CENTER for AMERICAN DEFENSE STUDIES
America First – Not Alone

CHINA THREAT - SECURITY BACKGROUNDER – 'Data Security in a 5G World' ©

*"The China Threat extends far beyond missiles, troops, ships and aircraft, it is a global danger encompassing everything from geopolitics and economics to culture and trade, and increasingly, to technology. The Chinese Communist Party's ambition to become the world's primary superpower by 2049 cannot be achieved without technological supremacy. In that vein, China's role in penetrating and dominating the worlds 5G networks takes on heightened concern. Dr. Robert Spalding's analysis, originally published last year by the **National Bureau of Asian Research (NBR)**, and reprinted here by CADS, with permission, adds valuable insights to the new menace."* ***Paul Crespo, President.***

'Data Security in a 5G World: Why It Matters More than Ever'

by Robert Spalding, Senior Advisor, CADS
March 16, 2020

China's attempts to gain dominance in the global telecommunications network is therefore a top priority for the CCP and its ambition to become the global superpower by the 100th anniversary of the founding of the People's Republic of China in 2049. Brigadier General (ret.) Robert Spalding argues that 5G networks must be built with data security as the top priority to both protect individual privacy and uphold democratic freedoms.

BACKGROUND

Data is the key resource of the 21st century. The 2017 National Security Strategy (NSS) mentions data eighteen times and recognizes that "data, like energy, will shape U.S. economic prosperity and our future strategic position in the world." The NSS calls for the government to "do a better job of protecting data to safeguard information and the privacy of the American people." Data is core to the rapidly developing technologies from artificial intelligence (AI) to the Internet of Things (IoT).

In a 5G era, these and similar information technologies will be increasingly powerful and harder to avoid in everyday life. For example, 5G can unleash the power of smart cities, where IoT devices embedded in the city will pick up speech, facial expressions, and gestures, transforming them into virtual push buttons for things like calling a rideshare. In a 5G world, all this data will go directly to the tech companies, presenting users—and democracies—with the question of who owns the data.

Current U.S. debates on who should build 5G networks are too narrowly focused and do not address the root of the problem, particularly when it comes to U.S. geopolitical competition with China in these spaces. This commentary will examine the technology, business, and social layers of this problem and share ideas for how U.S. policymakers could do a better job of protecting data.[1]

HOW DATA HAS RESHAPED THE GLOBAL ECONOMY

To understand the rising risk of unprotected data, it is important to understand the power of data in reshaping the global economy. In 2007 the release of the iPhone was met with a dismissive chuckle from Microsoft CEO Steve Ballmer. What he, like most executives at the time, failed to see was the future reshuffling of the economic order.[2] Over the next ten years, the economy would dramatically shift, and most companies that had been at the top of market capitalization like AT&T, GE, Exxon, and Shell would be replaced by technology companies like Facebook, Apple, Amazon, Netflix, and Google (FAANGs), which harness user data for profit.

Initially, user experience on the iPhone was poor. 3G networks did not provide the bandwidth needed to enable the apps, services, and new business models, like Uber and Airbnb. U.S. telecommunications companies would soon invest billions in 4G networks, making the United States, along with Japan, the leaders in 4G deployment. Yet while the carriers provided the networks that would enable improved user experience on the two major platforms (iOS and Android), for the most part these companies were unable to capitalize on the economic growth like the FAANGs did by profiting off data.

This financial mismatch between investors in the infrastructure and beneficiaries of the new e-economy created the strategic dilemma confronting the United States today. The U.S. government is looking to industry to, once again lead in 5G deployment, but the network operators do not see the business case, having failed to profit from 4G investments, and the equipment vendors do not respond to the network operators' demand for equipment.

China, led by the Chinese Communist Party (CCP), witnessed the power of data to transform the global economy and acted accordingly. As Kai-fu Lee documents in his book *AI Superpowers*, Alpha Go's dominating performance against the best Chinese Go player convinced the CCP leadership that AI, and therefore data, was key to China's future dominance. China would lead the next wireless revolution with the strategic decision to develop and deploy the largest scale 5G networks in the world.

THE TECHNOLOGY LAYER

The United States faces several challenges to leading on 5G and protecting data. First, U.S. wireless operators are mired in 4G debt as low margins on their network infrastructure have forced them to pursue other business opportunities than investing in 5G. The network operators' inability to pay off 4G investments is slowing the deployment of 5G networks in the United States. Further slowing this process is the government's insistence on building in millimeter wave (high band), which is the only spectrum the U.S government has made widely available and requires more than thirteen times the antennas to compensate for the short distances the radio waves in this frequency travel. No other country is building its nationwide networks primarily in high band.

Second, the manufacturing base for U.S. telecommunications infrastructure has been decimated by predatory behavior from Huawei and ZTE.

Third, Huawei and other Chinese companies have been very active in the development of 5G standards and technology, particularly in security. Industry standards bodies are supposed to be driven by industry rather than national strategy. As such, free market economies take a "hands off" approach, while China actively seeks to shape standards with a more state-led approach. By making standards submissions and filing the underlying patents, Chinese companies have ensured that networks that comply with 3GPP (the industry standards-setting body for 5G) are substantially designed in China.

This is problematic because it means that CCP principles can be baked into the design. The entire reason for global standards is to ensure compatibility among national standards so that devices work in all countries. Thus, by dominating the standards-setting bodies, China has increased the likelihood that all countries will be building 5G networks shaped excessively by China.

Fourth, even with quantum encryption or other new safeguards, 5G networks will still be subject to many of the same data-targeted cyberattacks currently present. Without a security-minded redesign of the network, they will not be fundamentally different in how they protect data.[3] And at an even more basic level, the internet was built for speed, connectivity, and resilience. Security was considered later, only as an additional capability. This means that regardless of who builds the network—Samsung, Nokia, or Ericsson—the data is still at risk.

In order to prioritize the protection of U.S. citizens' data, as recommended in the NSS, the United States needs to rethink its treatment of data. This would require that the industry construct a zero-trust (which assumes nothing on the network can be trusted) 5G network with built-in data-centric security—in other words, a 5G network that protects citizen data. This is not currently the path telecommunications operators are on.

Thus, what is needed is industry disruption—similar to how the introduction of the iPhone precipitated the rise of the FAANGs. Given that the U.S. government controls spectrum, it can use this lever to incentivize disruption by allowing spectrum use by those businesses willing to build according to government-approved security standards.

THE BUSINESS LAYER

The idea for a data-centric secure nationwide 5G network for the United States challenges the current business models based on open data. The FAANGs built their businesses using the open-data model to harness big data analytics, financial technology, e-commerce, and AI and machine learning. China has simultaneously been building its technologies via research partnerships between its tech companies and the FAANGs. The BAT companies (Baidu, Alibaba, and Tencent)—China's version of the FAANGs—are now poised to dominate the global 5G economy and the IoT.

Instead of the smartphone world dominated by the FAANGs in 4G, the BATs, if successful, will dominate the smart city. To that end, China is building out smart cities in China, with 50 such cities recently going live. Kai-fu Lee has stated as such: "If data were petroleum in the artificial intelligence era, then China would be Saudi Arabia."[4]

Those who can accumulate, and stockpile data, have the ability to feed AI and machine learning platforms to build more powerful, industry-leading companies. Large tech companies like Google and Facebook are now competing with Baidu and Tencent in the free world, but not at all in China, where they are blocked by the Great Firewall. Given the lax data regulations within China, the FAANGs will never be able to compete on an equal basis with the BATs because the datasets available across their respective enterprises favor Chinese tech companies, which can compete in all global markets. The diversity and depth of data mean that Chinese companies have a competitive advantage going forward.

Economically, this unbalanced competition is extremely important for Chinese companies. If the BATs can supplant the FAANGs, then this unlocks trillions of dollars in potential revenue for Chinese companies, and by default the CCP. Tik-Tok and WeChat have shown that Chinese apps can find widespread adoption outside China. The CCP's state-led business model gives China an advantage over capitalist countries. Because of the enormous value of data, the CCP can subsidize Huawei and the ZTE to the point where the network cost is absorbed by the revenue generated by the BATs. U.S. carriers cannot compete with this model. As a result, the United States faces the prospect of a future where it has lost not only most of its industrial capacity but also its leadership in technological innovation.

THE SOCIAL LAYER

In an internet-connected world, dominance in the technology and business layers translates into the social one. Samantha Hoffman, an analyst at the Australian Strategic Policy Institute, explains not only how data is used to fuel the building of Chinese big data and companies, but also how that same data flows to the propaganda arm of the CCP and the intelligence arm of the People's Liberation Army.[5] For example, Tencent's WeChat has more than one billion customers. The lives of people inside and outside the mainland revolve around the app, which is used for everything from dating and general communication to food delivery and travel arrangements. This data not only fuels WeChat's dominance, but it gives the CCP unfettered access to the lives of all customers.

As explained above, 5G and the IoT amplify the ability of Chinese tech companies, and by default the CCP, to gain more insight into people's behavior and potentially influence it without their consent. As 5G networks are built, the source of data that flows to the tech companies and the CCP will be the devices (such as cameras and microphones) that have been placed there by companies like Baidu.

Hoffman's research shows the full capability of an authoritarian big data and AI company to influence the citizens. Currently, the data collected about the behavior of Chinese citizens is used to develop a social credit score to decide on creditworthiness, job opportunities, or academic applications. The result from this score becomes more weighted in a 5G world. There is also the capability for these tools to influence purchasing patterns to favor certain brands over others. Importantly, they could be used to subtly influence populations toward embracing political parties or political systems.[6] As China extends its influence and digital infrastructure beyond its borders through its Belt and Road Initiative and Digital Silk Road, the CCP will seek to export its vision of digital authoritarianism by providing the ability to monitor citizens in connected countries.

CONCLUSION

Deploying a secure 5G network capability nationwide is paramount to both protect the American people and ensure that U.S. allies and partners do not succumb to CCP influence. The federal government has the levers to make this happen by using fiscal and spectrum policy to shape the United States' digital future.

To do so, it should take the following steps:

1. Enable dynamic sharing of spectrum without requiring upfront spectrum purchase. The government can instead take a portion of the revenue as compensation for use. This would enable faster deployment of secure 5G and open up the data space for more competition.
2. Provide loans and grants for deployment of rural 5G. Telecommunications infrastructure is currently not considered a good investment because increased capacity provides diminishing financial returns.
3. Require the sharing of physical resources like towers for industry newcomers. This would enable faster buildout and eliminate costly repetition of expensive infrastructure deployment.

4. Establish standards for zero-trust networks like post-quantum encryption, identity management, access control, and secure supply chains. Requiring zero-trust networks would give consumers and businesses the opportunity to choose where to place their trust.
5. Contribute a portion of defense funding to continuous research and development in hardware, software, and other vital information-related technologies. Telecommunications, networking, and computing are vital to the future of the digital economy. Since business usually focuses on market-based R&D, we need more government-sponsored basic science research that supports a healthy ecosystem.
6. Work with allies and partners to use developmental finance and funding related to national security to help other democracies build similar networks and programs around the globe. Free societies need to work together to promote data security and digital democracy, or they risk eroding their own democratic systems.

Implemented together, these tools could promote innovation in the IT industry and help establish the United States as a true 21st-century power. By fostering the domestic conditions for widespread secure 5G and promoting its deployment abroad, democratic systems can ensure their continued survival in the digital age.

BIOGRAPHY

Brigadier General (ret.) Robert Spalding is a Senior Fellow at the Hudson Institute, and a Senior Advisor at the Center for American defense Studies (CADS). He previously served as the senior director for strategic planning at the National Security Council. A former China strategist for the chairman of the Joint Chiefs of Staff and the Joint Staff at the Pentagon, Spalding also served as the senior defense official and defense attaché at the U.S. Embassy in Beijing. He is the author of the book Stealth War: How China Took Over While America's Elite Slept. The views expressed are those of the author.

ENDNOTES

[1] White House, *National Security Strategy of the United States of America* (Washington, D.C., December 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[2] Ben Sin, "These Are the People Who Thought the iPhone Would Fail," *Forbes*, January 7, 2017, https://www.forbes.com/sites/bensin/2017/01/09/these-are-the-people-who-thought-the-iphone-would-fail/#7ba8e59c544e.

[3] Defense Science Board Task Force, "Defense Applications of 5G Network Technology," 2019, https://dsb.cto.mil/reports/2010s/5G_Executive_Summary_2019.pdf.

[4] Gao Ge, "China Is to Data What Saudi Arabia Is to Oil, Kaifu Lee Tells AI Forum," Yicai Global, September 17, 2018, https://www.yicaiglobal.com/news/china-is-to-data-what-saudi-arabia-is-to-oil-kaifu-lee-tells-ai-forum.

[5] Samantha Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion," Australian Strategic Policy Institute, October 14, 2019, https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

[6] Julia Carrie Wong, "'It Might Work Too Well': The Dark Art of Political Advertising Online," *Guardian*, March 19, 2018, https://www.theguardian.com/technology/2018/mar/19/facebook-political-ads-social-media-history-online-democracy.

END OF CADS REPORT. NO MORE PAGES

This analysis originally appeared in the National Bureau of Asian Research (NBR) on March 16, 2020. It is reprinted here by the Center for American Defense Studies (CADS), with permission of the author.

www.americandefensestudies.org