

PANDEMIC, CHINA-US RIVALRY AND HUAWEI'S 'SAFE CITIES' IN SOUTHEAST ASIA

Mateusz Chatys

October 2020

SUMMARY

The coronavirus pandemic has made the rivalry between China and the United States even fiercer. While China has managed to take control of the transmission of the virus relatively quickly, as declared by the Chinese authorities, the United States is still unable to stabilize the situation and sees the only salvation in the rapid development of a vaccine. Everything indicates, however, that the Chinese model based on advanced surveillance technologies operating within the Safe City platforms, supported by tracking systems, has fully exposed the weaknesses of the West. One of the biggest beneficiaries of the pandemic will be Chinese technology companies and then China's model of pandemic crisis governance, which will use the still present fear of the pandemic to implement the solutions they propose. One of the main recipients will be the countries of Southeast Asia, because of the cultural similarity, as well as favorable economic terms of cooperation. Despite the paralysis related to the pandemic and the turmoil surrounding the presidential election, the United States is trying hard to limit the reach of Chinese technology giants by sanctions and fueling concerns about a potential espionage threat. While such arguments have been successful in the case of Australia and Japan, most Southeast Asian countries cannot afford the luxury of arbitrarily rejecting cooperation with China. Especially since Beijing has a vast range of tools, where the core is the Safe City platform, that will gradually increase the access of Chinese tech giants to Southeast Asian markets and further increase China's model in the region.

INTRODUCTION

Under the Belt and Road initiative (BRI), addressed mainly to developing countries, and along with a vision of infrastructural development, China tries to export its technological solutions, primarily in the field of various types of Artificial Intelligence (AI) software and surveillance infrastructure. On the one hand, the development of a surveillance infrastructure under the umbrella of Safe/Smart City projects and the collection of data about its citizens made it possible to further develop sophisticated software and hardware from such areas as the Internet of Things (IoT) and the AI.

The pandemic situation has strengthened the tendency to implement the China Model based on social control by advanced technology, which allows the government to cross privacy borders. In other words, vaccination should not be seen as the primary issue in the post-COVID world but rather further challenges to liberal values and the promotion of authoritarian regimes. Such outcomes may be particularly pronounced among the nations of the Global South the characteristics of which make them exceptionally vulnerable to solutions proposed by China and which are the main recipients of the BRI followed by Digital Silk Road (DSR).

The question arises as to whether the American policy primarily based on fueling concerns about potential security threats by Chinese tech companies and setting an ultimatum over the future of intelligence cooperation with the United States is sufficiently effective in the case of the Southeast Asia region. Based on the reaction of Southeast Asian countries to the Chinese strategy to combat the pandemic, it can be tempting to predict which model of technological development - Chinese or American - along with the management tools which come with it, will be further developed in this region. This is a particularly important issue because an intensifying US-China tussle to dominate technological standards will force countries to take sides, which may lead to the division of the world



Is the American policy, primarily based on fueling concerns about potential security threats by Chinese tech companies and setting an ultimatum over the future of intelligence cooperation with the United States, sufficiently effective in the case of the Southeast Asia region?



into different industrial blocs. This, in turn, may consequently paralyze global supply chains, the development of multilateralism, and the entire globalization process.

THE DIGITAL CHINA MODEL IN THE TIME OF COVID-19

When it comes to Beijing's technological expansion, it is identified mainly with the controversy over the potential effects of cooperation with companies such as Huawei or ZTE in the field of installing new generation high-speed 5G Internet infrastructure. The greatest concern is potential espionage activity conducted by tech companies on behalf of the intelligence agencies of the People's Republic of China. This is especially evident in the light of the 2014 Counter-Espionage law that states that "when the state security organ investigates and understands the situation of espionage and collects relevant evidence, the relevant organizations and individuals shall provide it truthfully and may not refuse." Moreover, according to Art. 7 of the 2017 National Intelligence Law "any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law". On this ground, and due to the past experience of people in charge of such companies as Huawei, Washington tries to encourage as many countries as it can - particularly among its allies - to resign from any form of cooperation with the Chinese tech giant.

In the time of the pandemic, the Chinese government rapidly mobilized a vast array of surveillance tools, ranging from dense networks of security cameras, advanced facial recognition software and location-tracking apps to flatten the curve of coronavirus infections. It saved the Chinese Communist Party from dramatic epidemiological effects, and more importantly from the loss of legitimacy of power, the more so since, in its initial stage, the coronavirus pandemic was downplayed by the Hubei authorities. The Chinese model of crisis management during the coronavirus pandemic accelerated the normative challenge to the validity of the liberal international order, the main architect of which, after the end of the Cold War, was the United States. In the case of China, there are legitimate concerns that the procedures put in place to quickly control the pandemic will remain in use even after the development of a COVID-19 vaccine. This is evidenced, for instance, by the statement of Hangzhou's Communist Party secretary, which expresses the belief that the application monitoring the health of the city's residents should be used

on a permanent basis. The Chinese pandemic strategy, whether we like it or not, has become a role model for other countries that have had to confront the spread of coronavirus. Although they did not directly use Chinese technological solutions, they began to create their own, similar to those used in China, such as smartphone applications monitoring health or people with whom phone owners had contact. As Chinese surveillance technologies and data collection protocols have proven to be extremely effective in containing the spread of COVID-19, their wider use could gain global legitimacy. All the more so as the Chinese model received official support from the director general of World Health Organization (WHO) which is the directing and coordinating authority on international health within the United Nation system, especially since the Chinese government is taking the leading roles in the UN agencies.

The Chinese pandemic strategy, whether we like it or not, has become a role model for other countries that have had to confront the spread of coronavirus.

CHINA'S TECHNOLOGICAL EXPANSION AND THE AMERICAN RESPONSES

The importance of technological expansion can be seen in the document from 2015 entitled "Vision and Actions on Jointly Building Silk Road Economic Belt and 21st-Century Maritime Silk Road" issued by the National Development and Reform Commission, Ministry of Foreign Affairs, and Ministry of Commerce of the People's Republic of China, with State Council authorization. Among others, there was a reference to improving international communications connectivity, and creating an Information Silk Road in order to expand information exchanges and cooperation among BRI countries. The Chinese side acknowledged that economic growth will be stimulated by implementing the new generation of the Internet, which is an essential element in the further development of advanced technologies and is also a potential source of profit from the rapidly growing Internet economy. Moreover, the value of the 5G infrastructure market in the six most developed countries of Southeast Asia (Indonesia, Malaysia, Philippines, Singapore, Thailand, Vietnam) in 2019 amounted to USD 98 billion, and it is estimated that in 2025 it will increase to USD 304 billion. Accordingly, Huawei is setting up innovation

centers and technology hubs in the region to help develop technological capabilities, but also to consolidate its position among Southeast Asian countries. That is why, for instance, Huawei is investing in a 5G ecosystem innovation center at the Digital Economy Promotion Agency and created OpenLab for USD \$15 million in Thailand. Huawei OpenLab was also established in Singapore.

The major characteristic of China's expansion is the offering of comprehensive platforms, like smart/safe city, containing a number of technologically advanced solutions, such as artificial intelligence software, tracking systems or surveillance infrastructure. In 2019, Chinese technology was already used by 47 out of 65 countries. Chinese tech companies such as Huawei, Hikvision, Dahua and ZTE completely dominate the reach of their AI technologies for surveillance, as they supply to 63 countries. It is worth noting that as many as 36 are signatories to President Xi Jinping's flagship geopolitical project, the BRI. Furthermore, the undisputed leader is Huawei Technologies Co., which cooperates with at least 50 countries. The Chinese company Hikvision, which has sold its technology to 15 countries, is in second place. Finally, the third place was taken by a non-Chinese company, namely the Japanese NEC Corporation with the result of 14 countries. For the record, the American IBM Corp. supplies AI surveillance technology for 11 states. The data from the report shows that, unlike the United States, Beijing has an extensive and coherent strategy for its technological expansion, and the success of the Chinese campaign against the coronavirus pandemic has become the best advertisement for solutions proposed by Chinese companies.

In order to better understand the Chinese model of technological expansion, it is necessary to carefully examine the measures taken by Beijing to fight the coronavirus pandemic with a special emphasis on tracking systems. At the beginning of October 2020, at least 120 such applications were active in 71 countries, including South Korea, Malaysia, Thailand and Singapore. In Asia alone, there are 21 examples of digital tracking, five physical surveillance and 36 contact tracing apps. Digital infrastructure of the tracking system enabled and activated by the government was also supported by private companies. However, it is worth mentioning that some of them contain a privacy policy and others don't, which should be noted by users of this type of apps - especially since,

in countries such as Indonesia, Brunei, and Thailand, only applications without protocols ensuring the privacy of the collected data are available. The lack of any alternative confronts citizens with the choice of whether they want to contribute to the flattening of the COVID-19 infection curve or protect their privacy. In Western countries, the choice would be obvious, but considering the cultural determinants in Asia, it can be assumed that a large part of society will be willing to sacrifice their right to privacy for the benefit of the public. It is therefore one of the many reasons why the Chinese model, despite a number of threats and doubts, can be successfully implemented in Southeast Asia.

In the meantime, Washington is consistently putting more Chinese companies on its blacklist to limit the possibility of their further development, and the violation of the intellectual property from American companies, and to prevent the construction of strategically sensitive infrastructure in the United States. Moreover, the US government has been systematically raising the concerns of other governments over the transparency of Chinese companies' activities and the risk of their cooperation with the Chinese government or intelligence agencies. To back up its argument, Washington makes the future of intelligence cooperation with other countries dependent on whether they decide to use Chinese technologies. While countries such as Japan and Australia quickly complied and banned the construction of 5G infrastructure in cooperation with Huawei, other American allies are not so clear-cut.

Washington criticizes Huawei's policy, arguing that it stands against values such as transparency, diversity of opinion, interoperability, and respect for human rights. Policy makers from the United States discourage use of Chinese 5G infrastructure but are unable to provide any alluring alternative themselves, as other companies that have this type of technology (although not at the same stage of advancement as their Chinese counterparts) are Swedish Ericsson and Finnish Nokia. The lack of the American contribution in this area, despite the huge funds allocated to R&D, in 2018 it was USD 582 billion (for comparison in China it was USD 468 billion), does not give the Southeast Asian countries a lot of choice, and as the popular saying goes "the absent are always in the wrong".

Notwithstanding, it must be remembered that the governments of Southeast Asian countries will be more inclined to prefer economic arguments over political ones. In most cases, they cannot afford to stall for time when it comes to technological development until the United States comes forward with their own propositions, which will certainly be much more expensive than those proposed by Beijing. Chinese companies that obtain government subsidies can offer very competitive prices, which is often the main reason

Notwithstanding, it must be remembered that the governments of Southeast Asian countries will be more inclined to prefer economic arguments over political ones.

for cooperation with companies such as Huawei, which, according to the 2019 report, has helped more than 200 cities across over 40 countries and regions implement smart city projects. On the other hand, the presence of the United States in this area in Southeast Asia is limited to Singapore and Thailand.

HUAWEI 'SAFE CITY' AS A PERFECT TOOL TO FIGHT THE PANDEMIC?

Smart cities incorporate many emerging technologies, from facial recognition systems and AI cameras to big data analysis. What is important is that the new generation of the Internet - 5G - enables the efficient functioning of all these elements. It is also worth paying attention to the distinction between "smart" and "safe" city categories. The first is primarily aimed at automating municipal functions while also incorporating surveillance functions. On the other hand, the safe city in most cases is focused on tasks related to surveilling and monitoring the population. The Safe City platform collects, integrates, and analyzes data from a wide range of sources, for example criminal records, other government databases, networked surveillance cameras, facial and license plate recognition applications, data labs and includes intelligence fusion capabilities and portable rapid deployment systems for use in emergencies. According to Huawei's description, "Safe City" (*anquan chengshi*) is providing "solutions that enable crucial visualization and convergence to maximize public safety" as well as "enabl[ing] advance prevention, precise resource allocation, efficient analysis, visualized command, and efficient coordination among multiple departments. They help governments reduce

crime rates and prevent and respond to crises more effectively, ensuring a safer environment". In the characteristics of the "Safe City" platform, how it increases the capabilities of authorities to ensure the safety of its citizens was emphasized. Although the period of the pandemic has shown that this is absolutely true, as it allowed for quick detection of disease outbreaks and preventive action in the form of quarantine for people at risk of infection, it is worth bearing in mind that the tools offered by this platform have many possible applications. Therefore, they can also serve the authorities to increase their control over citizens and limit their civil rights, as seen in China. This, in turn, may lead to the degradation of political systems and their transformation into authoritarian regimes.

According to the crime index, the three most dangerous countries in Southeast Asia are Malaysia, Cambodia and Vietnam. The problem of crime in Malaysia is noticed by policymakers, as evidenced by extensive cooperation with Chinese technology companies. For example, the Auxiliary Force (AFSB), part of the Royal Malaysia Police Cooperative, has been equipping its officers with cameras that use facial recognition capabilities designed by the Chinese AI start-up Yitu Technology. Malaysia is also working with China to implement the smart / safe city platform. In addition, authoritarian governments such as those in Vietnam and Cambodia see these solutions as a way of managing nationalism as well as maintaining and potentially strengthening their grip on power at the expense of their citizens' rights to privacy, even as they officially highlight other reasons such as the importance of crime control for public safety and attracting new foreign investments. Hence, such solutions as "Safe City", proposed by Huawei, are very popular. One of the most striking examples of such cooperation is the "Safe Philippines Project" worth over USD 400 million, where USD 24.7 billion will be covered by the Filipino government, while the rest will be paid through a soft loan from China Eximbank (wholly owned by the Chinese Government), according to the Department of the Interior and Local Government. The contractor of the project is the China International Telecommunication Construction Corporation (CITCC) which will provide equipment along with Huawei. The project will utilize high-definition and advanced CCTV cameras (around 12,000) to curb crime, especially drug crime, as evidenced by the flagship project of "war on drugs" implemented by President Rodrigo Duterte. In addition

to the Safe Philippines Project, it is worth noting that the two main domestic providers of telecommunications services in the Philippines – Globe Telecom and PLDT – use Huawei's infrastructure. Moreover, the government approved the installation of communications equipment on army bases by Dito Telecommunity, a consortium formerly known as Mislattel, which is part-owned by China Telecom. As such, it can be seen how closely the individual segments of modern technologies are interconnected. The implementation of one system is followed by the execution of another, as is the case of 5G infrastructure and the Safe City platform. It is also obvious that if the hardware and software supplier for several solutions is the same company, the costs of such a venture are much lower than for many different suppliers where there is no compatibility.

CONCLUSIONS

As triumphantly announced by Beijing the coronavirus pandemic has clearly demonstrated the superiority of the Chinese model over the Western, through the use of tracking systems and smart / safe city platforms. Most likely, one of the main effects of the pandemic will be the faster and deeper adoption of Chinese technological solutions to prevent devastating epidemiological and economic outcomes of another pandemic in the future. However, adopting such a strategy has both benefits and costs. The technologically advanced solutions proposed by China are characterized by a dual use possibility. In the event of a crisis, they help the government quickly recognize the threat and take appropriate preventive measures, but access to so much data and surveillance capabilities put civil and human rights at risk. The possibilities offered by this type of technology may lead to the degradation of the political system and transformation towards China's model, rather than the liberal values.



The possibilities offered by this type of technology may lead to the degradation of the political system and transformation towards China's model, rather than the liberal values.



countries in terms of data privacy, data security, and resilience to hacking and other cybersecurity risks. It turns out, however, that in the era of the COVID-19 pandemic, this may be an even more difficult task. Despite underestimating the first reports of the coronavirus pandemic, Beijing managed to contain the spread of the virus in the country relatively quickly, although it used a whole range of tools at China's disposal, including AI-powered public security platforms to cloud-linked medical software.



**CENTRE FOR
ASIAN AFFAIRS**
University of Lodz

RESEARCH OPINIONS ADVICE

FIRST OF THIS KIND UNIVERSITY BASED
THINK-TANK IN POLAND

OPINION-FORMING UNIT

POLITICAL AND BUSINESS ADVICES

ASIA EXPERIENCED TEAM

www.osa.uni.lodz.pl

