# What's Next for 5G in Southeast Asia?

*By Manoj Harjani and Gatra Priyandita*

## SYNOPSIS

*Given their development needs, Southeast Asian countries have adopted a nuanced and measured approach towards security concerns raised over the use of 5G telecom network equipment supplied by Chinese companies like Huawei and ZTE. Nevertheless, this does not mean that the region lacks an awareness of the risks involved. Countries with an interest in the security of Southeast Asian telecom networks should look to provide support that accounts for development needs. One promising area could be in adoption of open radio access network (O-RAN) technology, although this is not without challenges.*

## COMMENTARY

In recent months, announcements of successful tests by various Southeast Asian telecommunication companies in RedCap ("reduced capacity") 5G have been a reminder of the region's gradual rollout of fifth-generation networks. RedCap 5G is expected to facilitate a wider range of use cases for 5G, particularly for the Internet of Things, which is currently mostly served by 4G. Nevertheless, most of the region has yet to go beyond trials for 5G, and 4G will remain standard for some time.

In 2022, 5G plans made up just 2.2 per cent (26 million) of all mobile subscriptions (1.14 billion) in Southeast Asia, compared to 4G's 55.7 per cent (637 million). This stands in contrast to East Asia, where 5G made up 29.8 per cent of overall subscriptions (643 million out of 2.16 billion). Southeast Asia's global share is expected to increase but not drastically: by 2028, the region will make up 9.4 per cent of all subscriptions (433 million out of 4.62 billion), compared to 2.7 per cent (26 million out of 951 million) in 2022. Southeast Asia is therefore unlikely to become a significant global market for 5G in the short to medium term.

How, then, should we assess concerns over Southeast Asian use of equipment by Chinese suppliers like Huawei and ZTE? While the idea of "choosing a side" has petered out to some extent, narratives about decoupling or de-risking haven't gone away entirely. For years, the US and others have warned Southeast Asian states that Chinese equipment could facilitate state-sponsored cyber espionage. President Donald Trump's administration tried to convince Southeast Asian countries to limit or ban the use of Chinese equipment in their networks, and recent reports of the Malaysian government allowing Huawei to participate in its 5G rollout have been met with further calls for caution.

**Southeast Asia's Measured Approach to 5G**

Southeast Asian states have responded in different ways to China's expanding footprint in their telecommunications sectors. In 2020, Singapore's leading telcos didn't choose Huawei to develop national 5G networks, with contracts going instead to Ericsson and Nokia. Meanwhile, Vietnam opted to develop its own 5G technology. But Chinese suppliers appear to be mostly pressing on with business as usual – particularly in 4G, which attracts less attention and concern, but also in cloud computing and "smart city" technology.

However, their business-as-usual approach doesn't mean that regional governments aren't worried about the great-power competition over technology. Singapore's Minister for Communications and Information, Josephine Teo, has spoken about the region's desire to ensure that, instead of states "choosing" one vendor or group of vendors, there be "more interoperable systems and standards". This suggests that the region is adopting a nuanced and measured view of the role Chinese suppliers should play in its telecom networks, in contrast to the Western narrative, particularly popular in Washington, that Southeast Asia is at risk of being absorbed into a sphere of influence dominated by China.

It would be prudent to move beyond lecturing Southeast Asian governments about the threat posed by Chinese equipment, which is already well understood. For example, while Indonesia has emerged as a major market for Chinese telecom equipment, cybersecurity officials have shown deep awareness of the risks associated with its use. Nevertheless, meeting critical economic development goals often takes precedence. The cheaper prices offered by Huawei and ZTE – which can be as much as 30 per cent below the market rate – and their support for capability building often make their offers hard to refuse.

Despite lofty visions of using the transformative power of 5G technology to bolster economic growth, most of Southeast Asia is still at least a decade away from full implementation. Considering this, it would be productive for Western governments and their regional partners to focus on providing support that accounts for the region's development to facilitate reduced dependence on Chinese equipment.

**O-RAN as a Way Forward**

One way to do this would be to support the development of open (meaning non-proprietary) radio access network, or O-RAN, technology which is designed for interoperability among multiple vendors. This would allow the region to integrate

smaller indigenous equipment manufacturers into the network that may otherwise struggle to compete against major global suppliers. While Southeast Asian states have been slow in adopting O-RAN technology, some are seeing its potential to help navigate the deepening great-power technology competition. But O-RAN technology and equipment are pricey and regular testing may be out of reach for many countries. Progress on O-RAN technology is something governments interested in supporting Southeast Asia's telecom diversification can encourage.

At the regional level, initiatives such as the ASEAN 5G roadmap should also consider how to incorporate O-RAN technology. The US has already supported an ASEAN study on best practices for implementing 5G in Southeast Asia, which highlighted the potential of O-RAN in the region. The challenge will be in addressing the wide range of concerns among Southeast Asian countries that are at different stages in their development. Sustaining partnerships, dialogue, and capacity-building efforts with Southeast Asian governments for the long term will be critical.

*Manoj Harjani is a Research Fellow with the Military Transformations Programme at the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. Gatra Priyandita is an Analyst with the International Cyber Policy Centre at the Australian Strategic Policy Institute (ASPI). This commentary was originally published in The Strategist, an online publication of ASPI.*