The US-led campaign against the use of technology from the Chinese telecom giant Huawei — the world’s largest provider of telecom technology — in the rollout of 5G mobile networks around the world is shaping up to be a major battle between Washington and Beijing over the future of emerging technologies. Asian countries are struggling not to be sucked into that geopolitical rivalry as they decide who will build their networks.

ESSAYS BY
Henry Farrell & Abraham Newman 8
Andrew Grotto 13
A view from Huawei 16
Danielle Cave 18
Sun-sook Park 24
J. Berkshire Miller 30
Ananth Krishnan 36
Huong Le Thu 40
The Huawei Problem: A Risk Assessment
By Andrew Grotto

At the center of the controversy over whether countries should adopt 5G technology from Huawei is the incontrovertible fact that the Chinese Communist Party expects China’s companies — no matter their sector or whether they are public or private — to do its bidding, whether stealing intellectual property or even engaging in spying for Beijing. This should figure into any risk assessment of doing business with the company, writes Andrew Grotto.

LAST MONTH, amid intensifying criticism from the Chinese government and social media denizens behind the Great Firewall about Cathay Pacific staff taking part in the recent Hong Kong protests, the chairman of the city’s flagship airline told reporters its employees’ political views weren’t management’s business. “We certainly wouldn’t dream of telling them what they have to think about something,” Chairman John Slosar said. “They’re all adults.”

Within weeks, both he and Cathay CEO Rupert Hogg had abruptly resigned. Meanwhile, the Chinese government forced Cathay to ban employees who participate in the protests from servicing flights to the mainland. It also required the airline to submit information on crew members to the government.

The episode is a textbook example of the Chinese government’s practice of coercing companies into doing its bidding, outside of any transparent legal process. Cathay Pacific’s management has not been publicly accused of breaking any laws by permitting its employees to express their political views about freedom and democracy in Hong Kong. Instead, management’s sin appears to be that by treating its employees as any other mainstream, multinational company would — as free-thinking adults — it was insufficiently committed to Beijing’s goal of clamping down on dissent and making the protests go away.

The fact is, the Chinese government considers Chinese companies to be extensions of the state, whether a company likes it or not. And, it is willing to use legal and extra-legal means to impose its will on them. China’s economy may roil like a bubbling capitalist cauldron, but make no mistake: the Chinese Communist Party (CCP) is the chef, and Chinese enterprises are ingredients to be sliced, diced and chopped at the CCP’s discretion. Most of the time, the CCP’s interests and the interests of Chinese enterprises are aligned: make money, grow, support economic development, and so on. But when they aren’t, the safe money is on the CCP’s interests prevailing. Just ask the ousted Cathay executives.

This is why Huawei CEO Ren Zhengfei’s assertion earlier this year that Huawei would “never participate in espionage … [e]ven if we were required by Chinese law” is wishful thinking, at best. As I have argued similarly with respect to the Russian cybersecurity company Kaspersky Labs about its relationship with the Russian government, it doesn’t much matter whether Huawei is an enthusiastic collaborator with Chinese intelligence or a forced conscript. Chinese law gives the government sweeping authority to compel private businesses to support intelligence operations. Huawei’s private lawyers could argue with the government all they want about this. Unfortunately for Huawei, as long as its business operations and personnel are vulnerable to formal and informal forms of coercion by the Chinese government, the company and its executives are virtually powerless to resist the government’s demands.
How Great Is the Risk?

This risk factor attaches to any business dealings with a Chinese company, and to argue otherwise is naive. Instead, the pertinent question is, given this risk factor, what is its magnitude in a given case and can the risk be mitigated? In many cases, perhaps even most, the risk is de minimis, or at least manageable. A baby monitor manufactured by a Chinese company or with Chinese-origin components, for example, might potentially be used by Chinese security services as a clandestine listening device by requiring the manufacturer to install a backdoor prior to shipping or by exploiting a remote patching capability later. For most of the company’s customers, however, the risk of being spied on by the Chinese government is small, because they are not plausible intelligence targets or because exploiting the device wouldn’t lead to much harm in any event. (They can focus instead on other, non-China specific safety, security and privacy risks.)

But for some technologies, the risk is uniquely high and mitigation options restricted. The networking infrastructure and other technology that Huawei supplies fall squarely in this category, especially 5G networks. Occupying the network is the ultimate high ground for an attacker, and 5G networks are especially vulnerable because they are designed to be far more decentralized than legacy networking, which typically has hardware-defined chokepoints, meaning there are far more nodes for a defender to protect. In addition, 5G networking is defined and managed by software, which must be continually updated and patched. This means that the vendor, by definition, will have persistent access to the network’s most sensitive operations and functionality.

But there is more to Huawei than its country of origin and the nature of its wares. The company has also shown a selective approach to complying with the laws of the countries where it conducts business, further calling into question its trustworthiness. Perhaps most famously, Huawei’s CFO was arrested in late 2018 in Canada in connection with alleged efforts to circumvent US sanctions laws. The US Department of Commerce subsequently blacklisted the company from the US market, though the terms of the ban remain murky. And in August, reports emerged about Huawei executives in Africa helping governments there to spy on their political opponents. Huawei has also shown an apparent penchant for espionage, albeit of the corporate sort. It almost certainly stole routing hardware source code from Cisco over 15 years ago. In 2017, a US jury found that Huawei stole trade secrets from T-Mobile and ordered it to pay T-Mobile US$4.8 million in civil damages. The US Department of Justice (DOJ) is now prosecuting Huawei in connection with this incident. And in August, the DOJ filed criminal charges against a researcher who allegedly sought to steal intellectual property on Huawei’s behalf.

Huawei is not alone among Chinese actors in this respect: according to DOJ statistics, two-thirds of its trade secret cases from 2011-2018 involve China.

Does It Matter?

For some customers, these risk factors may not add up to a decision to refuse to do business with Huawei. Different customers will bring different risk tolerances and profiles to bear on such a decision. Huawei gear is often much less expensive than its competition, and it is a sad truth that price often prevails over security. In addition, some customers may not care whether they are vulnerable to Chinese espionage or cyber-attack. Either way, denying the existence of these risk factors is folly.

Of course, China is not the only country in the world that engages in espionage or views offensive cyber capabilities as an important tool in the security arsenal. And Huawei is not an isolated sinner in a sea of saints. Especially for digital technologies, a savvy customer should make investment decisions with these risks in mind for anything that comes into actual or potential contact with its networks. And governments should backstop these decisions with laws and regulations if customers and vendors neglect basic security and privacy responsibilities.

In key respects, the risk factors presented here about Huawei have little to do with the overall technology competition between China and the US. If Huawei were based in Russia — a country whose technology sector poses little competitive threat to American companies — the risks would be comparable in type, and perhaps even more severe in terms of overall threat level. But there would be no debate about the safety, security and privacy risks associated with Huawei equipment if Huawei were not in a commanding position to sell that equipment to customers around the world. Huawei is a poster child for China’s technological ambitions coming to fruition: the company’s revenues have quintupled over the past decade, it makes more mobile phones than Apple, and it is the global leader in terms of market share for mobile infrastructure equipment, edging ahead of Ericsson and Nokia. And while Huawei’s rise is due in no small part to shrewd business decisions, hard-working employees and a commitment to research and development, the company has also broken laws and stolen its competitors’ intellectual property.

Perhaps most saliently, it has also received considerable support from Beijing in the form of subsidized capital and a protected domestic market. The precise scale and scope of the support is unclear, but it appears to be massive. The government began treating it as a national champion in 1996 for the explicit purpose of blocking foreign telecom providers from the Chinese market. More recently, Huawei reports receiving hundreds of dollars in government grants every year, including more than US$220 million in 2018. It also has a US$100 billion line of credit from Chinese state-owned banks that enables it to offer financing to customers at below-market interest rates. Many of the company’s products are priced exceedingly low as well — so low that it is hard to see how Huawei breaks even, let alone turns a profit. It is doubtful that Huawei would be where it is today without the Chinese government’s robust backing for over two decades.

All this makes Huawei an especially better risk pill to swallow for American policy-makers who are also focused on the broader technological competition with China. Indeed, this “Huawei Problem” may be just the beginning of a broader trend, as products of all kinds, from trains to pacemakers, become fixtures in the digital environment as a result of embedded connectivity — and wrapped up in controversy around risk and digital competition.

Andrew Grotto is director of the Program on Geopolitics, Technology and Governance and William J. Perry International Security Fellow at Stanford University’s recently launched Cyber Policy Center. He is also a visiting fellow at the Hoover Institution.