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

RSIS COMMENTARY

www.rsis.edu.sg No. 092 – 9 May 2019

Can Trust Be Verified? Managing 5G Risk in Southeast Asia

By Donald K. Emmerson

SYNOPSIS

Nothing can fully protect a country from secret malfeasance involving the company it hires to provide and maintain its 5th generation wireless system (5G). But certain steps can lessen the risk. One is to learn how secure the firm's technology is; another is to estimate the chance that the laws and institutions in the firm's home country will prevent the government there from accessing the firm's data and algorithms without the user country's permission.

COMMENTARY

Trust but verify. That mantra from nuclear-weapons negotiation discourse during the Cold War is newly relevant today. Versions of the advice are circulating among governments in Southeast Asia and elsewhere as they weigh the security risks of partnering with this or that company to install the fifth-generation telecommunications technology known as 5G.

It is tempting to believe that a technical solution to the problem of unwanted risk exists — a clever digital tweak that will fully and permanently protect a 5G network's users. It does not. The best one can hope for is a "good enough" balancing of faith and proof that is — arguably, not assuredly — reassuring and realistic. Characteristics of the network-offering company in its home country and of the network-purchasing government in its own country will shape the 5G seller-buyer bargain and its location. This will occur on an eventual spectrum of arrangements between the unwise and the unworkable: unverified trust at one extreme end, trust-eliminating verification at the other.

Enter Huawei

China's Huawei Technologies is an ostensibly private (https://www.nytimes.com/2019/04/25/technology/who-owns-huawei.html) company founded in China's mercantilistic state-capitalist economy by a former People's Liberation Army engineer. Southeast Asian governments are considering whether to rely on Huawei's technology in an upcoming 5G world.

If a potential buyer insisted on continuous verification, Huawei would need to agree to the installation and maintenance of hardware and software designed to expunge from the system any present or future "back door" through which China's Ministry of State Security (MSS) or the Communist Party of China (CPC) could walk.

But even if Huawei agreed, would its software updates uphold that initial consent? Full prudence would oblige the user state to re-investigate the workings of the system whenever Huawei saw fit to alter the code. But whose investigators, employing what possibly proprietary knowledge, how thoroughly, and at whose and what expense?

Scheduled updates aside, if and as adaptive machine self-learning becomes increasingly the norm, 5G software will be continually changing itself, potentially opening new vulnerabilities to breaching and manipulation. And even if every new back door is somehow dismantled or prevented, the MSS or the CPC could simply knock on Huawei's physical front door at the company's headquarters in Shenzhen to ask for access to the system.

Fearing the visitor and obliged to comply with the intrusive prerogatives of the state authorised in China's National Intelligence Law, Article 7 (https://www.chinalawtranslate.com/%e4%b8%ad%e5%8d%8e%e4%ba%ba%e6%b0%91%e5%85%b1%e5%92%8c%e5%9b%bd%e5%9b%bd%e5%ae%b6%e6%83%85%e6%8a%a5%e6%b3%95/?lang=en), Huawei will open the door.

Whom To Trust?

Whom will you trust? And how much? Technical guardrails and patches can reduce but not remove the subjectivity of those necessary questions. In Southeast Asia, differing political and economic contexts will influence the answers. Other things being equal, governments indebted to China may feel less free to turn down Huawei. Lower-income countries may opt for Huawei because it is cheaper to do so. Poorer countries already tilted towards Beijing, such as Cambodia, may hire Huawei on both grounds.

History will also matter. Vietnam recently observed the 40th anniversary of its 1979 invasion by China and the brief war that followed.

Unsurprising in that context, Vietnam has granted its first 5G licence to a homegrown firm, Viettel, and is reportedly open to working with two Scandinavia-based multinationals—Nokia in Finland and Ericsson in Sweden (https://www.cio.com/article/3310197/how-is-vietnam-preparing-for-5g.html).

Huawei, Nokia, and Ericsson are competing neck-and-neck for shares in the global market for the radio access network (RAN) equipment needed to enable 5G transmission. One analyst's estimate of the three companies' shares of 5G

subscribers worldwide in 2023 who will be using their respective RANs has the distribution as follows: Huawei with 25 percent; Nokia and Ericsson each with 23 percent; and the remaining 30 percent split among other firms (https://www.telecompetitor.com/5g-ran-market-share-research-three-vendors-run-neck-and-neck/).

Food For Thought About Policy Choices

Relevant in this context is the devastating review of Huawei in the fifth annual report of the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board (https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-oversight-board-annual-report-2019), released in the United Kingdom on 28 March 2019.

Based on its investigation, the board found persisting "serious and systematic defects in Huawei's software engineering and cyber security competence" resulting in "extensive vulnerability" and "significantly increased risk" for users.

Huawei's products were judged as having "no end-to-end integrity" and the firm's software management was found "defective". The board had only "limited confidence" in Huawei's ability even "to understand the content" of its own products, presumably rendering the company incapable of diagnosing "identified issues" needing remedy.

Lessons To Be Learned

In cybersecurity, because perfection is impossible, it should not be made the enemy of the reasonably good. There is an opportunity here for governments and companies to scale up the methods that HCSEC used and the lessons it learned in the course of its experience investigating Huawei.

Those lessons could contribute to the drafting of a checklist of tests and standards for use by Southeast Asian and other states when choosing between G5 network providers. User states could benefit further by taking into account the trustworthiness not only of a given 5G firm, but of its home government as well.

Vietnamese officials may not have looked up the World Justice Project's 2019 Rule of Law Index of Constraints on Government Powers (https://worldjusticeproject.org/sites/default/files/documents/WJP-ROLI-2019-Single%20Page%20View-Reduced.pdf). It ranks 126 countries by the extent to which the government in each one is held accountable within an effective framework of law that limits its power. Finland and Sweden are respectively 3rd and 4th. The UK is 11th. China is 119th.

This is not an infomercial for Nokia or Ericsson in Scandinavia, nor for HCSEC in the UK. It is just a little food for possible thought about the policy choices that will shape the digital future of Southeast Asia.

Donald K. Emmerson heads the Southeast Asia Program in the Shorenstein Asia-Pacific Research Center at Stanford University, where he is also affiliated with the

Center on Development, Democracy, and the Rule of Law. He contributed this article specially to RSIS Commentary. His edited book, The Deer and the Dragon: Southeast Asia and China in the 21st Century, is forthcoming in 2019.

Nanyang Technological University
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
Tel: +65 6790 6982 | Fax: +65 6794 0617 | www.rsis.edu.sg