RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg No. 180 – 16 October 2020

Between Byte and Bark: Singapore, US & Chinese Tech

By Shashi Jayakumar and Manoj Harjani

SYNOPSIS

Investment by China's tech companies in Singapore has picked up considerable pace in recent months. Alibaba, ByteDance and Tencent have all made an intent to anchor a presence in Singapore that can tap on Southeast Asia's burgeoning consumer markets. At what price?

COMMENTARY

RECENT ANNOUNCEMENTS of Chinese tech giants Alibaba, ByteDance and Tencent investing in Singapore signal huge opportunities and potentially further cement Singapore's position as a hub where global flows of trade, investment, talent and data can interact productively in an enabling environment.

The flurry of investment will inevitably – given growing discord between China and the United States – pose multifaceted challenges for Singapore's policymakers. American efforts to target China's tech companies have become one of the most visible aspects of a rapidly intensifying strategic rivalry, with a key thrust of the Trump administration's accusations against China being that its technology represents a national security threat.

America's techno-nationalism

The Trump administration has attempted to turn the screw in a variety of ways. Beyond attempting to force a sale of TikTok to an acceptable (read: American) entity, it has used Department of Commerce Entity List designations to limit export of American semiconductor technology that Chinese companies like Huawei – a lynchpin in the global rollout of 5G networks – are reliant on.

Furthermore, the State Department's Clean Network initiative – which initially aimed to remove Chinese 5G technology from America's diplomatic communications systems – has since been expanded to cover mobile apps, app stores, cloud computing services, and even undersea cables.

China has begun responding to what it sees as provocations in a like manner. It plans to launch its own Unreliable Entities List and recently updated its technology export controls, which now include artificial intelligence (AI). China's Foreign Ministry also announced the Global Initiative on Data Security, which comprises an eight-point proposal to develop international data governance rules. This must be construed as a response to the Clean Network initiative and builds on the notion of cyber sovereignty championed by China in recent years.

The stage is clearly set for techno-nationalist lawfare, where legal tools become the means to achieve strategic ends. Beyond trade controls, investments are likely to remain in the crosshairs. The US has already strengthened its foreign investment screening mechanisms and has threatened to delist Chinese firms from American stock exchanges if they do not comply with US auditing requirements by the end of 2021. For its part, China will likely maintain or even expand its negative list which restricts foreign investments in selected sectors.

China's Byte

Some scrutiny of Chinese apps and technology is justified given Article 7 of China's National Intelligence Law, which compels compliance with requests from state intelligence agencies. Doubts over the independence of China's tech companies operating globally will also grow following the Chinese Communist Party (CCP) publishing the "Opinion on Strengthening the United Front Work of the Private Economy in the New Era".

The new guidelines aim to bring China's burgeoning private sector under tighter supervision of the CCP. Tech companies that could have eschewed direct links to the CCP and operated with some distance in the past may no longer have that option in future.

This is added ammunition to sustain future American scrutiny and pressure on its allies and partners, which could extend to technologies such as AI and cloud computing. While Singapore and other Southeast Asian countries have prioritised pragmatism and commercial considerations over geopolitics (as in the case of 5G rollouts), this matters little if the American political calculus overrides rational consideration of actual security threats.

The fact, for example, that TikTok user data is stored in Singapore may come under fire notwithstanding claims that this data is not subject to Chinese law, and despite respected independent commentators such as Ben Thompson observing, correctly, that "far more valuable data than anything TikTok could gather is trivially available to anyone, national security threat or not".

The American point is a simple-sounding one – an expanded Chinese tech presence means a heightened risk of espionage. The outlines of a further argument are coming into focus too – that seemingly non-threatening apps such as TikTok hoover up information, leading to a situation where Beijing has a "profile of every American".

Although there is no evidence of a systematic expansion of China's social credit system beyond its borders, there is concern, as CSIS' Jim Lewis observes, that the Chinese may in time extra-territorialise their surveillance state, leveraging on global deployments of surveillance technology by companies such as Hikvision.

Outlook for Singapore

America's attitude towards countries like Singapore, which have sought to remain neutral in the face of techno-nationalism, will likely evolve to further constrict space to manoeuvre. Besides official pronouncements, American officials and think-tankers have suggested on the conference and track 1.5 circuit that the US will necessarily have to recalibrate, and potentially rethink aspects of security cooperation and its relations with any country that welcomes Chinese technology in 5G or indeed any other area.

The Trump administration also appears to see Southeast Asia as a staging area to face a more assertive China, and Singapore, as one of America's strongest security partners in the region, could increasingly be expected to function as a node in the pushback against China's technological expansion. Earlier this year, for example, Assistant Secretary of State for Political-Military Affairs R. Clarke Cooper warned China over using Singapore's annual Air Show as "a platform for exploitation and theft".

Singapore has been on the radar before too. In 2018, the Trump administration intervened to block Broadcom – then a Singapore-headquartered semiconductor company – from acquiring the American wireless technology giant Qualcomm, citing national security concerns. The fear appears to have been that the sale would weaken American 5G development vis-à-vis China, which was not involved in the proposed sale.

Such seemingly tenuous logic may in time be increasingly evident in other spheres. Current scrutiny over Beijing's Thousand Talents programme is a case in point, and may expand to other countries hosting large numbers of Chinese academics.

Oversight and Risk

Interagency mechanisms that could address these issues, such as the National Security Coordinating Committee and Security Policy Review Committee, already exist in Singapore. These can examine potential threats – from any country – to Singapore's critical information and digital infrastructure and act as decision-making platforms. Necessarily, and unlike the Committee on Foreign Investment in the US – whose decisions are dissected somewhat openly – discussion in Singapore has traditionally occurred behind closed doors.

Policymakers will need to be clear about what the "threat" really is. Beyond security assessments of the technical variety, the long-term implications of foreign technology being embedded in Singapore's socio-political fabric merit closer examination. If technology from any country is deeply embedded and has a persistent slant, there may be socio-cultural ramifications, the long-terms effects of which are difficult to gauge at present.

Should policymakers dismiss the risk, society may over the long-term be shaped by repeated application of messages that are near-subliminal. This may lead to the balkanisation of thinking across different groups who are exposed to particular media. What all stakeholders (and these should include those concerned with Singapore's culture and society) actually need, therefore, is an expanded conception of national security, and innovative, holistic ways of assessing new risks.

Shashi Jayakumar is Executive Coordinator and Manoj Harjani a Research Fellow with the Future Issues and Technology research cluster, S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU).