Jamaica is around 200,000.[374] However, in terms of narratives, the biggest driver of China's messaging in the Caribbean is convincing Taiwan's remaining diplomatic allies to switch diplomatic recognition to China.[375] This is relevant to Jamaica's neighbors, but not to Jamaica directly due to its formal diplomatic relations with the PRC.

The Governance Layer

Jamaican leaders are not using China's involvement to crack down on political opponents or create a great firewall for the country. The Jamaican government has not sought to copy much of China's governance norms, laws, or regulations. Nonetheless, Jamaican national leaders are still actively seeking opportunities to work with Chinese companies despite concerns about how they could influence the country's digital information stack. This shows that China can make inroads in free democracies through its donations and research partnerships.

Prime Minister Andrew Holness illustrates how Jamaican national leaders are seeking more opportunities from Chinese companies. Since coming into office in 2016, PM Holness has noted that "the Jamaica-China relationship is at its strongest point in the history of our 47 years of diplomatic relations" while attending the 2019 China International Import Expo.[376] PM Holness further noted that China has a leading role in innovation and technology which provides opportunities for cooperation.[377] During that same trip, PM Holness visited Huawei's Shenzhen headquarters, where he supported the POE's operations in Jamaica. While at Huawei's Shenzen headquarters, he stated that "developing ICT infrastructure is one of the [Jamaican] government's important strategic objectives."[378] He also expressed that Huawei could play a role in improving government efficiency as well as fighting crime and maintaining public order.[379] Lastly, PM Holness praised Huawei for its ICT talent pipelines in Jamaica like the "Seeds for the Future" program.

Jamaica is doing well in other areas. In November 2013, Jamaica's House of Representatives passed the Defamation Bill 2013, making Jamaica the first country in the Caribbean to remove all laws related to criminal defamation from its legal framework.[380] Prior to reforming its defamation laws, Jamaica's laws on libel, slander, and defamation were traced back to the 19th Century, as well as shortly after the country achieved independence.[381]

Conclusion

Ties between China and Jamaica remain some of the strongest in the Western Hemisphere, going back to the use of Chinese laborers on the island and other British colonial possessions across the region. In recent years, China's interest in Jamaica has grown to focus on the island's strategic location and providing infrastructure that bolsters China's access to the island's ports. In halting Jamaica's adoption of China's digital information stack, the U.S. government's campaign to sanction and block Chinese telecommunication companies globally have had a positive effect. The lesson to be learned from Jamaica's case study is that for countries neighboring the U.S., the best way to halt China's control of the digital information stack is by furthering legislation that makes engaging in business with these companies more difficult.

About the Authors

Bryce Barros is the China affairs analyst at the Alliance for Securing Democracy at the German Marshall Fund. He previously served as an analyst at Kharon researching sanctioned actors and related commercial activities tied to the proliferation of weapons of mass destruction, strategic trade controls, supply chains, and human rights abuses in the Indo-Pacific. Prior to that, he interned at the Long Term Strategy Group researching Sino-American Strategic Competition and the China Britain Business Council researching Chinese market entry for U.K. and EU companies. He is a National Committee on U.S.-China Relations member, Truman National Security Project Fellow, Association of Certified Financial Crime Specialists member, Pacific Forum Young Leader, Aspen Security Forum Scholar, and a National Security Education Program David L. Boren Fellow & Scholar. He holds a BA in Political Science from Norwich University, an MA in International Affairs from Texas A&M University, and is an honorary graduate of the Republic of China (Taiwan) Military Academy. Bryce speaks Mandarin Chinese and Japanese, and spent nearly two decades specializing in the Indo-Pacific region.

Nathan Kohlenberg is a research assistant at the Alliance for Securing Democracy at the German Marshall Fund, where he tracks authoritarian interference activities in the MENA region and provides research support to fellows on issues including election interference, digital surveillance, and information manipulation on social media, among others. He previously served as a policy associate at the Truman National Security Project, where he remains a fellow. He has written about disinformation and foreign election interference in Defense One, Salon, Just Security, and elsewhere. Nathan received a BA from Carleton College in Minnesota and an MA from the Johns Hopkins School of Advanced International Studies, where he conducted research on the South China Sea conflict and contributed a chapter to South China Sea: Maintaining Peace/Preventing War, published by the JHU Press in 2017.

Etienne Soula is a research analyst with the Alliance for Securing Democracy based in Brussels. His research focuses on China's growing political and economic assertiveness in the transatlantic space. Etienne recently spear-headed the expansion of ASD's authoritarian interference tracker to cover over 150 incidents of Chinese interference in Europe and North America. He also contributes to weekly reports on Russian, Chinese, and Iranian diplomats and state-media activity using the Hamilton 2.0 dashboard. Etienne previously worked at the Carnegie Endowment for International Peace, the Hudson Institute, and NATO. Fluent in French and German, he holds a dual master's in international affairs from American University and the Université Libre de Bruxelles, as well as a law degree from the University of Nottingham.

Acknowledgements

This research was conducted with the support of the International Republican Institute. The authors would like to thank current and former IRI colleagues, including Matt Schrader, Adam George, Caitlin Dearing Scott, Hui Hui Ooi, Amy Studdart, David Shullman, the Technology and Democracy team, and the Countering Foreign Authoritarian Influence team, for their invaluable expertise and feedback.

The authors would also like to thank the Texas A&M University Bush School of Government and Public Service's Washington, D.C. campus for its assistance, as well as Henry Tugendhat of the United States Institute of Peace and Phil Robertson of Human Rights Watch for sharing their insights.

Endnotes

1 Lindsay P. Gorman, "A Future Internet For Democracies," The German Marshall Fund of the United States Alliance for Securing Democracy, October 2020, available at https://securingdemocracy.gmfus.org/wp-content/uploads/2020/10/Future-Internet.pdf, pg. 5-8

2 Dr Samantha Hoffman and Dr Nathan Attrill, "Supply chains and the global data collection ecosystem," Australian Strategic Policy Institute International Cyber Policy Centre, July 2021, available at https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2021-06/Supply%20chains.pdf?VersionId=56J_tt8xYXYvsMuhriQt5dSsr92A-DaZH, pg. 6

3 Gorman, 2020, pg. 2.

4 "Sunrise and Huawei Sign ICT Managed Services Agreement," Huawei, available at https://carrier.huawei.com/en/success-stories/products-and-solutions/huawei-sunrise-ict-managed-services-agreement

5 Sheridan Prasso, "China's Digital Silk Road Is Looking More Like an Iron Curtain," Bloomberg, 10 January 2019, available at https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain

6 "Assessing China's Digital Silk Road Initiative," Council on Foreign Relations, available at https://www.cfr.org/china-digital-silk-road/

7 Ibid.

8 Rebecca Arcesati, "The Digital Silk Road is a development issue," MERICS, 28 April 2020, available at https://merics.org/en/short-analysis/digital-silk-road-development-issue

9 Natalie Bannerman, "ZTE and MTN launch the first 5G SA network in East Africa," Capacity Media, 20 January 2020, available at https://www.capacitymedia.com/articles/3824841/zte-and-mtn-launch-the-first-5g-sa-network-in-east-africa ; "Mapping China's Tech Giants," Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/marker-418

10 Paul Triolo, Kevin Allison, Clarise Brown and Kelsey Broderick, "The Digital Silk Road: Expanding China's Digital Footprint," Eurasia Group, 8 April 2020, available at https://www.eurasiagroup.net/files/upload/Digital-Silk-Road-Expanding-China-Digital-Footprint.pdf pg. 2

11 New Southeast Asia-Japan 2 Cable to Link 9 Asian Countries," IEEE Technology Blog, 17 March 2018 available at https://techblog.comsoc.org/2018/03/17/new-southeast-asia-japan-2-cable-to-link-9-asian-countries/

12 Triolo, pg. 6

13 Nestor Gilbert, "64 Significant Cloud Computing Statistics for 2022: Usage, Adoption & Challenges," Finances Online, available at https://financesonline.com/cloud-computing-statistics/

14 Jonathan E. Hillman, "U.S. at risk of losing cloud computing edge to China," Politico, 26 August 2021, available at https://www.politico.com/newsletters/politico-china-watcher/2021/08/26/us-at-risk-of-losing-cloud-computing-edge-to-china-494105

15 "Tencent rolls out internet data centre," Bangkok Post, 11 June 2021, available at https://www.bangkokpost.com/business/2130503/tencent-rolls-out-internet-data-centre

16 Gorman, 2020, page 14.

17 "What is IoT [Internet of Things]?," Oracle, available at https://www.oracle.com/internet-of-things/what-is-iot/

18 Jen Clark, "What is the Internet of Things (IoT)?," IBM, 17 November 2016, available at https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

19 "What is a smart city? - Definition and Examples," TWI, available at https://www.twi-global.com/technical-knowledge/faqs/what-is-a-smart-city

20 Jen Clark, "What is the Internet of Things (IoT)?," IBM, 17 November 2016, available at https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/

21 "What is a smart city? - Definition and Examples," TWI, available at https://www.twi-global.com/technical-knowledge/faqs/what-is-a-smart-city

22 Alexandria Sahai Williams and Samora Kariuki, "#27 China-Africa Tech a guest post by Alexandria Williams," Frontier Fintech Newsletter, 1 August 2021, available at https://frontierfintech.substack.com/p/27-china-africa-tech-a-guest-post?r=9g5bu&utm_campaign=post&utm_medium=web&utm_source=twitter

23 Sascha-Domink Bachmann, Anthony Paphiti, "Why Huawei security concerns cannot be removed from US-China relations," The Conversation, May 10 2019, available at https://theconversation.com/why-huawei-security-concerns-cannot-be-removed-from-us-china-relations-116770

24 Chris Bing, "Chinese-authored spyware found on more than 700 million Android phones," Cyberscoop, November 15 2016, available at https://www.cyberscoop.com/android-malware-china-huawei-zte-kryptowire-blu-products/

25 Lithuania's cybersecurity body warns against Chinese-made phones, Authoritarian Interference Tracker, 23 August 2021, available at https://securingdemocracy.gmfus.org/incident/lithuanias-cybersecurity-body-warns-against-chinese-made-phones/

26 Mobile Vendor Market Share Myanmar, GlobalStats Statcounter, November 2020 - November 2021, available at https://gs.statcounter.com/vendor-market-share/mobile/myanmar

27 "Chinese firm donates computers to Zambian university," Xinhua Silk Road Information Service, 3 November 2021, available at https://en.imsilkroad.com/p/324599.html

28 "Chinese embassy in Laos donates electronic smart boards to Lao kids," Xinhua, 25 July 2020, available at http://www.xinhuanet.com/english/2020-07/25/c_139238701.htm

29 "China electronics technology taiji group of company donates 10 computers to University of Zambia," University of Zambia, November 2021, available at https://www.unza.zm/news/2021-11/china-electronics-technology-taiji-group-of-company-donates-10-computers-university-of

30 "Chinese firm Huawei donates 500 computer tablets to ministry," Jamaica Observer, 8 February 2021, available at https://www.jamaicaobserver.com/news/chinese-firm-huawei-donates-500-computer-tablets-to-ministry_211677 ; Huawei donates interactive classroom systems to Ministry of Education," Jamaica Gleaner, 19 November 2021, available at https://jamaica-gleaner.com/article/news/20211119/huawei-donates-interactive-classroom-systems-ministry-education ; "University of Technology, Jamaica Receives Huawei Donation of Tablets for Students" University of Technology, Jamaica, available at https://www.utech.edu.jm/news/university-of-technology-jamaica-receives-huawei-donation-of-tablets-for-students

31 Alex Hern, "Revealed: how TikTok censors videos that do not please Beijing," The Guardian, 25 September 2019, available at https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-

that-do-not-please-beijing

32 Peter Guest, Emily Fishbein, Nu Nu Lusan, "TikTok is repeating Facebook's mistakes in Myanmar," Rest of World, 18 March 2021, available at https://restofworld.org/2021/tiktok-is-repeating-facebooks-mistakes-in-myanmar/

33 Taylor Hatmaker, "Russian state media is still posting to TikTok a month after the app blocked new content," TechCrunch, 13 April 2022, available at https://techcrunch.com/2022/04/12/tiktok-russian-state-media-propaganda/

34 Jessica Clark, "Top 10 Cloud Providers in China," Back4App, available at https://blog.back4app.com/cloud-computing-providers-in-china/

35 Paul Triolo, Kevin Allison, Clarise Brown and Kelsey Broderick, "The Digital Silk Road: Expanding China's Digital Footprint," Eurasia Group, 8 April 2020, available at https://www.eurasiagroup.net/files/upload/Digital-Silk-Road-Expanding-China-Digital-Footprint.pdf pg. 6

36 Bret Schafer and Jessica Brandt, "How China's 'wolf warrior' diplomats use and abuse Twitter," The Brookings Institution, 28 October 2020, available at https://www.brookings.edu/techstream/how-chinas-wolf-warrior-diplomats-use-and-abuse-twitter/

37 "战狼2[Wolf Warrior 2]," Douban, available at https://movie.douban.com/subject/26363254/

38 Zheping Huang, "China's answer to Rambo is about punishing those who offend China - and it's killing it in theaters," Quartz, 8 August 2017, available at https://qz.com/1048667/wolf-warriors-2-chinas-answer-to-rambo-and-about-punishing-those-who-offend-china-is-killing-it-at-the-box-office/

39 Bret Schafer, Etienne Soula and Joseph Bodnar, "Hamilton Toplines: Dec 6-12, 2021," Alliance for Securing Democracy, 14 December 2021, available at https://securingdemocracy.gmfus.org/hamilton-toplines-dec-6-12-2021/

40 Gorman, 2020, pg. 7-8.

41 Finbarr Toesland, "Is a China-style 'Great Firewall' coming in Nigeria?," New African, 10 April 2021, available at https://newafricanmagazine.com/26999/ ; "Senegal aims to digital sovereignty with new China-backed data centre," Reuters, 22 June 2021, available at https://www.reuters.com/article/senegal-datacenter/senegal-aims-for-digital-sovereignty-with-new-china-backed-data-centre-idINL5N2O44D3

42 Ibid.

43 "Jamaican Prime Minister Andrew Holness Visits Huawei Headquarters in Shenzhen," Huawei, 6 November 2019, available at https://www.huawei.com/en/news/2019/11/jamaica-prime-minister-andrew-holness-visits-huawei

44 Valentin Weber, "The Worldwide Web of Chinese and Russian Information Controls," University of Oxford's Centre for Technology and Global Affairs, September 2019, available at https://www.ctga.ox.ac.uk/files/theworldwidewebofchineseandrussianinformationcontrolspdf

45 "Burmese Expert: China Helping Military Establish Cyber Firewall," Voice of America, 12 February 2021, available at https://www.voanews.com/a/east-asia-pacific_burmese-expert-china-helping-military-establish-cyber-firewall/6201972.html

46 Kadri Kaska and Maria Tolppa, "China's Sovereignty and Internet Governance," Estonian Foreign Policy Institute, June 2020, available at https://icds.ee/wp-content/uploads/2020/06/ICDS_EFPI_Brief_Chinas_Sov-

ereignty_and_Internet_Governance_Kadri_Kaska_Maria_Tolppa_June_2020.pdf, pg. 1

47 Gorman, 2020, pg. 27-29.

48 Stacie Hoffmann, Dominique Lazanski & Emily Taylor, "Standardising the splinternet: how China's technical standards could fragment the internet," Journal of Cyber Policy, 29 August 2020, available at https://oxil.uk/publications/2020-08-29-standardising-the-splinternet/Standardising%20the%20splinternet%20how%20China%20s%20technical%20standards%20could%20fragment%20the%20internet.pdf pg. 240 ; Anna Gross and Madhumita Murgia, "Inside China's controversial mission to reinvent the internet," Financial Times, 27 March 2020, available at https://www.ft.com/content/ba94c2bc-6e27-11ea-9bca-bf503995cd6f ; Anna Gross and Madhumita Murgia, "China and Huawei propose reinvention of the internet," Financial Times, 27 March 2020, available at https://www.ft.com/content/c78be2cf-a1a1-40b1-8ab7-904d7095e0f2 ; Kristen Cordell, "The International Telecommunication Union: The Most Important UN Agency You Have Never Heard Of," Center for Strategic & International Studies, 14 December 2020, available at https://www.csis.org/analysis/international-telecommunication-union-most-important-un-agency-you-have-never-heard

49 Patrick Lozada, "Comments of the Telecommunications Industry Association," National Telecommunications and Information Administration, 8 June 2020, available at https://www.ntia.doc.gov/files/ntia/publications/tia-06082020.pdf pg. 2

50 Mark Montgomery and Theo Lebryk, "China's Dystopian "New IP" Plan Shows Need for Renewed US Commitment to Internet Governance," Just Security, 13 April 2021, available at https://www.justsecurity.org/75741/chinas-dystopian-new-ip-plan-shows-need-for-renewed-us-commitment-to-internet-governance/

51 Ibid.

52 Lozada, pg. 2

53 Patrick Lozada, Tim Rühlig and Helen Toner, "Chinese Involvement in International Technical Standards: A DigiChina Forum," 6 December 2021, available at https://digichina.stanford.edu/work/chinese-involvement-in-international-technical-standards-a-digichina-forum/

54 "China to equip and train Solomon Islands police after anti-China unrest," The Guardian, 24 December 2021, available at https://www.theguardian.com/world/2021/dec/24/china-to-equip-and-train-police-in-solomon-islands-after-unrest

55 ibid ; "Solomon Islands switches recognition from Taiwan to China," DW News, 17 September 2019, available at https://www.dw.com/en/solomon-islands-switches-recognition-from-taiwan-to-china/a-50453667

56 "Pentagon warns China-Solomon Islands security deal could be destabilising," Yahoo! News, 15 April 2022, available at https://news.yahoo.com/pentagon-warns-china-solomon-islands-093000840.html

57 "What Is Seeds for the Future," Huawei, available at https://www.huawei.com/minisite/seeds-for-the-future/history.html

58 Alice Miller, "The CCP [Chinese Communist Party] Central Committee's Leading Small Groups," China Leadership Monitor No. 26, 2017, available at https://www.hoover.org/sites/default/files/uploads/documents/CLM26AM.pdf pg. 1

59 Ibid, pg. 6

60 "中共中央网络安全和信息化委员会办公室 [Office of the Central Cyberspace Affairs Commission]" and "中华人民共和国国家互联网信息办公室 [Cyberspace Administration of China]," available at http://www.cac.gov.cn/ ; "Constitution of the Communist Party of China," Xinhua, 24 October 2017, available at http://

www.xinhuanet.com//english/download/Constitution_of_the_Communist_Party_of_China.pdf ; "International Department Central Committee of CPC [Communist Party of China]," available at https://www.idcpc.org.cn/english/

61 "Constitution of the People's Republic of China," The National People's Congress of the People's Republic of China, 20 November 2019, available at http://www.npc.gov.cn/englishnpc/constitution2019/201911/1f65146fb6104dd3a2793875d19b5b29.shtml ; "State Council Organization Chart," The State Council of the People's Republic of China, 28 August 2014, available at http://english.www.gov.cn/state_council/2014/09/03/content_281474985533579.htm ; "中共中央网络安全和信息化委员会办公室 [Office of the Central Cyberspace Affairs Commission]" and "中华人民共和国国家互联网信息办公室 [Cyberspace Administration of China]," available at http://www.cac.gov.cn/

62 Alice Miller, "The CCP [Chinese Communist Party] Central Committee's Leading Small Groups," China Leadership Monitor No. 26, 2017, available at https://www.hoover.org/sites/default/files/uploads/documents/CLM26AM.pdf pg. 1, 6 ; "中共中央网络安全和信息化委员会办公室 [Office of the Central Cyberspace Affairs Commission]" and "中华人民共和国国家互联网信息办公室 [Cyberspace Administration of China]," available at http://www.cac.gov.cn/ ; "Constitution of the Communist Party of China," Xinhua, 24 October 2017, available at http://www.xinhuanet.com//english/download/Constitution_of_the_Communist_Party_of_China.pdf ; "International Department Central Committee of CPC [Communist Party of China]," available at https://www.idcpc.org.cn/english/ ; "State Council Organization Chart," The State Council of the People's Republic of China, 28 August 2014, available at http://english.www.gov.cn/state_council/2014/09/03/content_281474985533579.htm

63 State-owned Assets Supervision and Administration Commission of the State Council, 17 July 2018, available at http://en.sasac.gov.cn/2018/07/17/c_7.htm

64 "中国电信集团有限公司2020年度校园招聘公告 [China Telecom Group Co., Ltd. 2020 Annual Campus Recruiting Announcement]," State-owned Assets Supervision and Administration Commission of the State Council, 28 August 2019, ; http://www.sasac.gov.cn/n2588035/n2588325/n2588350/c3775951/content.html ; https://supchina.com/company-profiles/china-unicom/http://www.sasac.gov.cn/n2588035/n2588325/c12085785/content.html ; "大唐电信集团中高端人才招聘公告 [Datang Telecom Group Mid-to-High-end Talent Recruitment Announcement]," State-owned Assets Supervision and Administration Commission of the State Council, 15 May 2015, available at http://www.sasac.gov.cn/n2588035/n2588325/n2588350/c3775951/content.html ; "China Unicom (中国联通)," SupChina, available at https://supchina.com/company-profiles/china-unicom/

65 Jérôme Doyon , "Influence without Ownership: the Chinese Communist Party Targets the Private Sector," Institut Montaigne, 26 January 2021, available at https://www.institutmontaigne.org/en/blog/influence-without-ownership-chinese-communist-party-targets-private-sector

66 Sam Peach, "Why did Alibaba's Jack Ma disappear for three months?," BBC News, 20 March 2021, available at https://www.bbc.com/news/technology-56448688 ; Eamon Barrett, "New list of the richest people in China shows rise of the 'green' billionaire, Fortune, 28 October 2021, available at https://fortune.com/2021/10/28/richest-people-in-china-hurun-list-billionaires-green-new-energy/#:~:text=The%20top%20spot%20on%20Hurun's,net%20worth%20of%20%2460.5%20billion.

67 Laura He, "China is cracking down on data privacy. That's terrible news for some of its biggest tech companies," CCN, 8 July 2021, available at https://edition.cnn.com/2021/07/07/tech/china-didi-data-tech-crackdown-intl-hnk/index.html

68 "中华人民共和国国家情报法 [National Intelligence Law of the People's Republic of China]," The National People's Congress of the People's Republic of China, 12 June 2018, available at http://www.npc.gov.cn/npc/c30834/201806/483221713dac4f31bda7f9d951108912.shtml

69 Zach Dorfman, "Tech Giants are Giving China a Vital Edge in Espionage," Foreign Policy, 23 December 2020, available at https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/

70 "Does Huawei have ties to the Communist Party of China (CPC)?," Huawei, available at https://www.huawei.com/en/facts/question-answer/does-huawei-have-ties-to-the-cpc ; Lindsay Maizland and Andrew Chatzky, "Huawei: China 's Controversial Tech Giant," Council on Foreign Relations, 6 August 2020, available at https://www.cfr.org/backgrounder/huawei-chinas-controversial-tech-giant

71 Paul Nash, "China's "Going Out" Strategy," Diplomatic Courier, 10 May 2012, available at https://www.diplomaticourier.com/posts/china-s-going-out-strategy

72 Dr Yu Jie and Jon Wallace, "What is China's Belt and Road Initiative (BRI)?," Chatham House, 13 September 2021, available https://www.chathamhouse.org/2021/09/what-chinas-belt-and-road-initiative-bri

73 "Assessing China's Digital Silk Road Initiative," Council on Foreign Relations, available at https://www.cfr.org/china-digital-silk-road/

74 Ibid.

75 Ibid.

76 Carol Zhong and Annie Lee, "Huawei's Unusual $1.5 Billion Loan Involves Only Chinese Banks," Bloomberg, 9 July 2019, available at https://www.bloomberg.com/news/articles/2019-07-09/huawei-s-unusual-1-5-billion-loan-involves-only-chinese-banks

77 Chuin-Wei Yap, "State Support Helped Fuel Huawei's Global Rise," The Wall Street Journal, 25 December 2019, available at https://www.wsj.com/articles/state-support-helped-fuel-huaweis-global-rise-11577280736 ; Chuin-Wei Yap, "How the Journal Calculated Huawei's State Support," The Wall Street Journal, 25 December 2019, available at https://www.wsj.com/articles/how-the-journal-calculated-huaweis-state-support-11577280830

78 "Chinese Ambassador Zhao Yanbo Attends Huawei's "Seeds For the Future" Launching Ceremony," Embassy of the People's Republic of China in the Republic of Botswana, 27 March 2019, available at https://www.mfa.gov.cn/ce/cebw/eng/xwdt/t1650335.htm ; "Chinese embassy donates 2,000 Huawei Tablets to help Filipino students," Xinhua, 3 February 2021, available at http://www.news.cn/english/2021-02/03/c_139717720.htm ; "Building 5G Together for the Benefit of Humankind," Embassy of the People's Republic of China in Sweden, 2 November 2020, available at http://www.chinaembassy.se/eng/gdxw/202011/t20201102_2812813.htm

79 Steven Lee Myers, "An Alliance of Autocracies? China Wants to Lead a New World Order.," The New York Times, 29 March 2021, available at https://www.nytimes.com/2021/03/29/world/asia/china-us-russia.html ; Charles Edel and David O. Shullman, "How China Exports Authoritarianism," Foreign Affairs, 16 September 2021, available at https://www.foreignaffairs.com/articles/china/2021-09-16/how-china-exports-authoritarianism ; Alexis Leggeri, "What Happens to the CCP If China's Economic Growth Falters?," The Diplomat, 29 October 2020, available at https://thediplomat.com/2020/10/what-happens-to-the-ccp-if-chinas-economic-growth-falters/

80 David Shambaugh, China's Communist Party: Atrophy and Adaptation, 2008, pg 5 & 105

81 Jack Wagner, "China's Cybersecurity Law: What You Need to Know," The Diplomat, 1 June 2017, available at

https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

82 "Provisions on Efforts on Counter-espionage Security Precautions," China Law Translate, 26 April 2021, https://www.chinalawtranslate.com/en/counterespionage-precautions/

83 "National Intelligence Law of the People's Republic of China," 27 June 2017, available https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf pg. 2

84 Rogier Creemers, Paul Triolo, and Graham Webster, "Translation: Cybersecurity Law of the People's Republic of China [Effective June 1, 2017]," New America, 29 June 2018, available at https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/

85 Tracy Wut, Grace Tso, and Mini vandePol, " National Security Law in Hong Kong," Baker McKenzie, June 2020, available at https://www.bakermckenzie.com/-/media/files/insight/publications/2020/07/hong-kong-national-security-law-summary_160720.pdf

86 " Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region gazetted,"The Government of the Hong Kong Special Administrative Region, 6 July 2020, available at https://www.info.gov.hk/gia/general/202007/06/P2020070600784.htm

87 Newley Purnell, "Facebook, Twitter, Google Threaten to Quite Hong Kong Over Proposed Data Laws," Wall Street Journal, 5 July 2021, available at https://www.wsj.com/articles/facebook-twitter-google-warn-planned-hong-kong-tech-law-could-drive-them-out-11625483036

88 Xiang Wang, Aravind Swaminathan, Heather Sussman, Mimiao Hu and Ryan McKenny, "China's New Data Security Law: What International Companies Need to Know," Orrick, September 23 2021, available at https://www.orrick.com/en/Insights/2021/09/Chinas-New-Data-Security-Law-What-International-Companies-Need-to-Know ; "中华人民共和国数据安全法 [Data Security Law of the People's Republic of China]," China Law Translate, 10 June 2021, available at https://www.chinalawtranslate.com/datasecuritylaw/

89 Xiang Wang, Aravind Swaminathan, Heather Sussman, Mimiao Hu and Ryan McKenny, "China's New Data Security Law: What International Companies Need to Know," Orrick, September 23 2021, available at https://www.orrick.com/en/Insights/2021/09/Chinas-New-Data-Security-Law-What-International-Companies-Need-to-Know

90 Xiang Wang, Aravind Swaminathan, Heather Sussman, Mimiao Hu and Ryan McKenny, "China's New Data Security Law: What International Companies Need to Know," Orrick, September 23 2021, available at https://www.orrick.com/en/Insights/2021/09/Chinas-New-Data-Security-Law-What-International-Companies-Need-to-Know ; "中华人民共和国数据安全法 [Data Security Law of the People's Republic of China]," China Law Translate, 10 June 2021, available at https://www.chinalawtranslate.com/datasecuritylaw/

91 Xiang Wang, Aravind Swaminathan, Heather Sussman, Mimiao Hu and Ryan McKenny, "China's New Data Security Law: What International Companies Need to Know," Orrick, September 23 2021, available at https://www.orrick.com/en/Insights/2021/09/Chinas-New-Data-Security-Law-What-International-Companies-Need-to-Know

92 Xiang Wang, Aravind Swaminathan, Heather Sussman, Mimiao Hu and Ryan McKenny, "China's New Data Security Law: What International Companies Need to Know," Orrick, September 23 2021, available at https://www.orrick.com/en/Insights/2021/09/Chinas-New-Data-Security-Law-What-International-Companies-Need-to-Know ; "中华人民共和国数据安全法 [Data Security Law of the People's Republic of China]," China Law Translate, 10 June 2021, available at https://www.chinalawtranslate.com/datasecuritylaw/

93 Xiang Wang, Aravind Swaminathan, Heather Sussman, Mimiao Hu and Ryan McKenny, "China's New Data Security Law: What International Companies Need to Know," Orrick, September 23 2021, available at https://www.orrick.com/en/Insights/2021/09/Chinas-New-Data-Security-Law-What-International-Companies-Need-to-Know ; "中华人民共和国数据安全法 [Data Security Law of the People's Republic of China]," China Law Translate, 10 June 2021, available at https://www.chinalawtranslate.com/datasecuritylaw/

94 Xiang Wang, Aravind Swaminathan, Heather Sussman, Mimiao Hu and Ryan McKenny, "China's New Data Security Law: What International Companies Need to Know," Orrick, September 23 2021, available at https://www.orrick.com/en/Insights/2021/09/Chinas-New-Data-Security-Law-What-International-Companies-Need-to-Know ; "中华人民共和国数据安全法 [Data Security Law of the People's Republic of China]," China Law Translate, 10 June 2021, available at https://www.chinalawtranslate.com/datasecuritylaw/

95 Jesse Hirsh, "New Platform, Old Problems: How TikTok Recreates the Regulatory Challenges That Came Before It," Centre for International Governance Innovation, 18 May 2020, available at https://www.cigionline.org/articles/new-platform-old-problems-how-tiktok-recreates-regulatory-challenges-came-it/

96 Jesse Hirsh, "New Platform, Old Problems: How TikTok Recreates the Regulatory Challenges That Came Before It," Centre for International Governance Innovation, 18 May 2020, available at https://www.cigionline.org/articles/new-platform-old-problems-how-tiktok-recreates-regulatory-challenges-came-it/

97 Elena Botella, "TikTok Admits It Suppressed Videos by Disabled, Queer, and Fat Creators," Slate, 4 December 2019, available at https://slate.com/technology/2019/12/tiktok-disabled-users-videos-suppressed.html ; Alex Hern, "Revealed: how TikTok censors videos that do not please Beijing," The Guardian, 25 September 2019, available at https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing ; Jesse Hirsh, "New Platform, Old Problems: How TikTok Recreates the Regulatory Challenges That Came Before It," Centre for International Governance Innovation, 18 May 2020, available at https://www.cigionline.org/articles/new-platform-old-problems-how-tiktok-recreates-regulatory-challenges-came-it/

98 Elena Botella, "TikTok Admits It Suppressed Videos by Disabled, Queer, and Fat Creators," Slate, 4 December 2019, available at https://slate.com/technology/2019/12/tiktok-disabled-users-videos-suppressed.html

99 Jesse Hirsh, "New Platform, Old Problems: How TikTok Recreates the Regulatory Challenges That Came Before It," Centre for International Governance Innovation, 18 May 2020, available at https://www.cigionline.org/articles/new-platform-old-problems-how-tiktok-recreates-regulatory-challenges-came-it/

100 Dan Swinhoe, "What is a submarine cable? Subsea fiber explained," Data Centre Dynamics, 26 August 2021, available at https://www.datacenterdynamics.com/en/analysis/what-is-a-submarine-cable-subsea-fiber-explained/

101 Ibid.

102 Ibid.

103 "Huawei Marine Networks Rebands as HMN Technologies," HMN Technologies, available at https://www.hmntechnologies.com/enPressReleases/37764.jhtml

104 Benjamin Zawacki, "Of Questionable Connectivity: China's BRI and Thai Civil Society," Council on Foreign Relations, 7 June 2020, available at https://www.cfr.org/blog/questionable-connectivity-chinas-bri-and-thai-civil-society

105 David Hutt, "Thailand moves to strengthen EU ties amid US-China rivalry," Deutsche Welle, 30 July 2021,

available at https://www.dw.com/en/thailand-moves-to-strengthen-eu-ties-amid-us-china-rivalry/a-58706850

106 Freedom House classifies Thailand as "Not Free" in its Freedom in the World 2021 report, available at https://freedomhouse.org/country/thailand/freedom-world/2021; similarly, The Global State of Democracy reports published by the International Institute for Democracy and Electoral Assistance have classified Thailand as an "Authoritarian Regime" since 2014, available at https://www.idea.int/gsod/asia-pacific

107 Chartchai Parasuk, "Get past the Thai-China trade deficit," Bangkok Post, 16 September 2021, available at https://www.bangkokpost.com/opinion/opinion/2182627/get-past-the-thai-china-trade-deficit

108 Marwaan Macan-Markar, "Thai water project gives Beijing a new Belt and Road foothold," Nikkei Asia, 24 September 2021, available at https://asia.nikkei.com/Spotlight/Belt-and-Road/Thai-water-project-gives-Beijing-a-new-Belt-and-Road-foothold

109 Krabi coal power plant Thailand, Banktrack, last updated on 16 June 2020, available at https://www.banktrack.org/project/krabi_coal_power_plant/0/www.marubeni.com#updates

110 Rhea Menon, "Thailand's Kra Canal: China's Way Around the Malacca Strait," The Diplomat, 6 April 2018, available at https://thediplomat.com/2018/04/thailands-kra-canal-chinas-way-around-the-malacca-strait/

111 Benjamin Zawacki, "Of Questionable Connectivity: China's BRI and Thai Civil Society," Council on Foreign Relations, 7 June 2020, available at https://www.cfr.org/blog/questionable-connectivity-chinas-bri-and-thai-civil-society

112 Ibid.

113 Hutt, 2021.

114 Foreign Ministry Spokesperson Wang Wenbin's Regular Press Conference, Ministry of Foreign Affairs of the People's Republic of China, 2 December 2021, available at https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/2511_665403/202112/t20211202_10461360.html

115 Winston Qiu, "AAE-1 Cable Consortium Inks Construction and Maintenance Agreement," Submarine Cable networks, 31 January 2014, available at https://www.submarinenetworks.com/en/systems/asia-europe-africa/aae-1/aae-1-cable-consortium-inks-construction-and-maintenance-agreement

116 Asia Africa Europe-1 (AAE-1), ASPI, available at https://chinatechmap.aspi.org.au/#/map/marker-804

117 "MCT Submarine Cable Launch Promises Bright Future For Cambodian and Regional Telcos," Huawei, 15 March 2017, https://www.huawei.com/en/news/2017/3/mct-submarine-cable-launch

118 "New Southeast Asia-Japan 2 Cable to Link 9 Asian Countries," IEEE Technology Blog, 17 March 2018 available at https://techblog.comsoc.org/2018/03/17/new-southeast-asia-japan-2-cable-to-link-9-asian-countries/

119 Khettiya Jittapong, "China Mobile to buy $881mln stake in Thai billionaire's True Corp," Reuters, 9 June 2014, available at https://www.reuters.com/article/us-true-corporation-chinamobile-idUSKBN0EK0QA20140609

120 "China Mobile signs with True," Bangkok Post, 17 September 2019 available at https://www.bangkokpost.com/business/1751664/china-mobile-signs-with-true

121 "True selects China's ZTE to build 5G network in Thailand," Telecomlead, 29 July 2020, available at https://www.telecomlead.com/5g/true-selects-chinas-zte-to-build-5g-network-in-thailand-96134

122 "Thai regulator monitoring $8.6 bln merger of Telenor's Dtac and True Corp," Reuters, 24 November 202 1 available at https://www.reuters.com/markets/deals/thai-regulator-monitoring-86-bln-merger-telenors-dtac-

true-corp-2021-11-24/

123 Komsan Tortermvasana, "Merger details emerge," Bangkok Post, 25 November 2021, available at https://www.bangkokpost.com/business/2221147/merger-details-emerge

124 James Guild, "Thai Telcos Dtac and True Are Planning a Merger," The Diplomat, 30 November 2021, available at https://thediplomat.com/2021/11/thai-telcos-dtac-and-true-are-planning-a-merger/

125 "Huawei, ZTE and Nokia sign 5G deals with AIS," Telecom Review Asia, 2 September 2019, available at https://www.telecomreviewasia.com/index.php/news/industry-news/1685-huawei-zte-and-nokia-sign-5g-deals-with-ais

126 "AIS, Huawei forge 5G alliance," Bangkok Post, 28 September 2019, available at https://www.bangkokpost.com/business/1760269/ais-huawei-forge-5g-alliance

127 Patpicha Tanakasempipat, "Thailand's AIS says Huawei among bidders to build 5G core networks," Reuters, 14 July 2020, available at https://www.reuters.com/article/us-thailand-telecoms-huawei-5g-idUSKCN24F1AJ

128 Ibid.

129 Suchit Leesa-Nguansuk, "Huawei invests B475m in 5G research hub at Depa," Bangkok Post, 22 September 2020, available at https://www.bangkokpost.com/tech/1989431/huawei-invests-b475m-in-5g-research-hub-at-depa

130 Global Data Center Map, China Telecom Americas website, available at https://www.ctamericas.com/global-data-center-map/

131 "Tencent rolls out internet data centre," Bangkok Post, 11 June 2021, available at https://www.bangkokpost.com/business/2130503/tencent-rolls-out-internet-data-centre

132 "Huawei Technologies Thailand to invest 23 mln USD in new data center," Xinhua, 11 November 2020, available at http://www.xinhuanet.com/english/2020-11/11/c_139509334.htm

133 Ibid.

134 Tiimgum Sirvish, "PEA, Huawei link up for innovation centre," The Nation, 20 November 2017, available at https://www.nationthailand.com/business/30332105

135 "Huawei Technologies wins special PM's award for its contribution to Thailand," The Nation, 9 March 2021, available at https://www.nationthailand.com/business/30403488

136 "Thailand Prime Minister Meets Huawei CEO to Promote Collaboration on Digital Transformation and Talent Development," Huawei, 25 November 2021, available at https://www.huawei.com/en/news/2021/11/thailand-prime-minister-huawei-ceo-ren

137 Lithuania's cybersecurity body warns against Chinese-made phones, Authoritarian Interference Tracker, 23 August 2021, available at https://securingdemocracy.gmfus.org/incident/lithuanias-cybersecurity-body-warns-against-chinese-made-phones/

138 Patpicha Tanakasempipat, "Thailand's AIS says Huawei among bidders to build 5G core networks," Reuters, 14 July 2020, available at https://www.reuters.com/article/us-thailand-telecoms-huawei-5g-idUSKCN24F1AJ

139 Mobile Vendor Market Share Thailand, GlobalStats Statcounter, November 2020 - November 2021, available at https://gs.statcounter.com/vendor-market-share/mobile/thailand

140 Facial recognition: Thailand police departments, ASPI, available at https://chinatechmap.aspi.org.au/#/map/

marker-1535

141 Addition of Certain Entities to the Entity List, Industry and Security Bureau, 9 October 2019, available at https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list

142 "Sansiri – SKY ICT – SenseTime Sings MOU to Develop AI Products for Thailand's Real Estate Market," SenseTime, 23 December 2019, available at https://www.sensetime.com/en/news-detail/3798

143 Smart City Framework and Guidance for Thailand: Smart City services for Phuket, Huawei, 2019, available at https://www.huawei.com/mediafiles/MediaFiles/5/B/9/%7B5B9F4D7B-3F7E-4ED4-A9EE-3ECD-47D38554%7DSMART%20CITY%20FRAMEWORK%20AND%20GUIDANCE%20FOR%20THAILAND_SMART%20CITY%20SERVICES%20FOR%20PHUKET_EN.pdf

144 "Digital 2022: Thailand," We Are Social and Hootsuite, 15 February 2022, p.53, available at https://datareportal.com/reports/digital-2022-thailand

145 Digital 2021: Thailand," We Are Social and Hootsuite, 11 February 2021, p.47, available at https://datareportal.com/reports/digital-2021-thailand?rq=thailand

146 Ibid., p.67

147 Nuurrianti Jalli, "In South East Asia, TikTok has shown it can be the next platform for political activism," Scroll.in, 28 February 2021, available at https://scroll.in/article/988057/in-south-east-asia-tiktok-has-shown-it-can-be-the-next-platform-for-political-activism

148 Post Reporters, "PM takes to TikTok to woo youngsters," Bangkok Post, 11 February 2021, available at https://www.bangkokpost.com/thailand/general/2066071/pm-takes-to-tiktok-to-woo-youngsters

149 "Thailand: Spike in anti-vaccination TikTok clips sparks concerns," the Star, 10 October 2021, available at https://www.thestar.com.my/aseanplus/aseanplus-news/2021/10/10/thailand-spike-in-anti-vaccination-tiktok-clips-sparks-concerns

150 "Alipay Provides Payment Services At Ten More Overseas Airports," China Tech News, 5 October 2016, available at https://www.chinatechnews.com/2016/10/05/24293-alipay-provides-payment-services-at-ten-more-overseas-airports

151 "WeChat offers convenient e-payment services for Thai sellers, Chinese tourists," China Daily, 22 April 2017, available at https://www.chinadaily.com.cn/business/tech/2017-04/22/content_29039680.htm

152 "China's Alipay cooperates with Thai commercial bank," The Nation, 17 September 2017, available at https://www.nationthailand.com/Startup_and_IT/30326951

153 Emma Lee, "Ant Financial To Acquire 20% Stake In Thailand's Ascend Money," Technode, 20 June 2016, available at https://technode.com/2016/06/20/ant-financial-ascend/

154 Reuters Staff, "Factbox: Ant Group's investments overseas," Reuters, 28 October 2020, available at https://www.reuters.com/article/us-ant-group-ipo-strategy-international-idUSKBN27E07C

155 Serichon, "Opinion: Exploring the close ties between Thailand's CP Group and the Chinese Communist Party," Thai Enquirer, 27 July 2021, available at https://www.thaienquirer.com/30426/opinion-exploring-the-close-ties-between-thailands-cp-group-and-the-chinese-communist-party/

156 Eliza Gkritsi, "China to test digital currency transactions with Thailand, UAE," Technode, 24 February 2021, available at https://technode.com/2021/02/24/china-test-digital-currency-transactions-with-thailand-uae/

157 Roula Khalaf, Helen Warrell, "UK spy chief raises fears over China's digital renminbi," Financial Times, 11 December 2021, available at https://www.ft.com/content/128d7139-15d6-4f4d-a247-fc9228a53ebd

158 "5 more Thai media agencies sign partnership with Xinhua," Khaosod English, 20 November 2019, available at https://www.khaosodenglish.com/news/2019/11/20/5-more-thai-media-sites-sign-partnership-with-xinhua/

159 Tyler Roney, "Chinese Propaganda Finds a Thai Audience," Foreign Policy, 28 August 2019, available at https://foreignpolicy.com/2019/08/28/chinese-propaganda-finds-a-thai-audience/

160 Joshua Kurtlantzick, "Thailand's Press Warms to Chinese State Media," Council on Foreign Relations, 8 January 2020, available at https://www.cfr.org/blog/thailands-press-warms-chinese-state-media

161 Yuan Zhou, Zhang Zhihao, "China boosts soft power by training foreign journalists," China Daily, 17 October 2016, available at https://www.chinadaily.com.cn/china/2016-10/17/content_27077588.htm

162 "TNN will air Xinhua news reports locally," Bangkok Post, 2 January 2014, available at https://www.bangkokpost.com/business/387572/tnn-will-air-xinhua-news-reports-locally

163 Jane Tang, "China's Information Warfare and Media Influence Spawn Confusion in Thailand," RFA, 13 May 2021, available at https://www.rfa.org/english/news/china/thailand-infowars-05132021072939.html

164 Facebook post by the Chinese Embassy in Bangkok, 12 May 2021, https://www.facebook.com/846555798724560/posts/4020787351301373

165 Facebook post by the Chinese Embassy in Bangkok, 3 September 2021, https://www.facebook.com/846555798724560/posts/4352763731437065

166 Facebook post by the Chinese Embassy in Bangkok, 12 December 2021, https://www.facebook.com/846555798724560/posts/4659346494112119

167 Yu Qun, "Behind-scenes funding of Thailand protests show invisible Western hands," Global Times, 21 October 2021, available at https://www.globaltimes.cn/content/1204212.shtml

168 Facebook post by the Chinese Embassy in Bangkok, 14 April 2020, https://www.facebook.com/ChineseEmbassyinBangkok/posts/2942654555781330

169 Timothy McLaughlin, "How Milk Tea Became an Anti-China Symbol," The Atlantic, 13 October 2020, https://www.theatlantic.com/international/archive/2020/10/milk-tea-alliance-anti-china/616658/

170 Josh A. Goldstein, Aim Sinpeng, Daniel Bush, Ross Ewald, Jennifer John, "Cheerleading Without Fans: A Low-Impact Domestic Information Operation by the Royal Thai Army," Stanford Internet Observatory, 8 October 2020, available at https://stanford.app.box.com/v/202009-sio-thailand

171 Tracy Beattie, Albert Zhang and Elise Thomas, "The power dynamics of Thailand's digital activism," ASPI, 14 December 2020, available at https://www.aspistrategist.org.au/the-power-dynamics-of-thailands-digital-activism/

172 "From Troops to Trolls: Inside Thailand's Information Operations," Sydney Southeast Asia Centre, 15 September 2021, available at https://www.facebook.com/watch/live/?ref=watch_permalink&v=235154358152643

173 Ian Storey, "Thailand's Military Relations with China: Moving from Strength to Strength," ISEAS–Yusof Ishak Institute, 27 May 2019, available at https://www.iseas.edu.sg/images/pdf/ISEAS_Perspective_2019_43.pdf

174 Training: Provided training course to police, ASPI, available at https://chinatechmap.aspi.org.au/#/map/

marker-2183

175 Doug Bernard, "Thailand Set to Build China-like Internet Firewall," Voice of America, 28 September 2015, available at https://www.voanews.com/a/thailand-set-to-build-china-like-internet-firewall/2982650.html

176 Valentin Weber, "The Worldwide Web of Chinese and Russian Information Controls," University of Oxford's Centre for Technology and Global Affairs, September 2019, available at https://www.ctga.ox.ac.uk/files/theworldwidewebofchineseandrussianinformationcontrolspdf

177 Nithin Coca, "Tourism from China provokes an Internet crackdown in Thailand," Codastory, 12 March 2019, available at https://www.codastory.com/authoritarian-tech/tourism-from-china-provokes-an-internet-crackdown-in-thailand/

178 Gerard McDermott, "Thailand's Creeping Digital Authoritarianism," The Diplomat, 17 February 2021, available at https://thediplomat.com/2021/02/thailands-creeping-digital-authoritarianism/

179 Ahmed Shaheed, Interim report of the Special Rapporteur on freedom of religion or belief, United Nations General Assembly, 12 October 2020, available at https://undocs.org/en/A/75/385

180 Matt Spetalnick, Jeff Mason "Obama offers praise, pressure on historic Myanmar trip," Reuters, 19 November 2012, available at https://www.reuters.com/article/us-asia-obama-myanmar-idUSBRE8AI04320121119

181 "China is not happy about Myanmar's coup," The Economist, 10 July 2021, available at https://www.economist.com/asia/2021/07/10/china-is-not-happy-about-myanmars-coup

182 Sumanth Samsani, "Understanding the relations between Myanmar and China," Observer Research Foundation, 26 April 2021, available at https://www.orfonline.org/expert-speak/understanding-the-relations-between-myanmar-and-china/

183 Jason Tower, Priscilla A. clap, "Myanmar: China, the Coup and the Future," United States Institute for Peace, 8 June 2021, available at https://www.usip.org/publications/2021/06/myanmar-china-coup-and-future

184 Sreeparna Banerjee, Tarushi Singh Rajaura, "Growing Chinese investments in Myanmar post-coup," Observer Research Foundation, 9 November 2021, available at https://www.orfonline.org/expert-speak/growing-chinese-investments-in-myanmar-post-coup/

185 Marwaan Macan-Markar, "Myanmar embraces Russian arms to offset China's influence," Nikkei Asia, 9 February 2021, available at https://asia.nikkei.com/Spotlight/Myanmar-Crisis/Myanmar-embraces-Russian-arms-to-offset-China-s-influence

186 "Beijing Tells Regime It Fears Attack on Its Oil, Gas Pipelines in Myanmar," The Irrawaddy, 24 September 2021, available at https://www.irrawaddy.com/news/burma/beijing-tells-regime-it-fears-attack-on-its-oil-gas-pipelines-in-myanmar.html

187 SeaMeWe-5, Submarine Cable Map, available at https://www.submarinecablemap.com/submarine-cable/seamewe-5

188 SeaMeWe-3, Submarine Cable Map, available at https://www.submarinecablemap.com/submarine-cable/seamewe-3

189 Winston Qiu, "AAE-1 Cable Consortium Inks Construction and Maintenance Agreement," Submarine Cable networks, 31 January 2014, available at https://www.submarinenetworks.com/en/systems/asia-europe-africa/aae-1/aae-1-cable-consortium-inks-construction-and-maintenance-agreement

190 Ngwe Saung Landing Station, ASPI, available at https://chinatechmap.aspi.org.au/#/map/marker-983

191 Winston Qiu, "China-Myanmar International (CMI) Terrestrial Cable Launches for Service," Submarine Cable Networks, 15 November 2014, available at https://www.submarinenetworks.com/news/china-myanmar-international-cmi-terrestrial-cable-launches-for-service

192 "The Asia-Africa-Europe Cable (AAE-1) lands in Myanmar," People's Daily Online, 2 March 2016, available at http://en.people.cn/n3/2016/0302/c90000-9023967.html

193 John Reed, Richard Milne, "Telenor's sale of Myanmar unit to M1 sidelined over junta's opposition," Financial Times, 9 November 2021, available at https://www.ft.com/content/f04e5f0f-ab7f-4c6c-8d0f-27a7380e1a22

194 "Ooredoo plans 500Mbps LTE upgrade," Comms Update, 20 December 2017, available at https://www.commsupdate.com/articles/2017/12/20/ooredoo-plans-500mbps-lte-upgrade/

195 Ooredoo Myanmar 5G MoU, ASPI, available at https://chinatechmap.aspi.org.au/#/map/marker-2013

196 "ZTE, Together with Ooredoo, Build the Intelligent Operation Model in the Industry," Mobile World Live, 11 May 2021, available at https://www.mobileworldlive.com/zte-updates-2019-20/zte-together-with-ooredoo-build-the-intelligent-operation-model-in-the-industry

197 "Connecting the Future: 2016 Sustainability Report," Huawei, June 2017, p.66-67, available at https://www-file.huawei.com/-/media/corporate/pdf/sustainability/2016-huawei-sustainability-report-en-v2.pdf?la=en

198 Saw Yi Nanda, "MyTel anticipating 5G rollout next year if granted licence," Myanmar Times, 6 August 2019, available at https://www.mmtimes.com/news/mytel-anticipating-5g-rollout-next-year-if-granted-licence.html

199 "Interview: Huawei Myanmar will continue to play important role in the country's ICT sector," The Star,, 20 July 2020, available at https://www.thestar.com.my/aseanplus/aseanplus-news/2020/07/20/interview-huawei-myanmar-will-continue-to-play-important-role-in-the-country039s-ict-sector

200 Thet Su Aung, Ye Tike, "Myanmar Sticks With Huawei For Telecoms Buildout Despite China Concerns," Radio Free Asia, 2 October 2019, available at https://www.rfa.org/english/news/myanmar/myanmar-sticks-with-huawei-10022019163928.html

201 Applications of the BeiDou Navigation Satellite System, China Satellite Navigation Office, December 2018, p.46 available at http://www.beidou.gov.cn/xt/gfxz/201906/P020190605488535070471.pdf

202 "China, Myanmar to enhance science, technology cooperation," Xinhua, 23 November 2018, available at http://www.xinhuanet.com/english/2018-11/23/c_137627037.htm

203 Stephanie Pearl Li, Aj Cortese, "Xiaomi and other China smartphone titans dominate Myanmar," Nikkei Asia, 30 November 2020, available at https://asia.nikkei.com/Business/36Kr-KrASIA/Xiaomi-and-other-China-smartphone-titans-dominate-Myanmar

204 Mobile Vendor Market Share Myanmar, GlobalStats Statcounter, November 2020 - November 2021, available at https://gs.statcounter.com/vendor-market-share/mobile/myanmar

205 Stephanie Pearl Li, Aj Cortese, "Xiaomi and other China smartphone titans dominate Myanmar," Nikkei Asia, 30 November 2020, available at https://asia.nikkei.com/Business/36Kr-KrASIA/Xiaomi-and-other-China-smartphone-titans-dominate-Myanmar

206 Lithuania's cybersecurity body warns against Chinese-made phones, Authoritarian Interference Tracker, 23 August 2021, available at https://securingdemocracy.gmfus.org/incident/lithuanias-cybersecurity-body-warns-against-chinese-made-phones/

207 Mobile Vendor Market Share Myanmar, GlobalStats Statcounter, November 2020 - November 2021, available

at https://gs.statcounter.com/vendor-market-share/mobile/myanmar

208 Myat Pyae Phyo, "Huawei to Supply Mandalay's 'Safe City' Project with Cameras, Security Equipment," The Irrawaddy, 9 May 2019, available at https://www.irrawaddy.com/news/burma/huawei-supply-mandalays-safe-city-project-cameras-security-equipment.html

209 "Myanmar: Facial Recognition System Threatens Rights," Human Rights Watch, 12 March 2021, available at https://www.hrw.org/news/2021/03/12/myanmar-facial-recognition-system-threatens-rights

210 Hikvision Digital Technology, "Yangon goes live with Hikvision traffic management solution," Asmag.com, 27 September 2017, available at https://www.asmag.com/showpost/23776.aspx

211 Addition of Certain Entities to the Entity List, Industry and Security Bureau, 9 October 2019, available at https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list; Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China, White House, 3 June 2021, available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/executive-order-on-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/

212 "Myanmar: Coup Leads to Crimes Against Humanity," Human Rights Watch, 31 July 2021, available at https://www.hrw.org/news/2021/07/31/myanmar-coup-leads-crimes-against-humanity

213 "Facebook was the internet in Myanmar. What happens now that it's banned? | Tech in Culture," KrAsia, 24 February 2021, available at https://kr-asia.com/facebook-was-the-internet-in-myanmar-what-happens-now-that-its-banned-tech-in-culture

214 "Rohingya sue Facebook for $150bn over Myanmar hate speech," BBC, 7 December 2021, available at https://www.bbc.com/news/world-asia-59558090

215 Jon Porter, "Facebook blocked in Myanmar after users protest military coup," The Verge, 4 February 2021, available at https://www.theverge.com/2021/2/4/22266031/facebook-myanmar-blocked-instagram-whatsapp-military-coup-protest

216 Rafael Frankel, "An Update on the Situation in Myanmar," Facebook, 7 December 2021, available at https://about.fb.com/news/2021/02/an-update-on-myanmar/

217 Social Media Stats Myanmar, GlobalStats Statcounter, November 2020 - November 2021, available at https://gs.statcounter.com/social-media-stats/all/myanmar

218 "WeChat Launches in Myanmar," WeChat Blog, 3 July 2015, available at https://blog.wechat.com/2015/07/03/wechat-launches-in-myanmar/

219 Elisa Oreglia, "Chinese digital ecosystems go global: Myanmar and the diffusion of Chinese smartphones," Hong Kong Free Press, 27 January 2019, available at https://hongkongfp.com/2019/01/27/chinese-digital-ecosystems-go-global-myanmar-diffusion-chinese-smartphones/

220 Kyaw Lin Htoon, "Jade traders call for WeChat ban," Frontier, 12 November 2018, available at https://www.frontiermyanmar.net/en/jade-traders-call-for-wechat-ban/

221 Htike Nanda Win, "Myanmar women in China use WeChat to escape forced marriages," Myanmar Now, 14 February 2019, available at https://www.myanmar-now.org/en/news/myanmar-women-in-china-use-wechat-to-escape-forced-marriages

222 "Supporters and detractors of Myanmar's coup take fraught conflict to TikTok, Facebook, and Twitter," KrA-

sia, 30 June 2021, available at https://kr-asia.com/supporters-and-detractors-of-myanmars-coup-take-fraught-conflict-to-tiktok-facebook-and-twitter

223 Ole Tangen Jr., "The battle for Myanmar plays out on Twitter, TikTok and Telegram," Deutsche Welle, 20 April 2021, available at https://www.dw.com/en/the-battle-for-myanmar-plays-out-on-twitter-tiktok-and-telegram/a-57267075

224 "'I will shoot whoever I see': Myanmar soldiers use TikTok to threaten protesters," Reuters, 4 March 2021, available at https://www.reuters.com/article/us-myanmar-tiktok/i-will-shoot-whoever-i-see-myanmar-soldiers-use-tiktok-to-threaten-protesters-idUSKBN2AW17X

225 Peter Guest, Emily Fishbein, Nu Nu Lusan, "TikTok is repeating Facebook's mistakes in Myanmar," Rest of World, 18 March 2021, available at https://restofworld.org/2021/tiktok-is-repeating-facebooks-mistakes-in-myanmar/

226 KBZ Bank announces partnership with Huawei to offer greater financial access to all, KBZ Bank, 20 March 2018, available at https://www.kbzbank.com/wp-content/uploads/2019/05/KBZ-Huawei-partnership_ENG_20032018.pdf

227 Nan Lwin, "Huawei Extends Cloud Services to Myanmar as Firms Go Digital," The Irrawaddy, 20 October 2020, available at https://www.irrawaddy.com/news/burma/huawei-extends-cloud-services-myanmar-firms-go-digital.html

228 "Ant Financial invests $73.5 mn in Myanmar fintech Wave Money," International Finance, 20 May 2020, available at https://internationalfinance.com/ant-financial-invests-73-5-mn-myanmar-fintech-wave-money/

229 Nu Nu Lusan, Emily Fishbein, Peter Guest, "Myanmar's military coup has pushed its fledgling digital economy to the brink of collapse," Rest of World, 15 April 2021, available at https://restofworld.org/2021/myanmars-military-coup-has-pushed-its-fledgling-digital-economy-to-the-brink-of-collapse/

230 "Wave Money has lost half of its app users since Myanmar's coup in February," KrAsia, 16 August 2021, available at https://kr-asia.com/wave-money-has-lost-half-of-its-users-since-myanmars-coup-in-february

231 Elizabeth Jangma, "Thousands in Myanmar Protest to Demand Myitsone Dam Project be Scrapped," Radio Free Asia, 22 April 2019, available at https://www.rfa.org/english/news/myanmar/scrapped-04222019170858.html

232 Tin Htet Paing, "How China Pushes Its Agenda in Myanmar Media," Myanmar Now, 9 October 2019, available at https://www.myanmar-now.org/en/news/how-china-pushes-its-agenda-in-myanmar-media

233 Aung Thet Wine, "24-hr News Channel to Air in Burma," The Irrawaddy, 22 February 2010, available at https://www2.irrawaddy.com/article.php?art_id=17864

234 Tin Htet Paing, "How China Pushes Its Agenda in Myanmar Media," Myanmar Now, 9 October 2019, available at https://www.myanmar-now.org/en/news/how-china-pushes-its-agenda-in-myanmar-media

235 Ibid.

236 "Journalists and the China story: Myanmar," International Federation of Journalists, 7 July 2021, available at https://www.ifj.org/media-centre/news/detail/category/china-the-fight-for-freedom/article/journalists-and-the-china-story-myanmar.html

237 Teeranai Charuvastra, "China, As Told by China: Beijing's Influences Reach Thai Media and Beyond," Heinrich Böll Stiftung, 28 December 2019, available at https://th.boell.org/en/2019/12/28/china-told-china-bei-

jings-influences-reach-thai-media-and-beyond

238 Tin Htet Paing, "How China Pushes Its Agenda in Myanmar Media," Myanmar Now, 9 October 2019, available at https://www.myanmar-now.org/en/news/how-china-pushes-its-agenda-in-myanmar-media

239 Phil Thornton, "Myanmar: If independent media dies, democracy dies," International Federation of Journalists, 7 May 2021, https://www.ifj.org/media-centre/blog/detail/category/asia-pacific/article/myanmar-if-independent-media-dies-democracy-dies.html

240 Chinese Embassy in Myanmar, Facebook, available at https://www.facebook.com/paukphawfriendship/

241 Examples include a press conference given by the Chinese ambassador on 15 February 2021, available at https://www.facebook.com/191612647581463/posts/3697455966997096, and press conference in which the Chinese Foreign Minster Wang Yi answered questions about Myanmar on 7 March 2021, available at https://www.facebook.com/191612647581463/posts/3754850981257594

242 Diya Jiang, Kristina Kironska, "Chinese Media's Conflicting Narratives on the Myanmar Coup," The Diplomat, 14 August 2021, available at https://thediplomat.com/2021/08/chinese-medias-conflicting-narratives-on-the-myanmar-coup/

243 "Myanmar Protesters Say an Attack on China's Pipelines Would Be 'Internal Affair'," The Irrawaddy, 8 March 2021, available at https://www.irrawaddy.com/news/burma/myanmar-protesters-say-attack-chinas-pipelines-internal-affair.html

244 "West utterly manipulates Myanmar situation as a tool in anti-China campaign," Global Times, 17 March 2021, available at https://www.globaltimes.cn/page/202103/1218717.shtml

245 Jason Tower, Priscilla A. Clapp, "Myanmar: China, the Coup and the Future," United States Institute of Peace, 8 June 2021, available at https://www.usip.org/publications/2021/06/myanmar-china-coup-and-future

246 Fanny Potkin, Poppy Mcpherson, "How Myanmar's military moved in on the telecoms sector to spy on citizens," Reuters, 19 May 2021, available at https://www.reuters.com/world/asia-pacific/how-myanmars-military-moved-telecoms-sector-spy-citizens-2021-05-18/

247 "Myanmar's Legal Framework For Cybersecurity Needs To Be Built To International Standards," Myanmar Centre for Responsible Business, 10 May 2021, available at https://www.myanmar-responsiblebusiness.org/news/legal-framework-for-cybersecurity.html

248 "Myanmar: Scrap Sweeping Cybersecurity Bill," Human Rights Watch, 12 February 2021, available at https://www.hrw.org/news/2021/02/12/myanmar-scrap-sweeping-cybersecurity-bill

249 "Burmese Expert: China Helping Military Establish Cyber Firewall," Voice of America, 12 February 2021, available at https://www.voanews.com/a/east-asia-pacific_burmese-expert-china-helping-military-establish-cyber-firewall/6201972.html

250 Fanny Potkin, "EXCLUSIVE After pressuring telecom firms, Myanmar's junta bans executives from leaving," Reuters, 20 December 2021, available at https://www.reuters.com/world/asia-pacific/exclusive-after-pressuring-telecom-firms-myanmars-junta-bans-executives-leaving-2021-07-05/

251 Jason Tower, "China and Myanmar's Ousted Leaders: Mixed Signals, Cold Interests," United States Institute of Peace, 7 October 2021, available at https://www.usip.org/publications/2021/10/china-and-myanmars-ousted-leaders-mixed-signals-cold-interests

252 "Uganda, China mark 59 years of diplomatic ties," Xinhua, 18 October 2021, available at http://www.news.

cn/english/africa/2021-10/18/c_1310253203.htm

253 "China and Uganda Trade," OEC, available at https://oec.world/en/profile/bilateral-country/chn/partner/uga

254 Dr. Hakeem Onapajo and Dr. Christopher Isike, "The Global Politics of Gay Rights: The Straining Relations between the West and Africa," The Journal of Global Analysis, January 2016, available at https://therestjournal.com/wp-content/uploads/2019/03/JGA_Vol.6_No.1_A_2.pdf

255 Somini Sengupta, "Antigay Laws Gain Global Attention; Countering Them Remains Challenge," New York Times, 1 March 2014, available at https://www.nytimes.com/2014/03/02/world/africa/antigay-laws-gain-global-attention-countering-them-remains-challenge.html

256 Kristof Titeca and Anna Reuss, "After a violent election, Uganda's government faces three big challenges," Washington Post, 16 February 2021, available at https://www.washingtonpost.com/politics/2021/02/16/after-violent-election-ugandas-government-faces-three-big-challenges/

257 "Uganda loses its only international airport to China for failing to repay loan: Reports," India Today, 28 November 2021, available at https://www.indiatoday.in/world/story/uganda-international-airport-china-default-debt-repayment-1881674-2021-11-28

258 Tom Ogwang and Frank Vanclay, "Resource-Financed Infrastructure: Thoughts on Four Chinese-Financed Projects in Uganda," MDPI, 16 March 2021, available at https://www.mdpi.com/2071-1050/13/6/3259/pdf

259 Celine Sui, "China's Racism Is Wrecking Its Success in Africa," Foreign Policy, 15 April 2020, available at https://foreignpolicy.com/2020/04/15/chinas-racism-is-wrecking-its-success-in-africa/

260 Alison Gillwald, Onkokame Mothobi, Ali Ndiwalana, and Tusu Tusubira, "The State of ICT in Uganda," Research ICT Africa, May 2019, available at https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access-The-State-of-ICT-in-Uganda.pdf

261 Sophie Nyombi and Brian Kalule, "Uganda: Overview of Data Infrastructure in East Africa," Bowmans, 13 April 2021, available at https://www.bowmanslaw.com/insights/technology-media-and-telecommunications/overview-of-data-infrastructure-in-east-africa-uganda/

262 "Mapping China's Tech Giants," Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/marker-3611

263 "China's Telecommunications Footprint in Africa," Institute of Developing Economies, Japan External Trade Organization, available at https://www.ide.go.jp/English/Data/Africa_file/Manualreport/cia_09.html

264 "Mapping China's Tech Giants," Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/marker-3948

265 "Mapping China's Tech Giants," Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/marker-418

266 "China plays critical role in advancing Uganda's ICT development," Xinhua, 16 April 2019, available at https://archive.md/w6xKs

267 Ryan Huang, "Uganda orders probe into Huawei's fiber project," ZDNet, 3 October 2022, available at https://www.zdnet.com/article/uganda-orders-probe-into-huaweis-fiber-project/

268 "National Backbone Infrastructure Project (NBI/EGI)," NITA Uganda, available at https://www.nita.go.ug/projects/national-backbone-infrastructure-project-nbiegi

269 Edris Kisambira, "Uganda Telecom's network expansion almost complete," NetworkWorld, 21 May 2008,

available at https://www.networkworld.com/article/2279782/uganda-telecom-s-network-expansion-almost-complete.html

270 Natalie Bannerman, "ZTE and MTN launch the first 5G SA network in East Africa," Capacity Media, 20 January 2020, available at https://www.capacitymedia.com/articles/3824841/zte-and-mtn-launch-the-first-5g-sa-network-in-east-africa

271 "ZTE and MTN Uganda unveil the first 5G standalone network in East Africa," International Finance, 31 January 2020, available at https://internationalfinance.com/zte-and-mtn-uganda-unveil-the-first-5g-stand-alone-network-in-east-africa/

272 Scott Wingo, "China in Uganda: The Highs and Lows of the Belt and Road," Center for Advanced China Research, 27 June 2019, available at https://www.ccpwatch.org/single-post/2019/06/27/china-in-uganda-the-highs-and-lows-of-the-belt-and-road

273 "Mapping China's Tech Giants," Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/marker-1214

274 "City Surveillance for Kampala, Uganda," Uniview, 10 August 2017, available at https://www.uniview.com/News/Success_Cases/201708/789806_169683_0.htm

275 "Mapping China's Tech Giants," Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/marker-1214

276 Lauren Feiner, "Huawei employees intercepted encrypted messages to help African governments spy on political opponents, says WSJ," CNBC, 14 August 2019, available at https://www.cnbc.com/2019/08/14/huawei-employees-helped-african-governments-spy-on-opponents-wsj.html

277 Salem Solomon, "In Uganda, Dissidents Adapt to Evade Huawei Assisted Government Spying," Voice of America, 14 November 2019, available at https://www.voanews.com/a/africa_uganda-dissidents-adapt-evade-huawei-assisted-government-spying/6179464.html

278 Stephen Kafeero, "Uganda is using Huawei's facial recognition tech to crack down on dissent after anti-government protests," Quartz Africa, 27 November 2020, available at https://qz.com/africa/1938976/uganda-uses-chinas-huawei-facial-recognition-to-snare-protesters/

279 Tweet, @KagutaMuseveni, Twitter, 28 November 2019, available at https://twitter.com/KagutaMuseveni/status/1200120752114196481?s=20

280 "Huawei infiltration in Uganda," Privacy International, 25 June 2020, available at https://privacyinternational.org/case-study/3969/huawei-infiltration-uganda

281 "Mobile Vendor Market Share – Uganda," statcounter, GlobalStats, November 2021, available at https://gs.statcounter.com/vendor-market-share/mobile/uganda

282 "How one TECNO phone is putting users' privacy and security at risk," Privacy International, 10 August 2021, available at https://privacyinternational.org/long-read/4605/how-one-tecno-phone-putting-users-privacy-and-security-risk

283 "Chinese phones with built-in malware sold in Africa," BBC News, 25 August 2020, available at https://www.bbc.com/news/technology-53903436

284 Javira Ssebwabi, "PML Daily, Xinhua sign content partnership pact," PML Daily, 9 September 2019, available at https://www.pmldaily.com/news/2019/09/pml-daily-xinhua-sign-content-partnership.html

285 Angela Lewis, "How a Pay TV Company Is Serving up a Soft Power Win for China in Africa," The Diplomat, 14 February 2019, available at https://thediplomat.com/2019/02/how-a-pay-tv-company-is-serving-up-a-soft-power-win-for-china-in-africa/

286 Tweet, @XHNews, Twitter, 15 September 2021, available at https://twitter.com/i/web/status/1438156026679681026

287 Tweet, @globaltimesnews, Twitter, 11 August 2021, available at https://twitter.com/i/web/status/1425462004542738432

288 Tweet, @PDChina, Twitter, 4 February 2021, available at https://twitter.com/i/web/status/1357538690080231427

289 Tweet, @cgtnafrica, Twitter, 29 November 2021, available at https://twitter.com/i/web/status/1465270949197008899

290 Joan Banura, "KIU, Huawei Uganda to Establish an ICT Academy," PC Tech Magazine, 23 July 2021, available at https://pctechmag.com/2021/07/kiu-huawei-uganda-to-establish-an-ict-academy/

291 Mary Nankinga, "China To Train Uganda Police In Criminal Investigations," Uganda Police Force, 20 December 2017, available at https://www.upf.go.ug/china-train-uganda-police-criminal-investigations/

292 Benjamin Mulvey, "Foreign Students and China's Soft Power: The Case of Uganda," The Diplomat, 10 January 2020, available at https://thediplomat.com/2020/01/foreign-students-and-chinas-soft-power-the-case-of-uganda/

293 Tweet, @ChineseEmb_Uga, Twitter, 19 September 2019, available at https://twitter.com/ChineseEmb_Uga/status/1174600548533919744?s=20

294 "China and Nigeria Trade," OEC, available at https://oec.world/en/profile/bilateral-country/chn/partner/nga#historical-data

295 "Nigeria trims ties with Taiwan as it courts China," Reuters, 12 January 2017, available at https://www.reuters.com/article/us-taiwan-nigeria/nigeria-trims-ties-with-taiwan-as-it-courts-china-idUSKBN14W1BI

296 "China Global Investment Tracker," American Enterprise Institute, available at https://www.aei.org/china-global-investment-tracker/

297 "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/f1-Nigeria

298 Dipanjan Roy Chaudhury, "China reportedly investing $8.43 bn in Africa as part of Digital Silk Road initiative," The Economic Times, 15 October 2021, available at https://economictimes.indiatimes.com/news/international/world-news/china-reportedly-investing-8-43-bn-in-africa-as-part-of-digital-silk-road-initiative/articleshow/87039334.cms?from=mdr

299 Abdul-Gafar Tobi Oshodi, "Nigerians and China: Understanding the imbalanced relationship," The Africa Report, 1 June 2020, available at https://www.theafricareport.com/29060/nigeria-and-china-understanding-the-imbalanced-relationship/

300 Celine Sui, "China's Racism Is Wrecking Its Success In Africa," Foreign Policy, 15 April 2020, available at https://foreignpolicy.com/2020/04/15/chinas-racism-is-wrecking-its-success-in-africa/

301 'Tofe Ayeni, "China-Africa: Spotlight turned on abuse of Nigerian workers," The Africa Report, 3 September 2020, available at https://www.theafricareport.com/39952/nigeria-spotlight-on-abuse-of-local-workers-af-

ter-public-allegations/

302 Keith Bradsher and Adam Nossiter, "In Nigeria, Chinese Investment Comes With A Downside," New York Times, 5 December 2015, available at https://www.nytimes.com/2015/12/06/business/international/in-nigeria-chinese-investment-comes-with-a-downside.html

303 "Negative views of Russia on the Rise: Global Poll" http://downloads.bbc.co.uk/mediacentre/country-rating-poll.pdf

304 Dennis Quinn, "Nigerians living near a major Belt and Road project grew more positive toward China after it was completed," Pew Research Center, 23 April 2020, available at https://www.pewresearch.org/fact-tank/2020/04/23/nigerians-living-near-a-major-belt-and-road-project-grew-more-positive-toward-china-after-it-was-completed/

305 "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/f1-Nigeria,f5-Cable

306 "西非海缆系统 [WACS]," Huawei Marine, available at https://archive.fo/bzNBs

307 "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/f1-Nigeria,f5-Cable

308 "Infrapedia," available at https://www.infrapedia.com/app

309 Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/marker-492

310 "Huawei adds another contract to its Nigerian portfolio," Comms Update, 18 April 2005, available at https://www.commsupdate.com/articles/2005/04/18/huawei-adds-another-contract-to-its-nigerian-portfolio/

311 Ibid.

312 "ZTE wins contract with Nigerian government," RCR Wireless News, 28 April 2005, available at https://www.rcrwireless.com/20050428/archived-articles/zte-wins-contract-with-nigerian-government

313 "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/marker-928

314 "Etisalat, EXIM and Huawei sign MoU for strategic cooperation," Economic Times, 15 July 2011, available at https://archive.fo/Eopd1#selection-4495.0-4495.60

315 Olanrewaju Odunowo, "A $328 million Chinese loan to expand Nigeria's broadband access," TechCabal, 22 July 2020, available at https://techcabal.com/2020/07/22/techcabal-daily-a-328-million-chinese-loan-to-expand-nigerias-broadband-access/

316 "MTN Nigeria and Huawei Jointly Complete the Commercial Deployment of RuralStar 2.0," Press Release Point, 2 April 2018, available at https://www.pressreleasepoint.com/mtn-nigeria-and-huawei-jointly-complete-commercial-deployment-ruralstar-20

317 "Airtel expects to launch 4G in Nigeria within the next few months," Comms Update, 20 May 2017, available at https://www.commsupdate.com/articles/2017/05/30/airtel-expects-to-launch-4g-in-nigeria-within-next-few-months/

318 "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/marker-3613; "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.

au/#/map/marker-624

319 "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/marker-3961

320 "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/marker-1665

321 "Mapping China's Tech Giants," International Cyber Policy Centre, Australian Strategic Policy Institute, available at https://chinatechmap.aspi.org.au/#/map/marker-368

322 "Mobile Vendor Market Share Nigeria Nov 2020 – Nov 2021," StatCounter, available at https://gs.statcounter.com/vendor-market-share/mobile/nigeria

323 "Chinese phones with built-in malware sold in Africa," BBC News, 25 August 2020, available at https://www.bbc.com/news/technology-53903436

324 "Most used social media platforms in Nigeria as of the 3rd quarter of 2020," Statistia, February 2021, available at https://www.statista.com/statistics/1176101/leading-social-media-platforms-nigeria/

325 Mayozi John, "Huawei brings intelligent oil, gas to Nigeria," The Guardian, 10 June 2021, available at https://guardian.ng/business-services/huawei-brings-intelligent-oil-gas-to-nigeria/

326 "Nigeria lost $2.77bn to crude oil theft in 2019 – NEITI," Vanguard, 15 July 2021, available at https://www.vanguardngr.com/2021/07/nigeria-lost-2-77bn-to-crude-oil-theft-in-2019-neiti/

327 Aisha Salaudeen and Stephanie Busari, "China and Nollywood have signed up for their first major film collaboration," CNN News, 21 November 2019, available at https://www.cnn.com/2019/11/21/africa/china-nigeria-film-partnership/index.html

328 "China, Nigeria sign MoU on information exchange," Xinhua, 12 August 2017, available at http://www.xinhuanet.com/english/2017-08/12/c_136519466.htm

329 Emeka Umejei, "What is the Influence of Chinese Media in West Africa?" Council on Foreign Relations, available at https://www.cfr.org/sites/default/files/pdf/Chinese%20Media%20West%20Africa.pdf

330 Tweet, @PDChina, Twitter, 13 May 2021, available at https://twitter.com/i/web/status/1392744671273701381

331 Tweet, @XHNews, Twitter, 3 July 2021, available at https://twitter.com/XHNews/status/1411303091220058114?s=20

332 Tweet, @XHNews, Twitter, 6 January 2021, available at https://twitter.com/i/web/status/1346843068276690944

333 Nimi Princewill and Stephanie Busari, "Nigeria bans Twitter after company deletes President Buhari's tweet," CNN, 5 June 2021, available at https://www.cnn.com/2021/06/04/africa/nigeria-suspends-twitter-operations-intl/index.html

334 Nigeria at 61: Buhari lift Twitter ban, wit conditions," BBC, 1 October 2021, available at https://www.bbc.com/pidgin/world-58732512

335 Witney Schneidman, Dan Cooper, Mosa Mkhize, Sam Jungyun Choi, and Shivani Naidoo, "Tech Regulation in Africa: Recently Enacted Data Protection Laws," Inside Privacy, 9 December 2021, available at https://www.insideprivacy.com/data-privacy/tech-regulation-in-africa-recently-enacted-data-protection-laws/

336 Josh Horwitz, "China passes new personal data privacy law, to take effect Nov. 1," Reuters, 20 August 2021,

available at https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect--nov-1-2021-08-20/

337 Socrates Mbamalu, "EXCLUSIVE: Presidency Meets With China's Cyber Regulator to Build Nigerian Internet Firewall," Foundation for Investigative Journalism, 6 June 2021, available at https://fij.ng/article/exclusive-presidency-meets-with-chinas-cyber-regulator-to-build-nigerian-internet-firewall/

alliance for securing democracy