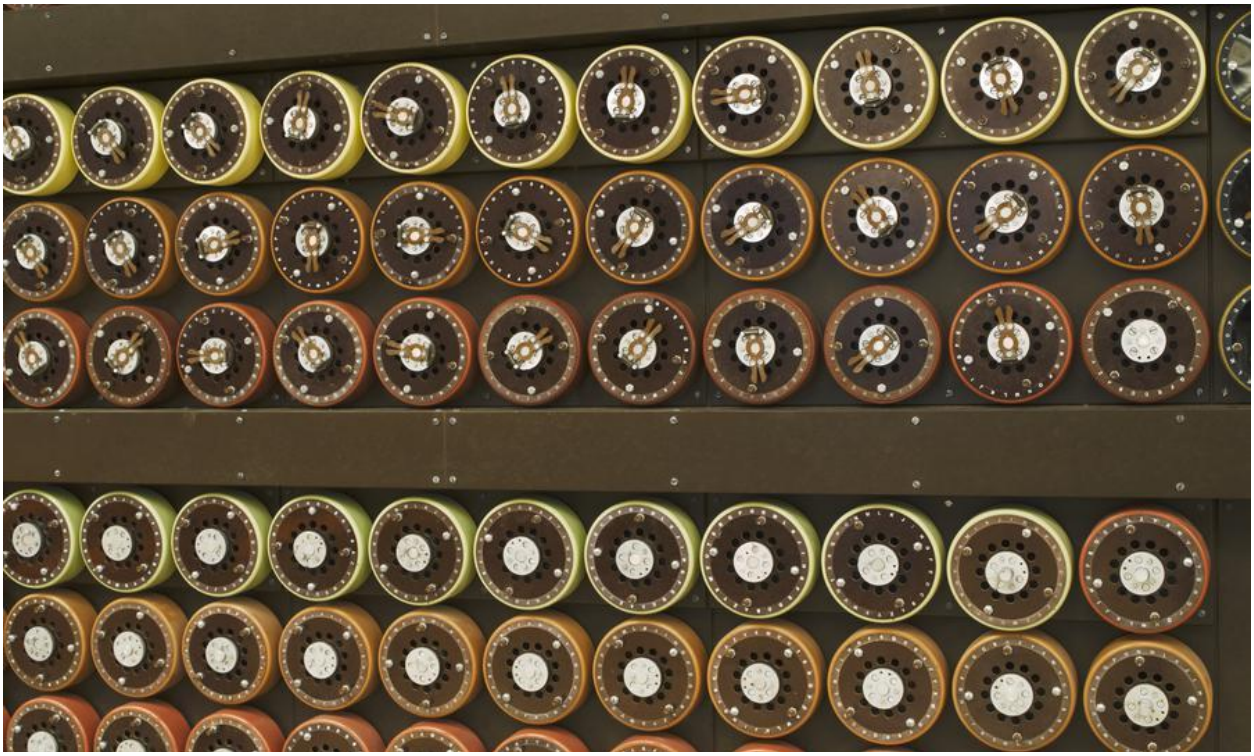
FEATURE

US 5G Strategy

US 5G strategy Signals interception |Analysis



Model Bombe code-breaking machine used at Bletchley Park during World War II to decipher messages transmitted by German forces using Enigma encoding machines. Photo: iStock

US-China tech war and the US intelligence community

China's 5G leadership means US eavesdropping will be blocked, spies unemployed

By Spengler

July 7, 2019

https://www.asiatimes.com/2019/07/article/us-china-tech-war-and-the-us-intelligence-community/

The US intelligence community's alarm at Chinese leadership in 5G mobile broadband has less to do with a threat of Chinese eavesdropping than with the likelihood that electronic eavesdropping will become next to impossible, thanks to quantum cryptography. I have had a number of conversations on the topic with US as well as Chinese sources, but this conclusion appears obvious from public sources.

America's intelligence community spends nearly $80 billion a year, including $57 billion for the National Intelligence Program and $20 billion for the Military Intelligence Program. Signals intelligence (SIGINT), mainly electronic eavesdropping, takes up the lion's share of the budget. Among other things the National Security Agency recorded more than half a billion calls and text messages of Americans in 2017. In response to a Freedom of Information Act lawsuit by the American Civil Liberties Union, the National Security Agency admitted — for the second time — that it improperly eavesdropped on Americans. The spooks' ability to tap the conversations of prospective terrorists, foreign

leaders like Germany's Angela Merkel and pretty well anyone it wants is a source of enormous power as well as justification for continued funding.

All of that is about to come to an end and the spooks will have to find something else to do. That has a great deal to do with the incipient tech war between China and the United States.

The US intelligence services argue that if China's national champion Huawei dominates the installation of 5G mobile broadband, it can build "back doors" into its hardware to steal information, and perhaps even sabotage communication and industrial control networks in case of conflict. The US has threatened its allies with a cutback on intelligence sharing if they use Huawei equipment. So far, no country but Japan has acceded to American demands. Huawei denies that it has the capacity or intention to steal data, but charges of this sort are hard to disprove.

"The issue comes down to whether we get everyone's data or China gets everyone's data," a former director of the Central Intelligence Agency told me recently. But I don't think that is the issue at all: More than one kind of technology now exists that will make eavesdropping impossible — not just difficult or expensive, but outside the realm of physical possibility.

The ultimate form of data security is quantum communications, an application of physics that China has pioneered. Two years ago Chinese scientists had a video call with colleagues in Vienna, creating the signal by entangling atoms halfway around the world. The system that makes the communication possible cannot be stolen, because any outside intervention destroys the signal itself. It is like a letter that disintegrates the instant you set eyes on it. Commercial applications of this technology may not be too far away. In 2018, Huawei conducted field trials for data security in optical networks with the Spanish telephone company Telefónica.

As Huawei wrote at the time:

The continuous growth in computational capacity has required a steady increase in key sizes and the complexity of key generation algorithms. And these techniques can become completely futile with the advent of quantum computers, able to apply the principles of quantum mechanics to resolve problems considered unsolvable so far, including breaking the keys used by current methods, thus rendering most of our security infrastructure useless… Quantum technologies themselves provide a solution to this vulnerability of current cryptographic key generation methods. Quantum principles can be applied to exchange a key between the two ends of a communications link, so that this key remains secure with respect to any attack, and any attack attempt becomes detectable.

Several other research groups are working on quantum cryptographic applications for 5G broadband, including physicists at the University of Bristol, SK Telecom and Toshiba Research. Given that the technology was proven in field tests two years ago, its adoption as a general solution to the problems of cryptography should not take long.

China's objective is not to steal the world's data (although Chinese intelligence agencies may swipe what they can opportunistically). Rather, it wants to dominate the construction and future upgrades of the world's communications infrastructure, linking it to Chinese commercialization (through e-commerce, e-finance and other means), Chinese industrial technology (through the Internet of Things), Chinese finance and Chinese logistics. The US Central Intelligence Agency's warnings about Huawei's links to the Chinese state are accurate, strictly speaking: All important telecommunications equipment makers cooperate with their national intelligence services, as America's Cisco did with the National Security Agency.

It is hard to avoid the conclusion that the US intelligence services are defending their SIGINT turf without due consideration for US strategic interests. The China hawks, e.g.

Senators Marco Rubio (R-FL) and Mitt Romney (R-UT), have demanded that Trump maintain America's ban on the shipment of electronic components and software to Huawei. But this may have baleful consequences for American interests. A glaring example is the threat to deny Huawei access to updates of Google's Android operating system, used by Huawei's mobile handsets. In response, Huawei will introduce its own mobile operating system to compete with Android. Long under development, the decision to launch an alternative to Android was accelerated by the prospect of an export ban.

China buys 400 million handsets a year, and its market is big enough to persuade developers to rewrite most of the 1.7 million native Android apps for its own operating system. At that point consumers around the world will be able to choose between Google's system and Huawei's with no loss of functionality. There are enough governments in the world, including in Europe, with a grudge against Google to give Huawei a critical advantage in important markets.

Huawei's handset business is a high volume but low margin affair, and ancillary to its main strategic objectives. The Chinese company would not have taken the trouble to compete with Google if its access to Android were not compromised. American technology companies have done their best to explain to President Trump that the Huawei ban may hurt them more than it hurts the Chinese, and these remonstrations appear to have influenced the US president's thinking.

I continue to believe that the United States cannot effectively restrict the spread of a technology under Chinese leadership without offering a superior product of its own. The fact that the United States has attempted to suppress Huawei's market leadership in the absence of any American competitor in this field is one of the oddest occurrences in the history of US foreign policy. If the US were to announce something like a Manhattan Project for 5G broadband and solicit the cooperation of its European and Asian allies, it probably would get an enthusiastic response. As matters stand, America's efforts to stop Huawei have become an embarrassment.

Editor's Note:

On Spengler

David Paul Goldman (born September 27, 1951) is an American economist, music critic, and author, best known for his series of online essays in the Asia Times under the pseudonym Spengler. Goldman sits on the board of Asia Times Holdings.