Free markets. Real solutions.

R STREET POLICY STUDY NO. 204
September 2020

HUAWEI AND NATIONAL SECURITY: LESSONS FOR 6G

By Kathryn Waldron

CONTENTS

INTRODUCTION

Fifth-generation (5G) wireless technology promises faster transmission of data, which, in addition to improving normal communication, opens the door to emerging technologies such as robot-assisted surgery or self-driving vehicles where real-time transmission of data is paramount. While the benefits of 5G have yet to be fully understood or realized, its potential should not be understated. However, this potential makes it all the more critical that these 5G networks are built with adequate security protections in mind. And several unresolved 5G security gaps exist—one of which is the residual risk associated with network equipment manufactured by companies based in the People's Republic of China (PRC)—most notably, Huawei.

U.S. government officials argue that the only way to protect the integrity of 5G networks is to prevent Huawei products and services from being incorporated into the network infrastructure—often called a "full-ban" approach. The Trump administration and various U.S. government agencies have thus engaged in a series of policies aimed at restricting Huawei's ability to do business both in the United States and abroad and have encouraged other countries to do the same.

However, many countries have proved reluctant to adopt a full-ban when it comes to their own 5G networks. This is not surprising given the full-ban approach is potentially very costly from both an economic and political standpoint. Huawei's products are often cheaper than those of competitors Ericsson or Nokia. Furthermore, following the United States' lead and snubbing Huawei in the name of national security risks antagonizing the Chinese government, who have previously promoted the company as a national champion. Indeed, Huawei deputy chairman Eric Xu previously warned: "The Chinese government will not just stand by and watch Huawei be slaughtered on the chopping board."[1]

Alternatives to the full-ban approach range from a "partial-ban"—wherein risky vendors like Huawei are restricted to certain parts of the network—to a full-out embrace of the Chinese company. The goal of this paper is to determine whether using Huawei equipment and services is, in fact, a legitimate national security concern, and then to compare the various approaches to determine which solution (if any) is best suited to mitigating this concern. The first part of this paper evaluates the risk posed by Huawei. Next, it compares the various risk mitigation strategies embraced by governments across the globe—with particular focus on the responses from the United States, the United Kingdom and Germany. Finally, it points out four lessons policymakers should keep in mind when planning for sixth-generation (6G) technologies.

1. Zak Doffman, "China Just Crossed A Dangerous Line For Huawei: New 'Retaliatory Responses' Threatened," *Forbes*, May 26, 2020. https://www.forbes.com/sites/zakdoffman/2020/05/26/china-just-crossed-a-dangerous-new-line-for-huawei-threatens-retaliatory-responses/#3a8faa4fff72.

CHINA, HUAWEI AND CHALLENGES TO 5G SECURITY

The challenge in rolling out this necessary infrastructure is caused by the fact that the Chinese company Huawei is currently one of the largest companies worldwide (along with Ericsson and Nokia) that manufactures the necessary infrastructure. And, significant debate exists about whether Huawei can provide secure 5G infrastructure abroad due to its location in China, the degree to which the company is under the control of the Chinese Communist Party and whether or not its equipment contains intentional backdoors that the Chinese government could exploit. Some of these concerns stem from the fact that Huawei's founder, Ren Zhengfei, has ties to the Chinese equivalent of the National Security Agency (NSA).[2] But the main national security concerns are rooted in the nature of Chinese law and the downstream effect on the degree to which the corporation can operate separately from the government.

Enacted in June 2017, China's National Intelligence Law grants authority to "national intelligence work institutions" to search premises and seize property when conducting defensive espionage, and compels organizations and individuals to cooperate with government intelligence institutions if asked.[3] Although Huawei has claimed that the Chinese government does not legally have the authority to compel it to build backdoors into its telecommunication system and that its "subsidiaries and employees outside of China are not subject to the territorial jurisdiction of the National Intelligence Law," many legal experts have disputed this interpretation. [4] One Chinese lawyer argued: "[Huawei] cannot refuse [because] the law stipulates that companies have an obligation to cooperate for national security and investigation needs. National security laws, the anti-terrorism law and other laws all require companies to assist the judiciary."[5]

This seems a viable concern as indeed, even in the United States, the Communications Assistance for Law Enforcement Act (CALEA) requires that telecommunications carriers and manufacturers "design their equipment, facilities, and services to ensure that they have the necessary surveillance capabilities to comply with legal requests for information."[6] It is therefore reasonable to assume that an even more restrictive government like China's would have similar—if not far more broad—access to the data handled by its private companies. And, perhaps not surprisingly, U.S. government officials claim to have evidence that Huawei "has the capability secretly to access sensitive and personal information in systems it maintains and sells around the world."[7]

Another concern stems from the opacity of the company's ownership structure. Huawei claims to be entirely employee owned, with no outside organizations (including the Chinese government) as shareholders.[8] However, a 2019 study accuses the company of deliberately misleading the public about its corporate structure, arguing that "regardless of who, in a practical sense, owns and controls Huawei, it is clear that the employees do not."[9] This, the authors explain, is because shares not held by the founder are held by a trade union committee affiliated with the Shenzhen Huawei Investment Holding Co., which merely represents Chinese employees who own shares, and:

> Given the public nature of trade unions in China, if the ownership stake of the trade union committee is genuine, and if the trade union and its committee function as trade unions generally function in China, then Huawei [is] effectively state-owned.[10]

If this is true—or even if the possibility exists—this is of grave concern because of all hostile, foreign adversaries, China's threat to the United States is unique in that it uses numerous, aggressive and sophisticated cyber tools intended to: steal intellectual property and other useful data; to compromise critical infrastructure; and to facilitate the manipulation of the political behavior of Americans. Moreover, in addition to these goals, it also seeks to achieve "comprehensive national power" that relies on an "innovation-driven growth model" and "military modernization."[11] This means that their efforts are far more comprehensive, multi-faceted and have far loftier long-term goals in mind.

2. Tom Gara, "On Questions Of National Security, Is Huawei Innocent Until Proven Guilty?", *The Wall Street Journal*, Oct. 8, 2012. https://blogs.wsj.com/corporate-intelligence/2012/10/08/on-questions-of-national-security-is-huawei-innocent-until-proven-guilty.

3. Staff, "What you need to know about China's intelligence law that takes effect today," *Quartz*, June 28, 2017. https://qz.com/1016531/what-you-need-to-knowabout-chinas-intelligence-law-that-takes-effect-today.

4. Yuan Yang, "Is Huawei compelled by Chinese law to help with espionage?", *Financial Times*, March 5, 2019. https://www.ft.com/content/282f8ca0-3be6-11e9-b72b-2c7f526ca5d0.

5. Ibid.

6. "Communications Assistance for Law Enforcement Act," U.S. Federal Communication Commission, March 24, 2020. https://www.fcc.gov/public-safety-and-homeland-security/policy-and-licensing-division/general/communications-assistance.

7. Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," *The Wall Street Journal*, Feb. 12, 2020. https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.

8. Claude Barfield, "Telecoms and the Huawei Conundrum: Chinese Foreign Direct Investment in the United States," *AEI Economic Studies*, November 2011, p. 5. https://www.aei.org/wp-content/uploads/2011/11/-telecoms-and-the-huawei-conundrum-chinese-foreign-direct-investment-in-the-united-states_103528582558.pdf.

9. Christopher Balding and Donald C. Clarke, "Who Owns Huawei?", April 17, 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3372669.

10. Ibid.

11. Daniel R. Coats, "Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community," Senate Select Committee on Intelligence, Jan. 29, 2019, p. 14. https://www.odni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf. (Hereinafter: *Worldwide Threat Assessment*).

In fact, according to the most recent *Worldwide Threat Assessment*: "China remains the most active strategic competitor responsible for cyber espionage against the US Government, corporations, and allies," and it notes more ominously that China's capabilities include not only the ability to alter online information in ways that shape the views of its own citizens, but "potentially the views of US citizens," as well.[12] The Federal Bureau of Investigation's (FBI) more recent March 2020 assessment agrees: "While several nation-states pose a cyber threat to U.S. interests, no other country presents a broader and more comprehensive threat to our ideas, innovation, and economic security than [China...] under the leadership of the Chinese Communist Party," adding that, "[w]hile cyber network operations remain a primary and possibly increasing collection tool, the CCP also relies on techniques such as intellectual property theft, purchases of U.S. corporations, and physical and property theft to acquire U.S. data."[13]

China uses cyber espionage to target key technology sectors in the United States when it cannot achieve its own national goals by other means.[14] In terms of the potential risk to critical U.S. infrastructure, the United States Intelligence Community (USIC) warns that China has the ability to launch cyber attacks that can cause a variety of effects and of varying duration, such as disruptions to natural gas pipelines.[15] China, Russia and other countries also pose a threat to other fundamental societal activities, like the upcoming United States presidential election.[16] And, while this type of malign, foreign influence operation or others, such as online disinformation campaigns or the use of deep fakes, are not the focus of this paper, all such operations require the collection of large datasets pertaining to the activities of Americans—much of which will be transmitted on 5G networks. After all, big data drives improvements in artificial intelligence and machine learning, and those technologies will be key assets in China's campaign to understand, predict and manipulate the political and other behavior of Americans.

For the purposes of the present study, perhaps the most concerning risks have to do with the ways in which China can use cyber technology created by Chinese companies "as routine and systemic espionage platforms against the United States and allies."[17] This is of growing concern, as the PRC has gained increasingly broad access to data located outside China through both lawful and unlawful means. As the FBI explains, even the otherwise lawful activities of Chinese companies acting abroad can carry substantial risk:

> Chinese companies are increasingly acquiring or launching social media applications not housed in mainland China for the global consumer market. These applications generate big data and collect PII, such as biometric information, contact lists, location data, log data, communication metadata, content (text and photographic), bank and credit card details, and financial transactions of U.S. persons.[18]

Here, even seemingly innocuous efforts to create and promote applications for broad download and use are actually attempts to mine large swaths of data from unsuspecting users. Moreover, China attempts to conceal its collection of such data and thus the FBI warns that "consumers should be aware of the privacy implications of any application they install, especially applications from foreign countries with weak data protection laws."[19]

In addition to such lawful data mining, the United States has accused the PRC of stealing personally identifiable information about many Americans through unlawful computer intrusions. For example, in February 2020, a federal grand jury indicted four individuals associated with the PRC's People's Liberation Army (PLA), alleging that they were responsible for the massive 2017 Equifax data breach that affected approximately 145 million people.[20]

Such problems are merely exacerbated by the competitive nature of the relationship between the United States and China in the realms of science and technology innovation. As the countries compete, we will see an increase in "efforts to acquire top talent, companies, data, and intellectual property via licit and illicit means" because China "view[s] strong indigenous science and technology capabilities as key to their country's sovereignty, economic outlook, and national power" and thus they will go to great lengths to ensure such capability.[21] Much of this competition centers around the global race to develop artificial intelligence as a key strategic technology.[22]

In short, China is a well-resourced, highly motivated and highly capable adversary that does not hesitate to use cyber

12. Ibid., p. 5.

13. Testimony of Clyde E. Wallace, Senate Judiciary Committee, "Dangerous Partners: Big Tech and Beijing," 116th Congress, March 4, 2020. https://www.fbi.gov/news/testimony/dangerous-partners-big-tech-and-beijing. (Hereinafter: Wallace testimony).

14. Ibid.

15. Ibid.

16. *Worldwide Threat Assessment*, p. 7. https://www.odni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

17. Ibid.

18. Wallace testimony. https://www.fbi.gov/news/testimony/dangerous-partners-big-tech-and-beijing.

19. Ibid.

20. "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax," U.S. Dept. of Justice, Feb. 10, 2020. https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.

21. *Worldwide Threat Assessment*, p. 15. https://www.odni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf.

22. Ibid., pp. 15-16.

means to achieve its national objectives. And this potentially includes embedding telecommunications equipment in global data networks that it can control and manipulate. Indeed, the USIC predicts that, with the adoption of 5G technologies, "US data will increasingly flow across foreign-produced equipment and foreign-controlled networks, raising the risk of foreign access and denial of service" or, in other words, increasing threats to the confidentiality, integrity and availability of data.[23]

U.S. POLICY RESPONSE

For these myriad reasons, U.S. intelligence officials and policymakers have been raising concerns about incorporating Huawei technology into American telecommunications systems for over a decade. For example, in 2008, scrutiny from the Committee on Foreign Investment in the United States (CFIUS) regarding possible software vulnerabilities halted Huawei's attempted acquisition of 3Com, a defense contractor and producer of anti-hacking software.[24] A similar situation occurred when Huawei attempted to purchase assets from American server producer 3Leaf.[25]

In 2018, the top-six U.S. intelligence chiefs, which includes the heads of the FBI, Central Intelligence Agency (CIA) and NSA, testified to the United States Senate Select Committee on Intelligence that they would not recommend private citizens use Huawei phones.[26] In particular, FBI Director, Christopher Wray explained that intelligence officials were "deeply concerned about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks."[27] Congress subsequently included a clause in the 2019 National Defense Authorization Act that banned the federal government and its contractors from using Huawei technology without a waiver. Huawei filed a lawsuit contesting the constitutionality of this ban, but the government's action was upheld.[28]

On May 25, 2019, the Trump administration issued an executive order that declared a national emergency in response to the threat of foreign adversaries acting against American information and communications networks. Specifically, the order prohibited:

> any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States, where the transaction involves any property in which any foreign country or a national thereof has any interest.[29]

And, although Huawei was not mentioned by name, the order effectively served as a ban against the company. In fact, several large telecom providers and consumer electronics stores had already stopped selling Huawei phones or other products. However, the order served to further isolate Huawei from American companies as in compliance with Trump's executive order, Google officially announced that Huawei phones not certified by Google prior to May 15 would not be able to use G Suite apps. Other American companies, such as Microsoft and Intel, also fell in line with the administration's direction with restricting Huawei's access to their products.[30] After the executive order, the United States Department of Commerce added Huawei to the "Entity List," which includes companies engaged in "activities contrary to US national security and/or foreign policy interests."[31] This action restricted exports from the United States to the company. However, loopholes in the foreign-produced direct-product rule still allowed Huawei to buy semiconductors and chipsets from foreign producers using American software and technology in their manufacturing. In a subsequent attempt to curtail this supply chain, the Department of Commerce's Bureau of Industry and Security recently amended the foreign-produced direct-product rule to subject semiconductors and chipsets to Export Administration Regulations, which will prohibit companies from selling them to Huawei or any of its affiliates without a license.[32] And this August, the Department of Commerce added another 38 Huawei affiliates to the Entity List, which "further restricts Huawei from obtaining foreign made chips

23. Ibid., p. 16.

24. Steven R. Weisman, "Sale of 3Com to Huawei is derailed by U.S. security concerns," *The New York Times*, Feb. 21, 2008. https://www.nytimes.com/2008/02/21/business/worldbusiness/21iht-3com.1.10258216.html.

25. Sinead Carew and Jessica Wohl, "Huawei backs away from 3Leaf acquisition," *Reuters*, Feb. 19, 2011. https://www.reuters.com/article/us-huawei-3leaf/huaweibacks-away-from-3leaf-acquisition-idUSTRE71I38920110219.

26. Sara Salinas, "Six top US intelligence chiefs caution against buying Huawei phones," *CNBC*, Feb. 13, 2018. https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html.

27. Ibid.

28. Sherisse Pham, "US judge rejects Huawei lawsuit challenging a ban on its products," *CNN Business*, Feb. 19, 2020. https://www.cnn.com/2020/02/19/tech/huawei-us-lawsuit-rejected/index.html.

29. President Donald J. Trump, "Executive Order on Securing the Information and Communications Technology and Services Supply Chain," The White House, May 15, 2019. https://www.whitehouse.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain.

30. C. Scott Brown, "The Huawei ban explained: A complete timeline and everything you need to know," *Android Authority*, August 25, 2020. https://www.androidauthority.com/huawei-google-android-ban-988382/.

31. "Commerce Adds Huawei Technologies Co. Ltd. to the Entity List," *Bloomberg*, May 15, 2019. https://www.bloomberg.com/press-releases/2019-05-15/commerce-adds-huawei-technologies-co-ltd-to-the-entity-list.

32. Office of Public Affairs, "Commerce Addresses Huawei's Efforts to Undermine Entity List, Restricts Products Designed and Produced with U.S. Technologies," U.S. Dept. of Commerce, May 15, 2020. https://www.commerce.gov/news/press-releases/2020/05/commerce-addresses-huaweis-efforts-undermine-entity-list-restricts.

developed or produced from U.S. software or technology to the same degree as comparable U.S. chips."[33]

The escalation of hostility has come from outside of the Department of Commerce as well. In February, the United States Department of Justice (DOJ) charged Huawei with federal racketeering and conspiracy to steal trade secrets from American companies.[34] Although the aggrieved companies were not named in the DOJ's press release, they are believed to include Cisco Systems, T-Mobile and Motorola Inc., all of which have filed suits accusing Huawei of intellectual property theft.[35] In June, the Federal Communications Commission designated Huawei and fellow Chinese company ZTE as national security threats, prohibiting money from the Federal Communications Commission's (FCC) Universal Service Fund being used on these companies' products or services.[36] And in July, the Federal Acquisition Regulation Council published an interim rule prohibiting all federal government contractors from selling Huawei hardware to the federal government and from using Huawei hardware.[37]

U. K. POLICY RESPONSE

Contrary to the United States' hawkish, full-exclusionary approach, other experts have argued that there is still a useful distinction between the core and the edge in 5G technology and thus a full ban on Huawei may not be necessary.[38] With this justification, the United Kingdom, for example, has (until recently) adopted a "partial-ban" approach, in which it continues to allow Huawei to be part of its 5G infrastructure, but only in its edge components.[39] Moreover, in order to mitigate any risk that Huawei's presence causes, it created the Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, which conducts periodic audits and technical examinations of Huawei equipment.

However, the success of such attempts to regulate and oversee Huawei's activities is, so far, questionable. For starters, the HCSEC is located in a facility that was created by Huawei in conjunction with the U.K. government to provide security evaluations of Huawei products. So, while the facility belongs to the U.K. arm of Huawei Technologies, that entity is ultimately owned by the Chinese parent company. Moreover, the Oversight Board, which reports on the HCSEC's work, contains representatives from both the HCSEC and Huawei, as well as U.K. government officials and senior representatives from the U.K.'s technology sector.[40] In light of this structure, at least to some degree, Huawei is overseeing itself, which is arguably a conflict of interests.

To date, there have been five independent audits to assess whether or not the HCSEC is able to conduct their work independently of their parent company, and the latest, conducted by Ernst & Young LLP, found no major concerns. They did, however, identify one, low-risk issue related to the "delivery of information and equipment within agreed Service Level Agreements," which basically means that information requested from Huawei was not always provided within the agreed upon time frame; a problem also identified in previous audits.[41] Nevertheless, the audit concluded that the Oversight Board was "satisfied that HCSEC is operating in line with the 2010 arrangements between HMG [Her Majesty's Government] and the company."[42] However, as a practical matter, this carries little weight, as it effectively means only that the Board is functioning as intended, not that Huawei equipment is free from risk.

In fact, the HCSEC has identified many security flaws in Huawei products. In 2018, for example, it notified U.K. telecom operators of at least several hundred security vulnerabilities.[43] According to the 2019 HCSEC report, Huawei had made little progress on remediating the vulnerabilities identified the previous year.[44] And, with regard to the implications for the U.K. National Security Risk, the report concluded:

33. Office of Public Affairs, "Commerce Department Further Restricts Huawei Access to U.S. Technology and Adds Another 38 Affiliates to the Entity List," U.S. Depart. of Commerce, August 17, 2020. https://www.commerce.gov/news/press-releases/2020/08/commerce-department-further-restricts-huawei-access-us-technology-and.

34. Office of Public Affairs, "Chinese Telecommunications Conglomerate Huawei and Subsidiaries Charged in Racketeering Conspiracy and Conspiracy to Steal Trade Secrets," U.S. Dept. of Justice, Feb. 13, 2020. https://www.justice.gov/opa/pr/chinese-telecommunications-conglomerate-huawei-and-subsidiaries-charged-racketeering.

35. Paul Rosenzweig and Kathryn Waldron, "Broadening the Lens on Supply Chain Security in the Cyber Domain," *R Street Policy Study* No. 170, April 2019, p. 3. https://www.rstreet.org/wp-content/uploads/2019/04/Final-No.-170.pdf.

36. "FCC Designates Huawei and ZTE as National Security Threats," Federal Communications Commission, June 30, 2020. https://www.fcc.gov/document/fcc-designates-huawei-and-zte-national-security-threats.

37. "Updated FAR Clause Expands Ban on Federal Contractor Use of Certain Chinese Telecom Equipment and Services," McGuireWoods Consulting, July 22, 2020. https://www.mcguirewoods.com/client-resources/Alerts/2020/7/updated-far-clause-expands-ban-federal-contractor-use-certain-chinese-telecom-equipment-services.

38. Justin Sherman, "Making Sense of a Huawei 'Partial Ban,'" *New America*, July 3, 2019. https://www.newamerica.org/cybersecurity-initiative/c2b/c2b-log/making-sense-huawei-partial-ban.

39. Paul Sandle, "Britain allows Huawei limited role in 5G networks," *Reuters*, Jan. 28, 2020. https://www.reuters.com/article/us-britain-huawei-tech/britain-allows-huawei-limited-role-in-5g-networks-idUSKBN1ZR1CL.

40. "Annual Report 2019: A Report to the National Security Advisor of the United Kingdom," Huawei Cyber Security Evaluation Oversight Board (HCSEC), March 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

41. Ibid., p. 2.

42. Ibid., p. 3.

43. Steve Ranger, "Huawei security: 'Significant' engineering flaws are a risk to our telecoms networks, says UK," *ZDNet*, March 28, 2019. https://www.zdnet.com/article/huawei-security-significant-engineering-flaws-pose-risk-to-networks-says-uk.

44. "Annual Report 2019," p. 3. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.

> The work of HCSEC summarised above reveals serious and systematic defects in Huawei's software engineering and cyber security competence. For this reason, the U.K.'s National Cyber Security Centre (NCSC) continues to advise the Oversight Board that it is only appropriate to provide limited technical assurance in the security risk management possible for equipment currently deployed in the UK, since NCSC has not yet seen a credible remediation plan.[45]

In other words, the NCSC warned the HCSEC that it is not possible to guarantee that the equipment already deployed in the United Kingdom is secure. And, while the HCSEC assesses Huawei products and makes recommendations, the U.K.'s overall 5G strategy is determined by its Department for Digital, Culture, Media and Sport. In 2019, that department's *U.K. Telecoms Supply Chain Review Report* determined that all vendors would be subjected to better cybersecurity standards, set by the Department.[46]

Despite its own acknowledgement that issues in Huawei equipment have not been remediated, the United Kingdom continued to cling to the idea that a strong, regulatory regime and additional oversight of high-risk vendors would mitigate risk. In January 2020, U.K. officials appeared utterly resistant to the urging of U.S. officials to ban Huawei from its 5G networks, announcing that Huawei would be allowed participate, albeit under certain restrictions. Instead of being completely prohibited, high risk vendors (which included Huawei) would be:

> [e]xcluded from all safety related and safety critical networks in Critical National Infrastructure; [e]xcluded from security critical 'core' functions, the sensitive part of the network; [e]xcluded from sensitive geographic locations, such as nuclear sites and military bases; [and l]imited to a minority presence of no more than 35 per cent in the periphery of the network, known as the access network, which connect devices and equipment to mobile phone masts.[47]

However, in July the United Kingdom did a surprising about-face, announcing that Huawei equipment would, in fact, be banned from the country's 5G network.[48] This reversal was generally seen as a victory for the Trump administration and a reflection of the United Kingdom caving for geopolitical reasons. In his announcement, Oliver Dowden, secretary of state for digital, culture, media and sport, stated:

> The new US measures restrict Huawei's ability to produce important products using US technology or software [...] Given the uncertainty this creates around Huawei's supply chain, the UK can no longer be confident it will be able to guarantee the security of future Huawei 5G equipment affected by the change in the US foreign direct product rules.[49]

British officials reportedly told Huawei officials the decision was a result of the United States Department of Commerce's actions, implying that if the American stance against China were to be relaxed in the future, the ban against Huawei could be revisited.[50]

GERMAN POLICY RESPONSE

Like the United Kingdom, Germany has also resisted American entreaties to ban Huawei from its 5G networks. And, indeed the German 5G strategy certainly acknowledges the importance of 5G security.[51] In fact, in 2019, Germany's Federal Office for Information Security (BSI) and its Federal Commissioner for Data Protection and Freedom of Information released a "catalog" of security requirements that any information and communications technology (ICT) provider would have to meet for 5G mobile networks.[52] It mandated, among other things, that:

> Security-related network and system components (critical key components) may only be used if they have been certified by the Federal Office for Information Security (BSI) and undergone IT security checks by a BSI-approved testing body. Critical key components may only be sourced from trustworthy suppliers/manufacturers, ie those that can provide assurance of their trustworthiness.[53]

45. Ibid., p. 20.

46. *UK Telecoms Supply Chain Review Report*, Dept. for Digital, Culture, Media and Sport, July 2019. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819469/CCS001_CCS0719559014-001_Telecoms_Security_and_Resilience_Accessible.pdf.

47. The Rt Hon Baroness Nicky Morgan, "New plans to safeguard country's telecoms network and pave way for fast, reliable and secure connectivity," Dept. for Digital, Culture, Media and Sport and the National Cyber Security Centre, Jan. 28, 2020 https://www.gov.uk/government/news/new-plans-to-safeguard-countrys-telecoms-network-and-pave-way-for-fast-reliable-and-secure-connectivity.

48. Adam Satariano et al., "U.K. Bars Huawei for 5G as Tech Battle Between China and the West Escalates," *The New York Times*, July 14, 2020. https://www.nytimes.com/2020/07/14/business/huawei-uk-5g.html.

49. Toby Helm, "Pressure from Trump led to 5G ban, Britain tells Huawei," *The Observer*, July 18, 2020. https://www.theguardian.com/technology/2020/jul/18/pressure-from-trump-led-to-5g-ban-britain-tells-huawei.

50. Ibid.

51. "5G Strategy for Germany," Federal Ministry of Transport and Digital Infrastructure, July 2017. https://www.bmvi.de/SharedDocs/EN/publications/5g-strategy-for-germany.pdf?__blob=publicationFile.

52. Federal Network Agency, "Bundesnetzagentur publishes key elements of additional security requirements for telecommunications networks," Federal Ministry of Economics and Technology, July 3, 2019. https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2019/20190307_SL.html.

53. Ibid.

Also, that they must be "sourced from those suppliers/manufacturers that can provide assurance of their trustworthiness in an appropriate manner."[54] And, while the catalog requires suppliers of critical components to sign a "no-spy clause," it is unclear whether this requirement can actually be enforced.[55] Moreover, based upon the rationale that barring particular entities would prevent a level playing field among an already limited number of equipment vendors, the catalog does not ban German ICT companies from using Huawei products as part of their networks.[56]

German officials argue that banning companies like Huawei is not advisable because diversity among suppliers is a crucial component of security. For example, at the 2020 annual World Economic Forum, German Chancellor Angela Merkel argued that "diversification and redundancy" were the best technical approaches to security and with respect to risky companies like Huawei suggested: "I don't think I make myself particularly secure if I completely eliminate providers in their entirety and then don't know how they develop."[57] In Merkel's view, then, the decision to ban a risky provider carries a risk of its own, as not doing business with companies like Huawei does not allow other countries and companies to stay abreast of their activities. German telecommunications companies have also argued that Huawei should not be banned from Germany. In August, Tim Höttges, the CEO of Deutsche Telekom, echoed the statements of government officials, arguing: "Regardless of politics, we should never allow dependence on one provider."[58]

While German officials are correct in identifying that a lack of diversity among suppliers is a serious security risk, preventing such 'monoculture' is only successful if the suppliers themselves are not actively working to abuse their position in said networks. Therefore, to ascertain capabilities and intent matters. And, while most software programs of any complexity contain flaws, the questions that must be asked are: whether those flaws were intentional or unintentional; whether and to what extent, a malicious actor or hostile governmental entity can exploit the flaws; and whether it is possible to effectively manage the associated risks.

54. Ibid.

55. Laurens Cerulus, "Why Germany's Huawei move irks more than just Washington," *Politico*, Oct. 16, 2019. https://www.politico.eu/article/germany-defies-us-on-huawei.

56. Andreas Rinke and Douglas Busvine, "New German rules leave 5G telecoms door open to Huawei," *Reuters*, Oct. 14, 2019. https://www.reuters.com/article/us-germany-telecoms-5g/new-german-rules-leave-5g-telecoms-door-open-to-huawei-idUSKBN1WT110.

57. Paul Carrel, "Risky to shut out any 5G provider completely: Merkel," *Reuters*, Jan. 23, 2020. https://www.reuters.com/article/us-davos-meeting-merkel-huawei-tech/risky-to-shut-out-any-5g-provider-completely-merkel-idUSKBN1ZM252.

58. Douglas Busvine, "Deutsche Telekom diversifies suppliers 'regardless of politics,'" *Reuters*, Aug. 13, 2020. https://www.reuters.com/article/us-deutsche-telekom-results-huawei-tech-idUSKCN2591A9.

LESSONS FOR 6G

Observing the increasingly hostile stance of the United States in regards to Huawei, as well as the struggle to persuade other countries of the correctness of this stance, provides us with a series of lessons policymakers should keep in mind when considering supply chain security and the future of telecommunications.

It is impossible to be truly neutral about a company's country of origin

It is undeniable that the biggest risk to using Huawei products stems from the fact that it is a Chinese company. While the question is still up for debate as to whether Chinese law allows its government to compel Huawei—either through formal legal process or informal but effectively compulsory means—to undertake surveillance or other malicious activities for or on behalf of the government, there is enough evidence to suggest they could that United States government officials should err on the side of assuming that the Chinese government has this power and can use it.

The HCSEC's discovery that Huawei equipment and software already contain numerous cybersecurity flaws significantly magnifies the risk to 5G networks. In theory, such flaws could enable a malicious actor to copy, alter or disrupt communications or data transmitted via such equipment. And, although it is unclear whether such flaws are intentional and whether they could (or would) be exploited, to the degree that they exist at all, the most effective cybersecurity framework must assume that malicious actors will use them for their own purposes.

Furthermore, even if the software contained no flaws or bugs at the time of being incorporated into 5G networks, there would still be the residual risk that comes from future updates. Software installed on any equipment is regularly and intentionally updated, although these updates generally require notice to, and the consent of, the network operators that have installed the software in their systems. However, these network operators may not always conduct a thorough examination of updates prior to installation for a variety of reasons that include a lack of time, resources or simply the inclination to do so.

Given this practical reality, it is not unreasonable to imagine a scenario in which Huawei could use the software update process to install tools that would enable it—at the direction of the Chinese government—to achieve the same ends a flaw or bug might. And, while it may stand to reason that Huawei and the Chinese government would know that some customers and foreign governments will eventually examine such software for bugs, it is a risk they may be willing to take immediately prior to or during a crisis from which the country could gain a strategic or tactical cyber advantage.

Put simply, for the purposes of creating a sound 5G infrastructure, it is too risky to "take their word for it" or to trust that China will not use any means at its disposal—including the manipulation of Huawei—to achieve its geopolitical ends.

Alliances are crucial to mitigating risk

While the U.K.'s reversal in regards to Huawei may be perceived as a particular win for the Trump administration, British officials aren't the only ones showing willingness to embrace more radical measures in the name of national security. Australia, Japan, New Zealand and India, among others, have all announced their intention to fully ban Huawei from their 5G networks.[59] And, this past July, the French National Cybersecurity Agency (ANSSI) was reported to have told French telecom companies that they won't be able to renew licenses for Huawei products once the licenses expire.[60]

Still, we should not mistake the decisions of the United Kingdom and others for global solidarity that a full ban is the best solution for dealing with Huawei. In June, Belgium's National Security Council followed the partial-ban strategy by restricting high-risk vendors in the "core" and "backbone" parts of 5G networks and capping use of such vendors in the "radio access" part of the network to 35 percent.[61] And there are still plenty of other countries where Huawei is still welcomed. For example, Huawei has been actively campaigning with different governments to play a leading role in the rollout of 5G networks across Latin and South America. In 2019, Huawei announced plans to create 5G telecommunications infrastructure in Argentina and Mexico as early as the next year. And at the 2019 BRICS summit Brazil's President Bolsonaro, stated: "China is increasingly part of Brazil's future."[62] In fact, most of the country's 4G networks were constructed by Huawei.[63]

The hesitation of some countries to follow American global leadership, especially when it is economically costly, is hardly surprising given that during his time in office, President Trump has frequently embarked on public tirades against America's traditional alliances, threatening to withdraw American support from the North Atlantic Treaty Organization (NATO) and liberally used tariffs and other economically punitive policies against allies. Even the United Kingdom admitted that their reversal regarding Huawei was not due to a true change in belief about the risk posed by Huawei but from the economic pressure resulting from the actions of the United States Department of Commerce. Therefore, U.S. policymakers must keep in mind that any national security strategy that relies upon global solidarity is likely to fail.

Excluding risky vendors is not enough to ensure network security

The way data is processed and distributed on a 5G network substantially erodes the distinction between the "core" and the "edge" for security purposes. As a result, the presence of Huawei equipment anywhere in a network poses enhanced risk that must be approached head on. And yet, limiting that equipment to the edge of the network is unlikely to be successful as a mitigation strategy even though the U.K. government appears to believe strongly that it is both possible and advisable to secure 5G networks by maintaining the distinction between the core and the edge of the network.

Few (if any) nations are closed off entirely from the rest of the world. If governments, corporations or individuals in one country communicate with a party in a foreign country, it is increasingly probable that those communications will be processed on Huawei equipment at some point in their travels—and this is true even if no Huawei equipment is present in a nation's domestic network. In the long run, it may be impossible for any country—including the United States—to avoid using Huawei equipment in its domestic networks if it wants them to provide high-quality performance at a competitive price. Forcing domestic telecommunications service providers to use second-rate and/or substantially more expensive equipment may impact their long-term viability, and may drag down the productivity of the nation's entire economy. In other words, if Huawei equipment is better and cheaper than that of its competitors, it will be hard for network operators to refuse to purchase and install Huawei equipment forever. In this sense, there may be some truth to Huawei's view that: "Restricting Huawei from doing business in the US will not make [it] more secure or stronger; instead, this will only serve to limit the US to inferior yet more expensive alternatives."[64]

In the short run, the United States' approach may reduce risks to the confidentiality, integrity and availability of data, but only insofar as the data is not transmitted to, from or through a location outside the United States. In the long run, any attempt—whether full or partial—to ban Huawei equipment from parts of 5G infrastructure may not be a sufficiently effective or realistic way to mitigate risk. Instead, U.S.

59. Ryan Daws, "India is the latest country preparing to ban Huawei from its 5G," *TechForge Media*, Aug. 14, 2020. https://telecomstechnews.com/news/2020/aug/14/india-latest-country-ban-huawei-5g.

60. Mathieu Rosemain and Gwénaëlle Barzic, "Exclusive: French limits on Huawei 5G equipment amount to de facto ban by 2028," *Reuters*, July 22, 2020. https://www.reuters.com/article/us-france-huawei-5g-security-exclusive/exclusive-french-limits-on-huawei-5g-equipment-amount-to-de-facto-ban-by-2028-idUSKCN24N26R.

61. Laurens Cerulus, "Belgium to cut down on Huawei gear," *POLITICO*, June 25, 2020 https://www.politico.eu/article/belgium-huawei-restrictions.

62. Ravi Bangar, "Will Huawei weather 5G storms in Latin America?", *Financial Express*, July 27, 2020. https://www.financialexpress.com/world-news/will-huawei-weather-5g-storms-in-latin-america/2036098.

63. Ibid.

64. Arjun Kharpal, "Here's how Trump's latest executive order could affect Huawei," *CNBC*, May 15, 2019. https://www.cnbc.com/2019/05/16/huawei-us-5g-block-after-trump-executive-order.html.

policymakers should assume in advance that the global telecommunications network will be vulnerable and seek additional, alternative measures to mitigate the risk. For example, the government's widespread adoption and encouragement of end-to-end encryption could help mitigate these risks by making it more difficult for Huawei to potentially access data. Similarly, the United States should seek to reduce barriers to global trade (such as tariffs) as retaliatory measures can make American and European companies less competitive internationally, which provides Chinese state-sponsored companies with additional appeal. Policymakers should also look to reduce any regulatory barriers to economic competition that are keeping potential American companies from entering the telecom market and providing more secure alternatives to Huawei.

CONCLUSION

China is a long-term threat to the United States and its allies, and it effectively uses a variety of cyber-enabled means to achieve its tactical and strategic objectives. This includes using Chinese commercial enterprises in a variety of ways. The presence of Huawei equipment in the global 5G supply chain presents a potential threat to American national security as, without legitimate checks on the power of the Chinese Communist Party, there is no way to truly ascertain the independence of Chinese companies from the Chinese government. Thus far, the United States and some of its allies have attempted either full or partial bans to mitigate the risk associated with the presence of Huawei equipment. However, while both of these strategies may work in different ways in the short term, they are unlikely to effectively mitigate the cybersecurity risk associated with Huawei's 5G equipment in the long run.

For example, the United States' full-ban approach does not address the reality that Huawei equipment is already present in significant portions of the global telecommunications infrastructure or that many countries and providers will purchase and install Huawei equipment in the future because it is relatively high quality, affordable and marketed effectively. Moreover, this approach is too similar to the very perimeter-only cyber-defense strategy that is no longer effective. It may also prove difficult for the United States to keep Huawei equipment out of U.S.-based networks because there are so few competitors in this market segment and because all of Huawei's main competitors in the 5G infrastructure market—Ericsson, Nokia and Samsung—are also foreign-based companies over which the U.S. government has limited control.

Yet, the partial-ban approaches of the United Kingdom and Germany are also ineffective. Although we assume that those governments conduct thorough and expert reviews of the Huawei equipment that they examine, it is possible that Huawei could update software for equipment that is already reviewed and installed in networks with code that could facilitate Chinese military and intelligence objectives, especially in a time of crisis, where there is a low probability of detection on a timely basis.

Instead, policymakers must look for alternative methods to ensure security, including technical solutions, such as treating telecommunication networks as zero-trust networks or widespread end-to-end encryption. Additionally, policymakers should seek to encourage additional entrants into the telecommunications market by removing regulatory barriers to entry, which would help address fears of creating a security monoculture. But these strategies must be embraced now if we want to ensure the future of telecommunications is secure. Otherwise, 6G will be here before we have prepared for it, with China potentially leading the way.

ABOUT THE AUTHOR

Kathryn Waldron is a fellow with the National Security and Cyber Security team at the R Street Institute.