Geopolitics & Technology – The Core of the 5G Problem

Lee-Makiyama, Hosuk

2019

Lee-Makiyama, H. (2019). Geopolitics & Technology – The Core of the 5G Problem (RSIS Commentaries, No. 245). RSIS Commentaries. Singapore: Nanyang Technological University.

https://hdl.handle.net/10356/136669

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

RSIS COMMENTARY

www.rsis.edu.sg No. 245 – 5 December 2019

Geopolitics & Technology

The Core of the 5G Problem

By Hosuk Lee-Makiyama

SYNOPSIS

Given how 5G networks underpin our supply-chains, the so-called Huawei problem is unlikely to be a part of a grand bargain between the US and China. However, an exclusion of Chinese 5G vendors may not be an option for Singapore and Europe who must respond by other means.

COMMENTARY

CYBER OPERATIONS are now relatively common strategic instruments deployed by world powers. But in the age of economic statecraft, where commercial interests are at the heart of foreign policy objectives, cyber operations are also a potent tool for industrial policy.

State-sponsored threat groups have collected trade secrets on behalf of their national champions and state-owned enterprises. These operations also often target surprisingly mundane companies in every sector, including chemicals, hotels, business software, airlines or banking.

5G and China-US Decoupling

5G deployment is central to the current United States-China decoupling *leitmotif*, due to how it will increase the overall attack surface. Market forecasts show that the amount of data stored on Cloud will increase by a factor eight, up to 160 zettabytes. The number of connected devices will triple in just three years as the Internet of Things (IoT) connects 26 billion new devices, including gauges, vehicle components, business equipment and household items.

Since most connected items lack the processing power or physical dimensions to host any security applications, the confidentiality of our networks comes down to the 5G network that links the devices.

But the risks are not attributable to just the *amount* of data – it is also *how* we use it. 5G underpins all other layers of critical infrastructure, such as road transports, shipments, financial architecture or utility grids; it enables new industrial applications used for real-time control. The rewards of cyber theft today are primarily valuable information, e.g. plans, blueprints or bids.

However, rivals will soon be able to obtain control over vital business or government functions; or even replicate entire organisations and processes with precise geo-locations, equipment settings and working methods.

These challenges affect all actors and not just China and the US. Competitive industries in regional hubs or knowledge-intensive economies like Singapore are natural targets as well. Estimates by the Centre for Strategic and International Studies (CSIS) in Washington DC show that cybercrime inflicts an annual loss of SG$2 billion in GDP or economic output. If the number is correct, the losses in R&D and job opportunities are equivalent to losing 2,000 employees amongst the country's best and brightest each year to the competitors.

Non-technical Causes to 5G Decoupling

The technical complexity of 5G makes our networks more vulnerable to threat actors, human errors and design flaws. Technical issues may be addressed through type certifications, screening of code, or reviews of supply-chain integrity by the national authorities before deployment but unable to weed out all the risks.

Manufacturers do not just build antennas, racks and base stations; they also maintain, run and update them, continuously under their control. In other words, vendors are trusted to put our national interests and user privacy at the forefront. However, the US National Security Agency (NSA) programs for upstream data collection showed that technology suppliers follow the laws and obligations in their home jurisdictions.

Also, China's new National Intelligence Law forces its businesses or citizens to surrender data or 'communication tools' shipped overseas. More importantly, the vulnerability against such state activities cannot be identified or mitigated by technical means.

Both China and the US' responses to 5G have resorted to modalities of economic statecraft – primarily trade policy instruments like import bans and export licensing. This is as much to protect their data as an attempt to change the parity of competitiveness between them. Both sides harbour strong resentment over the outcomes of the Uruguay Round or China's accession to the WTO, albeit for different reasons.

As both sides seek changes to the current global economic order, and given the strong complementarity of their economies, the decoupling is likely to result in a new mutually acceptable agreement.

However, the case of 5G is different and unlikely to be a part of such an accord. It is not the typical run-of-the-mill protectionism as the US does not even have any manufacturers to protect. Instead, the US and China's telecom standards may even diverge further, to the point where telecom equipment may no longer be interoperable.

Core in International Public Law

Meanwhile, Singapore and the European powers walk a very narrow corridor between the shadows cast by two competing visions – Trump's *America First* and Xi Jinping's *China Dream*. A new 5G risk assessment published by the European Union is forthright enough to admit that foreign intelligence activities pose a threat to its strategic autonomy.

Yet, a full decoupling is not a viable option even in the short-term: Huawei supplies and operates about half of the mobile networks in Germany, where dominant operators are pressured by their shareholders to pay out dividends rather than investing in high-end networks.

The Chinese market is also far more critical to Singaporean and European businesses than for their US counterparts. China accounts for five per cent of Germany's overseas investment stock – compared to just one per cent for the US – while China accounts for some staggering 20 per cent of Singapore's foreign investments. European 5G vendors – Nokia and Ericsson – are now marginalised in the Chinese market, and may not survive without it.

As all nations spy, we can no longer avoid the risks of bulk collection of data in our networks. In response, countries like Japan chose to award 5G licences to the operators with "most secure" components and rollout plans. France has opted to only partially exclude Chinese vendors from sensitive areas, including its administrative centre in Paris; the exclusion also applies to the core networks that funnel more data than the edge.

Limits of Diplomatic Solutions

A recent update of the German telecom regulations requires the operators to diversify amongst its suppliers to avoid becoming "monocultures", although Chancellor Merkel became subject to nation-wide ridicule when the threshold coincided precisely with Huawei's current market shares in German telecom operators.

Unilateral measures like partial exclusions or diversification merely limit the potential damage from breaches and disruptions but do not reduce the risk of incidents. Diplomatic solutions, like intergovernmental "no-spy" agreements, have widely proven to be ineffective. Unlike conventional non-proliferation treaties (that can be verified through site inspections or satellite imagery), there are no effective means to verify compliance with cyber operations.

Unlike other dimensions of US-China decoupling, the 5G problem has a core that is rooted in international public law, namely the right of foreign entities to seek redress in the Chinese legal system. In comparison, the Obama administration reformed several laws to introduce new safeguards after the Snowden revelations, including the

Judicial Redress Act of 2015 that allows designated countries to challenge and seek redress in the case of mishandling personal information by espionage.

The reforms – or concessions – thwarted the threat from several countries that may otherwise have shut down online platforms like Google and Facebook and blocked cross-border data flows for US multinationals. The parallels to the pending blockade against Chinese 5G equipment are conspicuous, and it would be remarkable if China were not asked to undertake equivalent reforms – even for keeping up the appearances.

A failure to make such demands against China would beg the question (from both the general public as well as US officials in Washington DC) why their governments treat Beijing more favourably and more trustworthy than the Obama administration.

Hosuk Lee-Makiyama is the director of Brussels-based European Centre for International Political Economy (ECIPE). He contributed this to RSIS Commentary as part of a series on Geopolitics and Technology.

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