The Heritage Foundation

ISSUE BRIEF

No. 4952 | APRIL 16, 2019

The U.S. Must Treat China as a National Security Threat to 5G Networks

Klon Kitchen

As an adversarial power, China cannot be allowed to use its government-controlled companies to gain a significant foothold in the United States' burgeoning fifth-generation (5G) wireless networks. Such a presence would be a clear national security threat that could decisively compromise American telecommunications and data infrastructure—including the communications integrity of the U.S. military and intelligence community. It would be equally damaging, however, to allow concerns about China to result in the nationalization of U.S. 5G networks.

The U.S. must not be complacent. Beijing's "civil-military fusion" practices must not be allowed to threaten U.S. national security. Further, the United States must meaningfully penalize Beijing's blatant attempts to threaten America's critical infrastructure and to use its technology industry as an extension of state espionage.

No, the U.S. Cannot Trust China on 5G Networks

China's intentions are clear: Beijing will, if not prevented, use the deployment of equipment, software, and services from Chinese state-controlled companies to compromise U.S. telecommunications networks—networks that carry significant volumes of military and intelligence data. Furthermore, the Chinese government will use its influence over the international standards for these technologies as a primary tactic in this plan.

To that end, the Chinese government is implementing a concerted strategy of civil-military fusion through the sale and deployment of 5G telecom systems that enables Chinese companies with state support to siphon, store, and exploit data transmitted on these systems, and leverages these same companies as extensions of the government's intelligence and national security apparatus.

This threat demands a response. The United States must not allow Chinese state-controlled companies to gain any significant position within America's emerging 5G networks. China has:

- Expedited the two-decades-old effort to meld its private and defense communities, with Chinese president Xi Jingping explaining in early 2018 that "[i]mplementing the strategy of military-civilian integration is a prerequisite for building integrated national strategies and strategic capabilities and for realizing the Party's goal of building a strong military in the new era."[1]

- Used Chinese telecommunications companies, such as Huawei, as the prototype of this civil-military fusion, where the company is not only heavily subsidized by the Chinese government, but it is also broadly accused of espionage by national security leaders in the United States, Australia, Japan, and New Zealand.[2] The United Kingdom and Germany also express grave doubts about the company's trustworthiness.[3]

This paper, in its entirety, can be found at **http://report.heritage.org/ib4952**

The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002
(202) 546-4400 | heritage.org

- Employed aggressive national security laws. All Chinese companies are legally required to "support, assist, and cooperate with national intelligence efforts,"[4] and government intelligence agencies are legally allowed to forcibly gain access to any server or data stored within the nation's borders.[5] This means that, regardless of a company's active complicity in spying, the only safe assumption is that any information collected by Chinese companies and held on Chinese servers will be exploited by the Chinese government.

No, the U.S. Should Not Nationalize 5G Networks

As the challenge of Chinese influence grows, some are concerned about efforts to nationalize part of the U.S. 5G networks in order to prevent the compromise of U.S. systems. That is a legitimate concern. Overly intrusive government solutions, however, are unnecessary and would undermine U.S. innovation and competitiveness.

The majority of concerns over nationalization appear to stem from a leaked draft proposal by a then-director on the National Security Council staff that included a policy option of having the U.S. government build a single, "secure" 5G network, and then lease access to this network to private service providers.[6] This policy was never formally proposed by the Administration, and multiple Administration officials have since publicly rejected the proposal.

That does not mean that concerns about nationalization are unfounded. Harvard professor Susan Crawford, for example, argues for a nationalized 5G network based on her assessment that, unlike China's government-driven efforts, the United States is critically behind in the deployment of fiber-optic cable—a prerequisite for 5G—and that this shortfall means "China, and not the US, will be the sandbox for new applications that require very-high-capacity network connections."[7]

While Professor Crawford and others who point out that China's broadband availability exceeds that of the United States are correct, this is an incomplete analysis, and the prescription for a government-run solution is an overcorrection that ignores the advantages of free-market innovations as well as the federal government's long track record of failed market ventures. In addition, while it is true that nearly 80 percent of Chinese broadband users have access to fiber-optic Internet, in contrast to the roughly 25 percent of American users,[8] this does not necessarily equate to a categorical advantage in innovation.

Further, there is reason to be skeptical of any model that depends on government for cutting-edge commercial innovation. In the U.S., as demonstrated by Amtrak, the United States Postal Service, and other government-supported entities, federally driven commercial offerings are frequently plagued by financial failure, service shortfalls, and a lack of innovation. There is no reason to believe that a nationalized 5G network would escape these challenges.

1. Zhou Xin, "Xi Calls for Deepened Military-Civil Integration," March 12, 2013, http://www.xinhuanet.com/english/2018-03/12/c_137034168_2.htm, (accessed April 8, 2018).
2. News release, "Chinese Telecommunications Device Manufacturer and Its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction of Justice," U.S. Department of Justice, January 28, 2019, https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade (accessed April 7, 2019).
3. Huawei Cyber Security Evaluation Centre (HSEC) Oversight Board, *Annual Report*, March 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf (accessed April 7, 2019), and Sean Keane, "US Reportedly No Longer Demands Huawei Ban from Germany," Cnet, April 9, 2019, https://www.cnet.com/news/us-reportedly-no-longer-demands-huawei-ban-from-germany/#ftag=CAD590a51e (accessed April 15, 2019).
4. China Law Translate, "National Intelligence Law of the P.R.C.," June 27, 2017, https://www.chinalawtranslate.com/en/%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/ (accessed April 7, 2019).
5. Catalin Cimpanu, "China's Cybersecurity Law Update Lets State Agencies 'Pen-Test' Local Companies," ZDNet, February 9, 2019, https://www.zdnet.com/article/chinas-cybersecurity-law-update-lets-state-agencies-pen-test-local-companies/ (accessed April 7, 2019).
6. Jonathan Swan et al., "Scoop: Trump Team Considers Nationalizing 5G Network," Axios, January 28, 2018, https://www.axios.com/trump-team-debates-nationalizing-5g-network-f1e92a49-60f2-4e3e-acd4-f3eb03d910ff.html (accessed April 1, 2019).
7. Susan Crawford, "Why America Needs a Nationalized 5G Network," *Wired*, February 8, 2018, https://www.wired.com/story/america-needs-more-fiber/ (accessed April 1, 2019).
8. C. Custer, "China to Top World in Fiber-Optic Broadband Penetration by 2017," Tech in Asia, May 17, 2016, https://www.techinasia.com/china-top-world-fiberoptic-broadband-penetration-2017 (accessed April 16, 2019).

That is not to say that the U.S. should not be concerned about its competitive posture on 5G development. In fact, a recent report by the Defense Innovation Board lists a number of difficulties facing the U.S.'s 5G rollout and concludes: "The country that owns 5G will own many of these innovations and set the standards for the rest of the world.... [T]hat country is currently not likely to be the United States."[9] The report draws conclusions based on what it cites as China's rapid growth as a global leader in 5G coupled with the U.S.'s relative slowness in allocating the necessary spectrum, its diminished ability to produce certain telecommunications equipment, and the lack of a coherent national 5G strategy.

No, the U.S. Can't Ignore the 5G Challenge

Industry is best suited to deliver and deploy the nation's 5G infrastructure. That does not absolve the federal government of its constitutional responsibility to provide for the common defense, protecting the people and the interests of the United States. The nation must forge a path so that these goals can be accomplished in a complementary fashion. There are some actions that the U.S. government can undertake now to start moving in the right direction and send Beijing a strong message. Specifically, the Administration should:

- **Share threat information with industry.** U.S. government concerns about Chinese technologies and related services cannot be expressed exclusively in classified or other constrained environments. If the U.S. government wants industry to operate in ways that do not provoke national security concerns or make them worse, the government must share its telecommunications security concerns in a detailed and broadly sharable manner.

- **Determine disqualifying factors.** The U.S. government should clearly communicate with industry and with America's foreign partners and allies, as well as the Chinese, which legal frameworks, activities, and business practices will result in exclusion from U.S. 5G infrastructure, services, and other emerging-technology integrations. Further, the U.S. should encourage other nations to adopt these standards as a way of maintaining pressure on countries and companies working against U.S. and allied interests.

- **Block vulnerabilities.** The U.S. should block any foreign technology from U.S. markets that creates vulnerabilities in critical infrastructure or that provides hostile foreign actors with "backdoors" to U.S. data. Doing this will impose significant pressure on China and others to improve poor security practices and it will spur domestic security research in the U.S. that will incrementally improve the safety of the hardware and software supply chains into the United States. The U.S. should encourage the remaining four Five Eyes countries—Australia, Canada, New Zealand, and the United Kingdom—to implement similar exclusionary measures.

- **Block untrusted companies.** The Committee on Foreign Investment in the United States should block foreign companies from U.S. investments if they have a history of producing hardware or software with known vulnerabilities. This would be especially helpful in mitigating the challenge of Chinese investment in, and purchase of, American start-ups that might embrace poor security practices in return for rapid access to capital.

- **Prepare for "zero-trust" networks.** Currently, Huawei controls approximately 30 percent of the global mobile communications market and could win as much as 50 percent of the global 5G market. Even if the U.S. is able to secure its own wireless networks from foreign spying and interference, the vast majority of networks around the world will be developed and managed by the Chinese. This requires the U.S. defense and intelligence communities to begin mitigating this threat and developing new networking strategies that will allow the U.S. to operate and thrive in a "zero-trust" environment—meaning operating on networks that are owned and managed by China or other hostile actors. While it is too soon to cede 5G to U.S. challengers, it is prudent to begin preparing for worst-case scenarios.

9. Milo Medin and Gilman Louie, "The 5G Ecosystem: Risks & Opportunities for DoD," Defense Innovation Board, April 3, 2019, https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF (accessed April 7, 2019).

In many times during its history, the U.S. has mastered the challenge of dealing with threats from adversaries while preserving America's capacity to thrive and innovate. America is up to this challenge as well, but it must act.

*—**Klon Kitchen** is Senior Research Fellow in the Douglas and Sarah Allison Center for Foreign Policy, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.*