KKI

Policy Brief

KE-2022/17

Southeast Asia in the US-China Tech Rivalry II. Digital Infrastructure Development and Data Governance

Délkelet-Ázsia az USA és Kína technológiai háborújában II. Digitális infrastruktúra és adatszabályozás

PÉTER GORECZKY

INSTITUTE FOR FOREIGN AFFAIRS AND TRADE

KKI Policy Brief
Series of the Institute for Foreign Affairs and Trade

Publisher:
Institute for Foreign Affairs and Trade

Reviewed by:
Tamás Péter Baranyi

Typesetting:
Tamás Lévárt

Editorial office:
H-1016 Budapest, Bérc utca 13-15.
Tel.: + 36 1 279-5700
E-mail: info@ifat.hu
http://kki.hu

ISSN 2416-0148
https://doi.org/10.47683/KKIElemzesek.KE-2022.17

Abstract: The economic development of Southeast Asia is increasingly dependent on establishing a cutting-edge digital infrastructure. In some segments of digital infrastructure, for example, data centre operations, the presence and strategy of the two nations' tech companies in Southeast Asia has mainly been driven by market considerations. As for smart and safe city solutions, submarine internet cables, and 5G infrastructure, investment projects are linked to security concerns to a greater extent and are increasingly affected by the tech rivalry of the two great powers. The maze of geopolitical and business motivations and interests makes it more challenging for ASEAN nations to navigate the tech war and face the dual challenge of rapidly developing the digital infrastructure and avoiding taking sides in tech decoupling. The lack of global legislation on digital issues enables great tech powers to push their own data governance models. An intensifying clash between the US and China over data governance concepts would pose a risk to the evolution of adequate local legislation in the ASEAN region.

Keywords: China, USA, ASEAN, tech war, digital infrastructure, data governance

Összefoglalás: *Délkelet-Ázsia gazdasági fejlődése egyre inkább függ a korszerű digitális infrastruktúra kiépítésének sikerétől. Egyes területeken, mint például az adatközpontok esetében, az USA és Kína technológiai vállalatainak jelenlétét és stratégiáját elsősorban piaci megfontolások vezérlik. A smart city és safe city projektek, a tengeralatti internet kábelek és az 5G infrastruktúra terén azonban a beruházási projekteket már erősebben befolyásolja a két nagyhatalom tech háborúja. A geopolitikai és üzleti motivációk és érdekek keveredése miatt nehezebb az ASEAN országoknak helyes stratégiát választani és kezelni azt kettős kihívást, hogy gyors ütemben fejlesszék digitális infrastruktúrájukat, ugyanakkor elkerüljék, hogy az USA vagy Kína oldalára álljanak a technológiai szétválásban. A digitális folyamatok globális szabályozásának hiánya lehetőséget teremt a két nagyhatalom számára, hogy saját adatszabályozási modelljüket igyekezzenek elterjeszteni. Az USA és Kína közti esetleges erősödő összeütközés ezen a téren veszélybe sodorná a megfelelő helyi szabályozás kifejlődését az ASEAN régióban.*

Kulcsszavak: *Kína, USA, ASEAN, technológiai háború, digitális infrastruktúra, adatszabályozás*

INTRODUCTION

The enormous demand for infrastructure development in Southeast Asia is a recurring topic of policy briefs and studies focusing on the region. Beside the need for roads, railway lines, ports, and water treatment facilities, the economic

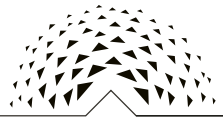
development of the region is increasingly dependent on establishing a cutting-edge digital infrastructure. According to estimates from global consulting firm AT Kearney, by 2025 the 5G rollout could increase enterprise revenues by 18-22% in the ASEAN countries. Indonesia is expected to benefit the most, followed by Malaysia, Singapore, and Thailand. To fulfil this potential, mobile operators in the region will have to invest roughly USD 10 million into 5G infrastructure by 2025.

Therefore, it is not surprising that Southeast Asia is increasingly becoming an arena for competing telecommunication superpowers. Due to the escalating tech war between the US and China, digital infrastructure development has become a highly politicised issue around the globe, to which the ASEAN region is particularly exposed. Beyond the physical infrastructure, the accelerating digital transformation in Southeast Asia makes adequate data governance more important than ever. However, although this issue poses a challenge of global scale today, and data is the lifeblood of digital economy, global governance on digital issues has been unable to keep up with the pace of technology development. This provides room for great tech powers to push their own data governance models and thereby project their influence in the data-driven global economy. This can is the strategic level of the US-China tech rivalry to which the ASEAN region is increasingly exposed.

This two-part policy brief explores whether the escalating tech war creates opportunities or risks for the ASEAN region. Part 1 evaluated the US-China tech rivalry at the corporate level, also exploring its consequences for Southeast Asia. Part 2 of the policy brief analyses the implications of the tech war for the region in the field of digital infrastructure and data governance. Within digital infrastructure, the policy brief focuses on 5G rollout, the development of submarine internet cables, data centres, and smart city solutions.

FROM BUSINESS TO GEOPOLITICS: MOTIVATIONS IN BUILDING DIGITAL INFRASTRUCTURE

Following Part 1 of this policy brief, which focused on the company-related aspects of the US-China tech competition, this part of the analysis looks at data centre operations, an item of digital infrastructure that is also often linked to Big Tech. When analysing the competitive landscape, it is quite clear that both US-based and Chinese tech companies are active in Southeast Asia as they react to the expansion of the market and try to benefit from the digital transformation in the region. Google and Facebook both operate data centres in Singapore and plan to set up another one in Indonesia. Microsoft has similar plans regarding the country. As for China, Tencent has two data centres in Bangkok and plans to open its second one in Indonesia as well. Alibaba also is expanding its data centre operations in Thailand.



While establishing data centres is mainly driven by the market strategies of large technology companies, political considerations and tech rivalry is already reflected in building smart and safe cities. Critics say that related technologies are potential tools for digital authoritarianism and leave countries vulnerable to cyber-attack. The tech decoupling of the two great powers has generated an international debate on the export of Chinese technology and the surveillance practices related to smart and safe city solutions. There is a growing fear that by selling smart city projects, Chinese companies assist Beijing in the struggle for global dominance in setting technology standards. As Chinese companies have been in the crossfire of critics and have received much media attention recently, it might seem as if they dominated the global market, especially the neighbouring region of Southeast Asia. However, the real competitive landscape looks quite different both globally and in the ASEAN region. While due to Western critics Huawei has gained global fame among smart and safe city solution providers, several rankings prove that there are more US-based companies among the leading enterprises in this sector. According to Navigant Research, Cisco and IBM can be considered leaders in the smart city business, while Huawei is a contender. Meticulous Research also places several US-based enterprises in the top 10 companies, while China is only represented by Huawei. The competitive situation in Southeast Asia does not reflect a Chinese dominance, either. Since its establishment in 2018, the ASEAN Smart Cities Network (ASCN) has launched several pilot city projects. According to a study from ISEAS Yusof Ishak Institute, out of the twenty projects launched by 2019, Chinese companies were involved in four, while their US counterparts participated in three. Japanese companies are also strongly represented on the list, which shows that this business is a multiplayer game in Southeast Asia. Moreover, in some projects Chinese technology providers collaborated with US-based and German companies, questioning the perception that the smart and safe city business is about taking sides in the great power rivalry.

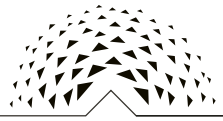
Submarine internet cables are also becoming an increasingly politicised segment of digital infrastructure development. Today, roughly 98% of the world's internet traffic and telephone communication flows through undersea cables. Although they can be considered highly critical digital infrastructure, international regulation provides low-level guarantees to protect them from sabotage and espionage. Even the countries that are connected to multiple cables and therefore have the opportunity to reroute data traffic consider cable damage a critical threat. Western analysts and politicians tend to suppose that China considers submarine cables strategic assets that could be tapped or severed in any future conflict. These concerns are reflected in the statement of former US Secretary of State Mike Pompeo, who highlighted undersea cables as an aspect of US-China tensions and declared that the US needs to "ensure the undersea cables connecting our country to the global internet are not subverted for intelligence gathering by the People's Republic of China at hyper scale". So much is certain

that in 2015 China started to build its first international undersea cable that would carry data between the country and the ASEAN nations. Since then, China has built several submarine cables that connect ASEAN countries or the islands of the Philippines or Indonesia. The launch of the Digital Silk Road accelerated China's submarine cable building activity worldwide, with Huawei Marine at the forefront of the expansion. Before being sold to the Hengtong Group in 2020, Huawei Marine laid transcontinental connections that avoid US and allied territory and could become even more valuable during a conflict.

The US regulators took Mr. Pompeio's statement seriously and started to block any direct cables to the Chinese mainland or Hong Kong and push Chinese partners out of cable projects. This is what happened to a project of Facebook, Amazon, and China Mobile, which aimed to lay down a cable connecting San Francisco and Hong Kong, as US officials voiced concerns that a connection to China via Hong Kong would jeopardize data security. Facebook and Amazon had to amend their investment plans and requested approval from the US government to operate a new cable between the Philippines and California after China Mobile had quit the project. In addition, US tech behemoths are engaged in building further cable connections between the US and Southeast Asia. People in much of the ASEAN region primarily access the internet through mobile data, and any new cable project provides an opportunity to improve access. Facebook is one of the anchor investors in the BiFrost cable system, expected to be ready for service from 2024, which will connect Singapore, Indonesia, and the Philippines to the West coast of the United States. Google is involved in the Apricot cable system, which is also planned for 2024 and will connect Singapore, Indonesia, and the Philippines. As an investor Google is engaged in the Echo cable project, which will connect Singapore and Indonesia directly to the United States.

Within digital infrastructure development, 5G rollout has probably received the most attention worldwide over the past few years. This was mainly due to the fact that 5G technology and infrastructure has become the most prominent battlefield of the US-China tech war. The concerns mostly derive from the nature of the technology. Unlike earlier network generations, 5G architecture applies technologies that allow providers to access and analyse the chain of networks from users to data storages. This new feature of the network has generated an international debate on whether mobile operators should partner with Chinese 5G vendors, resulting in a US-led global campaign against Huawei.

In the ASEAN region, Huawei and Chinese telecommunication companies are welcomed in general. Until recently countries were open to Huawei technology, and they included Chinese vendors in the bidding process. Anti-Huawei sentiment was growing only in Vietnam, territorial disputes in the South China Sea driving most Vietnamese telecommunication service providers to abandon cooperation with Huawei. Vietnam's largest mobile telecommunication provider, Viettel, for instance, has been conducting 5G testing in partnership with Ericsson and Qualcomm since November 2020. Nevertheless, in a Bloomberg interview Viettel's CEO underlined



that the decision not to use Huawei for its 5G networks was a technological one and not tied to geopolitical considerations or the US ban on the Chinese company. Indonesia has opted for a different strategy. The president of Telkom Indonesia, the country's leading phone carrier, left the door open for Huawei in 5G regardless of the US restrictions on the company.

Nevertheless, data from the ISEAS Yusof Ishak Institute show that starting from mid-2020, many telecommunication providers in the region have begun to diversify away from Chinese technology. Singapore is a good example for the trend, as its largest telecommunication provider, Singtel, selected Ericsson in 2020 as the vendor to build the company's 5G infrastructure network, while other local service providers decided to partner with Nokia. The trend is also reflected in the State of Southeast Asia Survey Report 2020, showing that in seven ASEAN member states Samsung is a more preferred 5G developer than Huawei. Respondents preferred the Chinese company over Samsung only in Cambodia, Laos, and Malaysia. US companies were preferred over their Chinese counterparts in Vietnam and the Philippines.

Despite the recent diversion away from Huawei among Southeast Asian major mobile network operators, and despite being seen as a trusted partner, Samsung only has a minor presence as a supplier of 5G infrastructure in the region. The same applies for US-based telecommunication companies like Altiostar, Cisco, and Qualcomm. Despite the positive perceptions in Vietnam and the Philippines, these companies have no significant presence as 5G vendors in the region. As US-based telecom companies are lagging behind their Chinese, European, and Korean counterparts in terms of 5G technology patent registrations, their influence will likely remain limited on 5G rollout in the ASEAN region.

COMPETING DATA GOVERNANCE MODELS

As highlighted in the introduction, global governance on digital issues has been unable to keep up with the pace of technology development, creating one of the greatest challenges for the new economic era. In the absence of a globally accepted data governance model, countries have to make a choice between Chinese and Western paradigms. The EU's approach puts individual rights in the focus of data protection frameworks. The European Union's General Data Protection Regulation (GDPR) represents a high level of standards in managing the personal data of EU citizens. The United States has no federal policy on the protection of data privacy, only state-level regulations and private-sector practices. China, on the other hand, considers data as a strategic asset of the state that provides advanced privacy protection of individual and business data but allows government surveillance at the same time. As the Center for Strategic and International Studies points out, all three of these models have some traction across the Asia-Pacific region. The negotiation of trade agreements and establishing non-binding principles are

the main tools for developing data governance in the region. Among the ASEAN countries, Singapore has been a frontrunner in pushing the data governance program, and it has made considerable efforts to build international standards and interoperability through digital economic agreements. The ASEAN itself has approved a Data Management Framework (DMF) and also proposed a Model of Contractual Closes (MCC) for cross-border data transfer in 2021. The DMF provides ASEAN companies with a detailed guide on setting up a data management system, while MCCs function as templates for contractual terms and conditions that businesses may adopt or modify in their own legal agreements.

As for the role of free trade agreements (FTAs) in developing unified data governance standards in the region, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) can be considered the world's leading trade agreement in the treatment of data and has become a global benchmark of its kind. However, only four ASEAN member states are included, while all ASEAN countries participate in the Regional and Comprehensive Economic Partnership (RCEP) led by China. Nevertheless, the RCEP is far less ambitious in terms of digital issues than other trade agreements in Asia, which reflects China's more prohibitive approach to data, especially the control of data within its borders. At the same time, China's data governance model has not been fully adopted by the RCEP, and the country is expected to promote its concept of data sovereignty bilaterally among like-minded states instead. The case of Vietnam indicates that receptivity is definitely there: on 1 June, 2017, China's new Law on Cybersecurity came into effect. Five days later Vietnam's Ministry of Public Security sent its own proposal regarding a draft of the Cybersecurity Law to the Vietnamese government, which was almost identical to that of China. Officials of the Vietnamese ministry admitted that, among others, they had studied the new Chinese legislation prior to preparing their own proposal.

China has been actively promoting its own concept of 'data sovereignty' at a global level as well. This is reflected in the Global Initiative on Data Security, unveiled by Foreign Minister Wang Yi in September 2020. At the same time, Chinese tech companies that are involved in building digital infrastructure in Southeast Asia are subject to the data governance legislation of China, which means that these companies as investors contribute to spreading the Chinese model in the region. Considering the enormous demand for building digital infrastructure, developing ASEAN countries are unlikely to refuse Chinese investments solely because they oppose China's data governance concept.

The US has a particular interest in blocking the extensive adoption of China's data governance model in Southeast Asia. Doing so would harm the United States' economic interests in the region, and it would give China an advantage in the norm-setting competition in one of the fastest-growing digital economies globally. As the United States does not have a unified federal-level

model of legislation on data privacy, promoting its data governance program in the ASEAN region seems more challenging. Moreover, disparities in the development of the digital economy and in the economic exposure to China make it even more difficult to build a regional approach to data governance. On the one hand, the US tries to manage these challenges by teaming up with like-minded partners, e.g. South Korea or Japan, to support regional initiatives and partner with Singapore in establishing an ASEAN-Singapore Cybersecurity Centre of Excellence. On the other hand, the US channels its influence towards ASEAN's digital economy via the Digital Connectivity and Cybersecurity Partnership, which aims to increase the adoption of cybersecurity best practices in targeted countries as well as provide export market access to US companies in Southeast Asia.

CONCLUSIONS

This two-part policy brief explored whether the escalating tech rivalry between the US and China is creating opportunities or risks for the ASEAN region. The findings of Part 1 highlighted that the presence and strategy of the two nations' tech companies in Southeast Asia has mainly been driven by market considerations. This is also true for some segments of digital infrastructure development, such as data centre operations. In addition, there are multiple examples that US-based and Chinese companies cooperate in some digital infrastructure development projects in the ASEAN region. In terms of smart and safe city solutions, the market expansion strategies of tech companies play a major role, although these development projects are linked with security concerns to a greater extent and are increasingly affected by the tech rivalry of the two great powers. This is even more evident in the case of submarine internet cables. Weakly protected by international regulation, regional development of this critical digital infrastructure is also determined by corporate market strategies and the technology decoupling efforts of the two great powers. Currently, 5G rollout is the segment of digital infrastructure development where it is the most difficult to make purely market-driven investment decisions. At the same time, this is the sole field of digital infrastructure development, in which the presence of the US significantly lags behind that of China in the ASEAN region. It is important to note that the competitive landscape in general looks much more balanced between the two great tech powers than is often suggested by media reports.

Nevertheless, making long-term and cost-effective investment decisions will become more difficult in those fields of digital infrastructure that are increasingly determined by great power tech rivalry in Southeast Asia. The mixture of geopolitical and business motivations and interests make it more challenging for ASEAN nations to navigate the tech war and face the dual challenge of developing digital infrastructure rapidly and avoiding taking sides in the rivalry. Diversification could

be an adequate strategy to decrease exposure to one of the great tech powers, and it seems to work in the case of the smart city pilot projects of the ASEAN Smart Cities Network. Theoretically, 5G could also be a field of diversification, as mobile network operators benefit from a multi-vendor model. However, opportunities for such a strategy could narrow if the tech war escalates further.

Furthermore, the real challenge for the region is to develop a harmonised data governance system that contributes to the integrity of the ASEAN nations and reflects the interests of the intra-ASEAN digital economy. In that sense, an intensifying clash of the US and China over data governance concepts would pose a risk to the evolution of an adequate local legislation. Therefore, the ASEAN nations have particular interest in avoiding a single narrative becoming dominant globally.