AMERICAN FOREIGN POLICY COUNCIL

DEFENSE TECHNOLOGY PROGRAM BRIEF

Mend the Gap: 5G, the US-UK Split over Huawei, and National Security Implications

By: Michael Sobolik

BRIEFING HIGHLIGHTS

Britain's decision [to allow Huawei built 5G infrastructure] presents acute challenges to the U.S. In making its choice, London failed to consider the way in which the Chinese Communist Party (CCP) conceptualizes economic competition and military development – and how this context might impact its own network security. The UK's decision may jeopardize intelligence sharing within the FVEY network, and will almost certainly complicate strategic planning within NATO.

◆ ◆ ◆

London claims to share concerns about the security risks Huawei's presence poses to telecommunication networks. Britain's National Cyber Security Centre stated that it has always considered the company higher risk, that Huawei's low quality products made them susceptible to exploitation, and that the PRC could order Huawei to conduct espionage activity under China's 2017 National Intelligence Law. Even so, the British government is basing its technical understanding of 5G on Huawei's own assessments that directly contradict the positions of the United States, Australia, and European telecommunication companies.

◆ ◆ ◆

In testimony before the Senate Armed Services Committee in March 2020 Secretary of Defense Mark Esper stated, "If our NATO allies incorporate Huawei technology it may very well have a severe impact on our ability to share information, to share intelligence, to share operational plans, and for the alliance to conduct itself as an alliance."

◆ ◆ ◆

It is unclear whether the U.S. still has a window of opportunity to blunt Huawei's 5G market dominance. Washington can protect its own networks, and even encourage private companies like Dell and Microsoft to further their plans for a homegrown 5G solution, but it is unclear whether any such company would be competitive globally soon enough to offer an alternative.

BACKGROUND ON 5G

5G, or "fifth generation," is the latest iteration of telecommunications technology. Unlike the transition from 3G to 4G ten years ago, which brought about marginally faster processing speeds, this upcoming transition will revolutionize technology in everyday life. A 5G network will be able to service ten times more devices in a given square mile than a 4G system, and do so at twenty times the processing speed.[1] This capability enables new possibilities for devices to interact with each other. This synergy, called the Internet of Things (IoT), will underpin a broad range of technology, from autonomous vehicles and remote medicine to "smart houses" and "smart cities."

On January 28, 2020, the British government concluded its security assessment on the nation's 5G infrastructure buildout. At the center of Downing Street's internal deliberations was Chinese telecommunications giant Huawei, and the implications of allowing an entity with connections to the Chinese government into its next-generation networks. The timing of the decision coincided with "Brexit," the UK's withdrawal from the European Union, which saddled Britain with the need to negotiate a series of new bilateral free trade agreements, most urgently with Washington and Beijing. But Britain's commercial reliance on China's market clashed with its longstanding intelligence partnership with the Five Eyes (FVEY) countries – the United States, Canada, Australia, and New Zealand – further politicizing the review.

Ultimately, British Prime Minister Boris Johnson decided to allow "high risk vendors" like Huawei to participate in the country's 5G buildout, subject to a 35% market cap with technological and geographic restrictions.[2] British authorities claimed they had forged a win-win solution that achieved market diversity while protecting networks, thus avoiding the need to choose politically between the U.S. and China. In public remarks with Prime Minister Johnson two days later, U.S.

Michael Sobolik *joined AFPC as a Fellow in Indo-Pacific Studies in September 2019. His work covers American and Chinese grand strategy, regional economic and security trends, America's alliance architecture in Asia, and human rights. Michael also serves as editor of AFPC's* Indo-Pacific Monitor *e-bulletin, AFPC's review of developments in the region. His analysis has appeared in* The Diplomat, The Hill, The National Interest, *and* Providence. *Prior to joining AFPC, Michael served as a Legislative Assistant in the Senate from 2014 to 2019 and managed an Indo-Pacific policy portfolio. While in the Senate, Michael drafted legislation on China, Russia, India, Taiwan, North Korea, and Cambodia, as well as strategic systems and missile defense.*

Secretary of State Mike Pompeo insisted that he was "very confident that our two nations will find a way to work together to resolve this difference," and that "the Five Eyes relationship… is deep, it is strong, and it will remain."[3] A month after these comments, however, President Trump approved an interagency review led by the National Security Council (NSC) to determine whether the U.S. needs to relocate military and intelligence assets from the UK.[4]

Despite Washington's public efforts to save face, Britain's decision handed a significant defeat to the United States and a commensurate victory to the People's Republic of China (PRC). Moreover, the British decision could become part of a larger pattern. For instance, German Chancellor Angela Merkel has signaled her desire to avoid an outright ban on Huawei and her inclination to adopt security standards that mirror Britain's approach.[5] Recent reports also indicate that France will allow high risk vendors like Huawei to equip portions of its 5G network.[6]

Britain's decision presents acute challenges to the U.S. In making its choice, London failed to consider the way in which the Chinese Communist Party (CCP) conceptualizes economic competition and military development – and how this context might impact its own network security. The UK's decision may jeopardize intelligence sharing within the FVEY network, and will almost certainly complicate strategic planning within the North Atlantic Treaty Organization (NATO). Policymakers in Washington will need to grapple with these challenges in the months ahead.

THE ESSENCE OF THE DISPUTE

Behind Washington and London's antipodal positions on Huawei is a fundamental disagreement over the structure of a 5G network. Central to this disagreement is the concept of a network "core" and "edge."

In the 4G networks that populate the world today, personal devices like computers and smart phones connect to the internet via a series of antennae and base stations called the Radio Access Network (RAN). RAN hardware and software is located at a network's "edge," where people live, work, and travel. Telecommunications companies install base stations and antennae in alleyways, along highways and throughout city blocks to service the general population.

When someone at the edge connects to the internet, the RAN relays queries from devices to the "core," the network's hub that handles sensitive functions related to privacy and information content like online credit card payments and messages. RAN equipment routes this encrypted content appropriately, but in theory it only serves a "dumb" function while software at the "smart" core decrypts data and resolves queries. In practice, law enforcement agencies and designated individuals at network providers retain access to information passing through base stations (a concept known as "lawful intercept"), but RAN manufacturers like Huawei, Nokia, and Ericsson do not have this authorized access.[7]

*Behind **Washington** and **London's** antipodal positions on Huawei is a **fundamental disagreement** over the structure of a **5G network**. Central to this disagreement is the concept of a network "core" and "edge."*

For many countries, this distinction between a 4G network's core and edge provided an elegant solution for securing information. As long as core hardware and software were secure, the thinking went, the entire network was secure. Even if a high risk vendor's equipment and components were present in the RAN, they merely performed routing functions, and the vendor itself could not enter or exploit the system because the data remained encrypted while in transit. This assumption opened many doors for Huawei into developed nations, including Britain.[8] In 2010, the UK's National Cyber Security Centre (NCSC) partnered with Huawei and established the Huawei Cyber Security Evaluation Centre (HCSEC), an organization that allows British engineers to examine Huawei products and test for vulnerabilities.[9] NCSC Technical Director Ian Levy pointed to the HCSEC as a factor that informed Britain's decision to continue partnering with Huawei in 5G.[10]

However, the shift from 4G to 5G marks a fundamental break in network structure. Because the Internet of Things (IoT) depends on low latency and essentially zero-buffering, processing speeds need to run orders of magnitude faster than those a 4G system can service. Reducing lag in 5G demands that the physical space between a network's core and edge be at least significantly reduced – at most, it must be blurred. In the short term, telecommunications companies will install more

base stations in a given area while bringing core hardware physically closer to the edge. In the medium- to long-term, virtualized functions (i.e., core software) will by necessity run on edge hardware as devices within the IoT grow increasingly interdependent. The seamless integration and zero-lag that autonomous vehicles, remote medicine, and "smart cities" demand will necessitate this shift.[11]

As core functions move to the edge, network security will grow in importance and complexity. The State Department has insisted that this structure places a premium on vendor trust, not on a government's ability to control risk.[12] Australia reached this conclusion after its 5G review in 2018, forecasting that in 5G "the distinction between the core and the edge will disappear over time… Government has found no combination of technical security controls that sufficiently mitigate the risks."[13]

The British government does not share this understanding of 5G networks, however. When NCSC Technical Director Ian Levy announced the Huawei decision in January 2020, he insisted that "sensitive functions [i.e. the network core] are still sensitive functions and you can put your arms around them."[14] According to Levy, even if a mature next-generation network required core processing within edge infrastructure – a technology called mobile edge compute (MEC) – as long as a high risk vendor like Huawei was not supplying MEC software, the network would remain "equivalently safe."[15] For its part, Huawei had commissioned a report from consulting firm Ovum that reached similar conclusions in July 2019. It noted: "From a security perspective, this separation means that RAN operation cannot affect core security protocols. The RAN is the 'idiot savant' of the 5G mobile network. It is brilliant at transferring radio data between user devices and the core, but it does little else. The focus of 5G security concerns is therefore the 5G core."[16]

Shortly before British Prime Minister Boris Johnson announced the final Huawei decision, U.S. government officials traveled to Europe to dispute these assumptions. Led by Deputy National Security Council Advisor Matthew Pottinger, the delegation delivered intelligence to British and German officials that indicated Huawei has maintained backdoor access into its equipment since 2009. According to an exclusive February 12, 2020 *Wall Street Journal* report, Washington shared evidence of the Chinese company's ability to exploit the "lawful intercept interfaces" reserved for law enforcement and service providers.[17] A German Federal Foreign Office document characterized the U.S. intelligence as akin to a "smoking gun."[18] Moreover, European telecommunications company Ericsson has raised concerns about high-risk vendors operation within 5G edge networks that directly contradict the position of Ovum and Huawei:

> Some papers, such as Ovum's *The Facts on 5G* argue that RAN is a largely insignificant part of a 5G network and cannot affect the confidentiality and integrity of 5G services. Technically however, this is wrong, as the [5G base station] is the termination point for encryption and integrity protection and, potentially, the user plane can be accessed in clear text… *the technical aspect of security in RAN is as critical as the core network when it comes to confidentiality and integrity* (emphasis added).[19]

The UK insists that it has never found a concrete instance of Huawei behaving nefariously. This assessment ignores the CCP's unique understanding of warfare, expressed within its autarkic economy, that birthed ***Huawei*** *and fostered its current dominance. The company's* ***success*** *is a* ***microcosm of the Party's*** *decades-long* ***campaign to subvert*** *the U.S.-led* ***international order.***

London claims to share concerns about the security risks Huawei's presence poses to telecommunication networks. In its final announcement on January 28, 2020, Britain's National Cyber Security Centre stated that it has always considered the company higher risk, that Huawei's low quality products made them susceptible to exploitation, and that the PRC could order Huawei to conduct espionage activity under China's 2017 *National Intelligence Law*.[20] Article 7 of that law mandates that PRC citizens and organizations "shall support, assist and cooperate with the state intelligence network…"[21] Even so, the British government is basing its technical understanding of 5G on Huawei's own assessments that directly contradict the positions of the United States, Australia, and European telecommunication companies.

Moreover, the UK insists that it has never found

a concrete instance of Huawei behaving nefariously.[22] This assessment ignores the CCP's unique understanding of warfare, expressed within its autarkic economy, that birthed Huawei and fostered its current dominance. The company's success is a microcosm of the Party's decades-long campaign to subvert the U.S.-led international order.

HUAWEI AND CHINESE STRATEGY

The CCP's concept of national security is expansive. In remarks to the PRC National Security Commission in April 2014, Secretary General Xi Jinping advocated for a "holistic view" based on "political, homeland, military, economic, cultural, social, science and technology, information, ecological, resource, and nuclear security."[23] The PRC finalized its *National Security Law* the following year and adopted Xi's framework. Article 2 defines national security as "the relative absence of international or domestic threats to the state's power to govern… and the ability to ensure a continued state of security."[24] This broad understanding of national security colors the Party's approach to economic development and geopolitical competition. In remarks to members of the Chinese Academy of Sciences (CAS) and the Chinese Academy of Engineering (CAE) the same year, the subtext in Xi's exhortation to "catch up" and "surpass" world leaders in scientific and technological development was unmistakable. Both institutions have links to the State Administration for Science, Technology and Industry for National Defense (SASTIND), the lead policymaking body within the PRC for integrating civil and military development.[25]

From the days of Mao Zedong to Deng Xiaoping, catching up to the industrialized world was the overriding strategic objective of the CCP. The tragedy of the "Great Leap Forward," a dual-tracked agrarian and industrial plan designed to leapfrog past the Soviet Union that induced mass starvation and death, was the CCP's first attempt to do so. Under Deng Xiaoping's market-oriented reforms, the People's Republic of China (PRC) grew from a backwater Communist economy to an industrial juggernaut within 20 years. By 2012, the PRC was one of the world's largest economies and constituted 18% of global manufacturing.[26]

But simply catching up was never the ultimate goal. Mao made his intentions clear in a conversation with Soviet Premier Alexei Kosygin in 1965: "The U.S. and the USSR are now deciding the world's destiny. Well, go ahead and decide. But within the next 10-15 years you will not be able to decide the world's destiny. It is in the hands of the nations of the world, and not in the hands of the imperialists, exploiters, or revisionists."[27] Ten years prior, Mao had been even more candid: "Our objective is to catch up with America and then to surpass America."[28] Deng Xiaoping's dictum to "hide our capabilities and bide our time" was a tactical decision to conceal these intentions from the world.

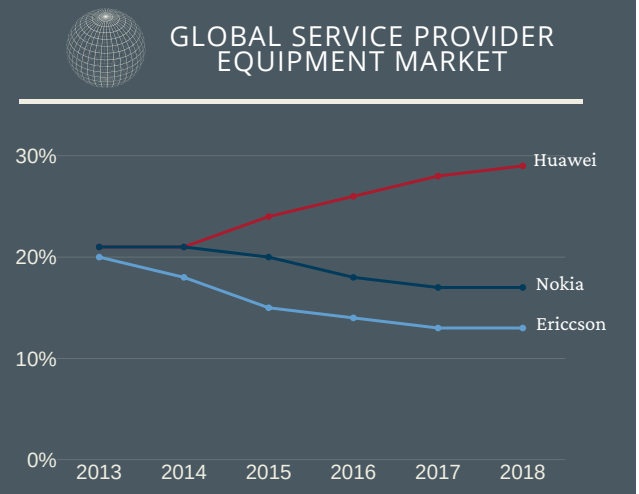
When the United States and other Western governments welcomed the PRC into the World Trade Organization (WTO), they were hopeful that the Chinese leadership would realize the economic gains of free trade and become a willing participant, or a "responsible stakeholder," in the global free trade regime.[29] Chief among Western expectations was that China would transition away from a planned economy to a market economy. But the Party's ambitions, as well as its fusion of economic and security competition, required an innovative approach to capitalism – specifically, retaining state ownership and control of critical industries[30] and restricting foreign access to its domestic market.[31] Huawei's rapid ascent and success occurred within this context, and typifies the Party's determination to maintain state control of a wide range of industries it views as strategically important.

In 1983, Ren Zhengfei, a member of the PLA engineering corps, retired from military service. After brief employment at state-owned Shenzhen Electronics Corp., Ren left and founded Huawei with an $8.5 million loan from a state bank. By 1993, Huawei had secured a contract with the PLA and sourced indigenously-produced components directly to the army. The following year, Ren scored a meeting with Communist Party General Secretary Jiang Zemin and pushed him to close China's market to foreign telecommunications companies, a step that Jiang took in 1996. Huawei dominated the market in China by offering steep discounts and undercutting its competition, in some cases offering free services to government entities.[32]

Today, Huawei's market dominance is global and covers next generation equipment, components, and devices. Within China, the PRC reserves 70% of its telecommunications market for Huawei and fellow tech giant ZTE. In global markets, Chinese subsidies and government financing have allowed Huawei to undercut Western companies. A leaked 2017 White House memorandum warned that "Huawei has gone from a market

share in radio infrastructure of roughly 11 percent in 2011 to a share equal to or greater than Ericsson and Nokia, the two largest Western mobile infrastructure suppliers. Similarly, in routing, Huawei more than doubled its market share in an 18-month period, and in several areas or routing it has caught or surpassed market leader Cisco."[33] Two years later, Huawei's telecommunications equipment captured 29% of the global market, surpassing European competitors Nokia and Ericsson with 17% and 13% respectively (see Figure 1).[34] Within Europe, Huawei and ZTE succeeded in capturing 40% market share of 4G equipment within fifteen years.[35]

FIGURE 1



Source: "Telecommunications equipment" encompasses Broadband Access, Carrier IP Telephony, Microwave, Mobile RAN, Optical, SP Router and CE Switch, and Wireless Packet Core. See Stefan Pongratz, "Key Takeaways – Worldwide Telecom Equipment Market 2018," Dell'Oro Group, March 4, 2019, https://www.delloro.com/telecom-equipment-market-2018-2/.

According to a 2012 report from the House Permanent Select Committee on Intelligence (HPSCI), nominally private companies like Huawei and ZTE are still beholden to the CCP, which can "exert influence over the corporate boards and management of private sector companies, either formally through personal choices, or in more subtle ways."[36]

As such, it is impossible to separate Huawei as a company from the Party's strategic ambitions. Its historical links to the PLA are troubling enough, but the CCP's broad understanding of national security turns every policy realm into a battleground. The 2013 edition of *The Science of Military Strategy* singles out telecommunication networks as the "basic foundation of society and have become critical for national security and the development of national interest and a major new domain for military conflict."[37] Telecommunications equipment from companies like Huawei therefore expose host nations to risk of exploitation, espionage, influence, and disruption.

THE CRUX OF THE CHALLENGE

In February 2019, Secretary Pompeo traveled throughout Europe to warn partners of these risks. While in Hungary, he was candid about the stakes involved: "It also makes it more difficult for America to be present. If that equipment is co-located where we have important American systems, it makes it more difficult for us to partner alongside them."[38] However, Pompeo did not publicly specify equipment or locations, and Hungary's Foreign Minister Peter Szijjarto deflected his concern: "When it comes to cooperation with Russia or cooperation with the People's Republic of China, that does not harm us being reliable as a NATO ally."[39] And when Britain announced its decision in January 2020, Foreign Secretary Dominic Raab insisted that Huawei's presence in 5G networks was a separate issue from the security and intelligence considerations. "I want to be absolutely clear that nothing in this review affects the country's ability to share highly sensitive intelligence data over highly secure networks both within the UK and our partners including the Five Eyes," he said.[40]

Raab could technically be correct. The FVEY network is secretive, but intelligence sharing among partners likely takes place over highly secured networks independent of civilian infrastructure. Pompeo's public vote of confidence in FVEY reinforces this assumption. Even so, neither Raab nor Szijjarto addressed the broader issue of co-location.

The United States military maintains 259 military sites throughout 13 European countries (see Figure 2).[41] Its presence there reassures NATO partners and deters Russian territorial ambitions, but these bases and the personnel that man them are also integrated into America's global posture. In a crisis scenario, the Department of Defense's (DoD) top priority is joint mobilization – the process of deploying personnel and material into the priority theater efficiently and quickly. This process is global in scope. According to DoD's guidance on the subject, "Two important attributes of [Global Force Management] include being able to globally assess force sourcing risk to address mitigation options and enabling global sourcing with the best force sourcing option, regardless of command, organization, or Service to which the force or personnel are assigned."[42]

FIGURE 2

DOD MILITARY SITES IN EUROPE

Source: U.S. Department of Defense, "Base Structure Report – Fiscal Year 2018 Baseline: A Summary of the Real Property Inventory Data," n.d., https://www.acq.osd.mil/eie/Downloads/BSI/Base%20Structure%20Report%20FY18.pdf.

Joint mobilization is also complex. DoD divides joint mobilization into twelve resource areas,[43] but key among them are manpower, equipment, facilities, services, and communications. The forward-deployed U.S. military relies on host-nation support to supplement these resources and "offset requirements for corresponding US military resources that are not affordable or practical to maintain in peacetime."[44] While most of this process takes place over classified U.S. military networks, logistics functions like administration and personnel data, communications with contractors, and deployment force lists often rely on unclassified networks, including the U.S. military's Non-secure Internet Protocol Routing Network (NIPRNet) and commercial telecommunication infrastructure.[45] Relying solely on secured networks in a crisis may be difficult because the joint mobilization process by definition bleeds into domestic infrastructure.[46] The DoD has openly identified its reliance on unclassified networks as a primary threat.[47]

In 4G networks, a vendor like Huawei could monitor network traffic and gain advance intelligence of mobilization by virtue of lawful intercept exploitation. In the age of 5G, Huawei's ability to intercept, surveil, and disrupt networks increases as the core/edge distinction breaks down. According to Mike Burgess of the Australian Signals Directorate, "[t]he distinction between core and edge collapses in 5G networks. That means a potential threat anywhere in the network will be a threat to the whole network."[48]

Put bluntly, Huawei infrastructure has the ability to detect early warning indicators of NATO military mobilization, and could sabotage active operations in a host nation.

*Put bluntly, **Huawei infrastructure** has the ability to detect early warning indicators of NATO military mobilization, and **could sabotage active operations** in a host nation.*

This risk is not theoretical. In April 2019, the *Washington Post* reported that the U.S. Embassy in Germany had warned Berlin that Huawei's presence in German 5G networks "could in the future jeopardize nimble cooperation and joint mobilization, particularly in times of crisis."[49] The Department of State has relayed these concerns to Capitol Hill as well. After Britain announced its decision to limit Huawei equipment to the RAN, Senator Ted Cruz (R-TX) cautioned that doing so "will not succeed in limiting Huawei's ability to conduct espionage, interfere with critical infrastructure or mobilization, or even access more sensitive nodes in the telecom network."[50] Secretary of Defense Mark Esper echoed these assessments in testimony before the Senate Armed Services Committee in March 2020. "If our NATO allies incorporate Huawei technology," Esper noted, "it may very well have a severe impact on our ability to share information, to share intelligence, to share operational plans, and for the alliance to conduct itself as an alliance."[51]

These military risks could have political ramifications within FVEY in ways that are difficult to quantify. The partnership collects and shares highly sensitive signals intelligence (SIGINT) on space tracking, early warning indicators, and ballistic missile defense kill chain.[52] This cooperation among the U.S., UK, Canada, Australia, and New Zealand is based on implicit trust. Even assuming communications remain secure within the FVEY network, the United States and other participants will now need to weigh the political risk of a partner whose critical infrastructure and digital economy rely on potentially compromised equipment.

GIVING IN, OR GIVING UP?

The United States faces difficult decisions regarding its relationship with Great Britain, the NATO alliance, and Europe as a whole. Washington's campaign to isolate Huawei through legal action[53] and financial sanctions[54] has on the whole failed to persuade European allies and partners of the risk the company poses to their governments. A 2019 report by Oxford Information Labs characterizes these actions as little more than "white noise" that "impairs [America's] ability to make the case for an American-led international order as it did in the Cold War."[55] Recent disagreements between the U.S. and the "E3" (Great Britain, France, and Germany) on the Nord Stream II natural gas pipeline and the 2015 Iran nuclear deal known as the Joint Comprehensive Plan of Action provide the backdrop for the contemporary impression of America that prevails in Europe today: one that is unwilling to cooperate and resistant to seeking multilateral outcomes. The final report of the 2020 Munich Security Conference eloquently captured the current divide. "Today, however, it is evident that something more fundamental at play," it reads. "The Audience came away with a distinct impression that there was no common understanding of what the West represents."[56]

As America grapples with this challenge, policymakers are caught between two antipodal perspectives. Some in Washington are calling for the U.S. government to step into the telecommunications market and inject capital into Western companies, even buying a controlling stake in them, as a way to more effectively compete with Huawei. U.S. Attorney General William Barr made this very argument back in February,[57] but others inside the Trump administration had already proposed a similar plan in 2017 for the American 5G buildout.[58] *The Better Utilization of Investment Leading to Development (BUILD) Act of 2018*, a law passed by the 115th Congress that authorizes the International Development Finance Corporation (formerly the Overseas Private Investment Corporation) to buy a controlling stake in overseas companies, typifies this approach of countering Chinese economic influence.[59]

*Washington's **campaign to isolate Huawei** through legal action and financial sanctions has on the whole **failed to persuade European allies** and partners of the risk the company poses to their governments.*

Simultaneously, several members of Congress are raising doubts about the health of U.S.-UK relations and the outlook for FVEY. Weeks before Britain's Huawei decision, senators introduced legislation that would prohibit U.S. intelligence agencies from sharing intelligence products with any country that permits Huawei to operate within its 5G networks.[60] And in response to the British government's choice, some members have even gone so far as to call into question the viability of the "special relationship" between Washington and London.[61] The frustration captured in these statements and legislation stems from a longstanding ideological division between America and Europe on security matters. "It is time," Robert Kagan wrote in 2003, "to

stop pretending that Europeans and Americans share a common view of the world, or even that they occupy the same world."[62] There is an appetite among some in Washington to call it quits with Europe if its countries jeopardize NATO cooperation and fail to take their own security seriously.

Policymakers should weigh these options with care. Marshalling state resources to create a "Western Huawei" does not play to America's strengths. Indeed, adopting the PRC's economic model moves the U.S.-China competition to territory favorable to the CCP, for the American political system will never be able to match Chinese funding dollar-for-dollar. By definition, the free market cannot produce "national champions." Western governments flirt with statist economic agendas if they seek to replicate China's strategy. Moreover, it is unclear whether the U.S. still has a window of opportunity to blunt Huawei's 5G market dominance. Washington can protect its own networks, and even encourage private companies like Dell and Microsoft to further their plans for a homegrown 5G solution, but it is unclear whether any such company would be competitive globally soon enough to offer an alternative.[63]

*The **United States needs to** take steps to insulate and **protect its "special relationship"** with the **UK**. This means that Washington should refrain from reflexively seeking to blacklist the UK from FVEY on the basis of its concerns over China.*

Moreover, attempting to do so plays into CCP propaganda. PRC diplomats regularly call on Western governments to allow fair competition and open markets to Huawei, and more recently they have portrayed American concerns about network security as a protectionist agenda.[64] British Prime Minister Boris Johnson adopted this rhetoric as well, challenging Washington to "tell us what is the alternative."[65] German Chancellor Angela Merkel, for her part, has expressed reservations about banning a company "simply because it's from a certain country."[66] Of course, taking these statements at face value ignores the PRC's autarkic model that produced Huawei, the company's track record of intellectual property theft,[67] and the CCP's political control over companies like Huawei via China's 2017 *National Intelligence Law*. Nonetheless, they reflect a significant wellspring of support that China now enjoys among Western nations.

Moreover, the United States needs to take steps to insulate and protect its "special relationship" with the UK. This means that Washington should refrain from reflexively seeking to blacklist the UK from FVEY on the basis of its concerns over China. The history of U.S.-UK intelligence sharing, after all, began in 1917 when London intercepted the "Zimmerman Telegram" and warned Washington about Germany's intent to bring Mexico into World War I.[68] Britain also shared intelligence on the Nazi ENIGMA code with the U.S. during World War II.[69] And America's successful resolution of the Cuban Missile Crisis owed a great deal to the British Secret Intelligence Service and its Russian asset Colonel Oleg Penkovsky.[70] Britain, in short, has a proven track record as a dependable intelligence ally for America.

The United States, moreover, continues to derive great benefit from British intelligence today. According to James S. Cox, the former Deputy Assistant Chief of Staff Intelligence at NATO Supreme Headquarters, the FVEY network relies extensively on UK intelligence for Western Russia. Other sources also suggest that the UK has a special assignment for Africa.[71] Given Russia's 2014 invasion of Ukraine and Vladimir Putin's larger territorial ambitions, as well as China's extensive operations throughout Africa, U.S. intelligence agencies would be rash to hastily discard a relationship with British counterparts that spans a century. Doing so would risk isolating the United States from erstwhile partners and fulfill the fears of many governments who are not yet prepared or able to make a strategic choice between Washington and Beijing.

MEND THE GAP

What, then, is the proper way forward? It begins with an internal review. Before Washington weighs adjustments in economic policy or reevaluates strategic partnerships, policymakers in Executive Branch agencies should complete the NSC-led risk assessment that seeks to glean the answers to a number of critical questions.

For the Department of Defense, these include:

- How does the DoD expect 5G technology to impact military mobilization, specifically with resource areas it relies upon from host nations?
- How many active acquisition and cross-servic-

ing agreements does the DoD have with host nations that allow high-risk vendors into their domestic telecommunications networks?
- Of those agreements, what resource area(s) of joint mobilization do these host nations provide to the DoD?
- What is the level of dependence these resource areas have on telecommunications networks with equipment from high-risk vendors?
- What is the likelihood of a high-risk vendor's ability to intercept, surveil, or disrupt host nation support?
- What is the estimated impact of interception, surveillance, and disruption? If it is substantial, can the DoD mitigate risk while maintaining partnerships with the host nations in question?

For the Office of the Director of National Intelligence, a different set of questions applies, among them:
- Is the U.S. intelligence community (IC) confident in its ability to share intelligence in a secure manner with governments that have high-risk vendors operating in domestic telecommunications networks?
- Could the presence of high-risk vendors in foreign telecommunications networks impact or compromise the work of American assets in-field?

As for the Department of State, it should determine whether foreign governments have acknowledged or share U.S. government concerns about the impact of high-risk vendors on joint mobilization efforts. If not, why not?

The stakes are high. Huawei's dominance and market share complicates America's national security equities throughout Europe. The company's success threatens to bifurcate the West and weaken America's alliance network. U.S. policymakers need to recognize this threat. But they also need to avoid acting hastily, instead taking the time to assess risk and measure impact. The global security network that served Americans so well in the previous century depends on it.

ENDNOTES

1. Patterson Clark, "The What, When, and How of 5G," *Politico*, February 25, 2020, https://www.politico.com/news/agenda/2020/02/25/the-what-when-and-how-of-5g-114485.
2. Government of the United Kingdom, National Cyber Security Centre, "NCSC advice on the use of equipment from high risk vendors in UK telecoms networks," January 28, 2020, https://www.ncsc.gov.uk/guidance/ncsc-advice-on-the-use-of-equipment-from-high-risk-vendors-in-uk-telecoms-networks.
3. William James, "Pompeo backs 'Five Eyes' intelligence sharing despite UK decision on Huawei," Reuters, January 30, 2020, https://www.reuters.com/article/us-britain-usa-huawei-pompeo/pompeo-backs-five-eyes-intelligence-sharing-despite-uk-decision-on-huawei-idUSKBN1ZT1IV.
4. Eli Lake, "The U.S.-U.K. Alliance Could Soon Get Much Weaker," *Bloomberg*, March 5, 2020, https://www.bloomberg.com/opinion/articles/2020-03-05/u-k-huawei-decision-prompts-u-s-review-of-intelligence-assets.
5. Katrin Bennhold and Jack Ewing, "In Huawei Battle, China Threatens Germany 'Where It Hurts': Automakers," *New York Times*, January 16, 2020, https://www.nytimes.com/2020/01/16/world/europe/huawei-germany-china-5g-automakers.html.
6. Mathieu Rosemain and Gwénaëlle Barzic, "Exclusive: France to allow some Huawei gear in its 5G network – sources," *Reuters*, March 12, 2020, https://www.reuters.com/article/us-france-huawei-5g-exclusive/exclusive-france-to-allow-some-huawei-gear-in-its-5g-network-sources-idUSKBN20Z3JR.
7. Bojan Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks," *Wall Street Journal*, February 12, 2020, https://www.wsj.com/articles/u-s-officials-say-huawei-can-covertly-access-telecom-networks-11581452256.
8. James Kynge and Nic Fildes, "Huawei: the indispensable telecoms company," *Financial Times*, January 31, 2020, https://www.ft.com/content/24b01f0e-441e-11ea-a43a-c4b328d9061c.
9. Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board, "Annual Report 2019: a report to the National Security Adviser of the United Kingdom," March 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/790270/HCSEC_OversightBoardReport-2019.pdf.
10. Ian Levy, "The future of telecoms in the UK," National Cyber Security Centre, January 28, 2020, https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk.

11. Janka Oertel, "Europe and China after Brexit: The 5G question," European Council on Foreign Relations, December 19, 2019, https://www.ecfr.eu/article/commentary_europe_and_china_after_brexit_the_5g_question.
12. U.S. Department of State, "Press Briefing with Deputy Assistant Secretary Robert Strayer," July 11, 2019, https://translations.state.gov/2019/07/11/press-briefing-with-deputy-assistant-secretary-robert-strayer/.
13. Government of the United Kingdom, Minister for Communication and the Arts, "Government Provides 5G Security Guidance To Australian Carriers," August 23, 2019, https://www.minister.communications.gov.au/minister/mitch-fifield/news/government-provides-5g-security-guidance-australian-carriers.
14. Levy, "The future of telecoms in the UK."
15. Ibid.
16. David Kennedy, "The Facts on 5G: How 5G networks are being built in the real world," Ovum, July 26, 2019, 4, http://huaweihub.com.au/wp-content/uploads/2019/07/The-Facts-on-5G-Final-Report.pdf.
17. Pancevski, "U.S. Officials Say Huawei Can Covertly Access Telecom Networks."
18. Caitlin Yilek, "Germany has evidence Huawei worked with Chinese intelligence," *Washington Examiner*, January 29, 2019, https://www.washingtonexaminer.com/news/germany-has-evidence-huawei-worked-with-chinese-intelligence.
19. "Security in 5G RAN and core developments," Ericsson, November 29, 2019, https://www.ericsson.com/en/reports-and-papers/white-papers/security-in-5g-ran-and-core-deployments.
20. Government of the United Kingdom, National Cyber Security Centre, "NCSC advice on the use of equipment from high risk vendors in UK telecoms networks."
21. *National Intelligence Law of the People's Republic*, June 27, 2017, http://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.
22. Ibid.
23. Xi Jinping, "A Holistic View of National Security," in *Xi Jinping: The Governance of China* (Beijing: Foreign Language Press, 2014), 222.
24. Peter Mattis, "U.S. Responses to China's Foreign Influence Operations," testimony before the House Committee on Foreign Affairs, Subcommittee on Asia and the Pacific, March 21, 2018, https://docs.house.gov/meetings/FA/FA05/20180321/108056/HHRG-115-FA05-Wstate-MattisP-20180321.pdf.
25. Greg Levesque and Mark Stokes, "Blurred Lines: Military-Civil Fusion and the 'Going Out' of China's Defense Industry," Pointe Bello, December 2016, 21, https://static1.squarespace.com/static/569925bfe0327c837e2e9a94/t/593dad0320099e64e1ca92a5/1497214574912/062017_Pointe+Bello_Military+Civil+Fusion+Report.pdf.
26. "Share of Manufacturing Exports by Country," Manufacturing Institute, Updated October 2013, http://www.themanufacturinginstitute.org/Research/Facts-About-Manufacturing/Foreign-Trade-and-Investment/Share-of-Exports/Share-of-Exports.aspx.
27. Jonathan T. Ward, *China's Vision of Victory* (Atlas, 2019).
28. Ibid.
29. Robert Zoellick, "Whither China? From Membership to Responsibility," remarks to the National Committee on U.S.-China Relations, September 21, 2005, https://www.ncuscr.org/sites/default/files/migration/Zoellick_remarks_notes06_winter_spring.pdf.
30. Sean O'Connor, "SOE Megamergers Signal New Direction in China's Economic Policy," U.S.-China Economic and Security Review Commission, May 24, 2018, https://www.uscc.gov/sites/default/files/Research/SOE%20Megamergers.pdf
31. Michael Hirson, "State Capitalism and the Evolution of 'China, Inc.': Key Policy Issues for the United States," Testimony before the U.S.-China Economic and Security Commission on "China's Internal and External Challenges," February 7, 2019, https://www.uscc.gov/sites/default/files/Hirson_USCC%20Testimony_FINAL.pdf.
32. Keith Johnson and Ellias Groll, "The Improbable Rise of Huawei," *Foreign Policy*, April 3, 2019, https://foreignpolicy.com/2019/04/03/the-improbable-rise-of-huawei-5g-global-network-china/.
33. Jonathan Swan, David McCabe, Ina Fried, and Kim Hart, "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. See also leaked White House memorandum, "Secure 5G: The Eisenhower National Highway System for the Information Age," https://assets.documentcloud.org/documents/4361020/Secure-5g.pdf.
34. "Telecommunications equipment" encompasses Broadband Access, Carrier IP Telephony, Microwave, Mobile RAN, Optical, SP Router and CE Switch, and Wireless Packet Core. See Stefan Pongratz, "Key Takeaways – Worldwide Telecom Equipment Market 2018," Dell'Oro Group, March 4, 2019, https://www.delloro.com/telecom-equipment-market-2018-2/.
35. Strand Consult, "The real cost to rip and replace of Chinese equipment in telecom networks," October 2019, 12, https://d110erj175o600.cloudfront.net/wp-content/uploads/2019/10/Strand-Consult_The-real-cost-to-rip-and-replace-of-Chinese-equipment-in-telecom-networks-003-1.pdf.
36. "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," House Permanent Select Committee

on Intelligence, October 8, 2012, 13, https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf.
37. As cited in Larry Wortzel, "The Chinese Way of Asymmetric War," in Ilan Berman, ed., *The Logic of Irregular War: Asymmetry and America's Adversaries* (Lanham: Rowman & Littlefield, 2017), 13.
38. Lesley Wroughton and Gergely Szakacs, "Pompeo warns allies Huawei presence complicates partnership with U.S.," Reuters, February 10, 2019, https://www.reuters.com/article/us-usa-pompeo-hungary/pompeo-warns-allies-huawei-presence-complicates-partnership-with-u-s-idUSKCN1Q0007.
39. Ibid.
40. Latika Bourke, "Boris Johnson allows Huawei to build parts of UK's 5G network," *Sydney Morning Herald*, January 29, 2020, https://www.smh.com.au/world/europe/boris-johnson-allows-huawei-to-build-parts-of-uk-s-5g-network-20200129-p53vlr.html.
41. U.S. Department of Defense, "Base Structure Report – Fiscal Year 2018 Baseline: A Summary of the Real Property Inventory Data," n.d., https://www.acq.osd.mil/eie/Downloads/BSI/Base%20Structure%20Report%20FY18.pdf.
42. U.S. Department of Defense, Joint Staff, "Joint Mobilization Planning," October 23, 2018, I-2, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp4_05.pdf.
43. The full list is: legal authorities, funding, environment, manpower, material and equipment, transportation, facilities, industrial base, training base, joint health services, communications, and host-nation support. Ibid, xiii-xiv.
44. Ibidem, xiv.
45. Ibidem; See also Larry Wortzel, "The Chinese Way of (Cyber) War," *AFPC Defense Dossier* iss. 4, August 2012, 4, https://www.afpc.org/uploads/documents/august2012.pdf.
46. Ibid, and author's private conversations with China experts.
47. U.S. Department of Defense, "Joint Communications System," Joint Publication 6-0, October 4, 2019, II-3, https://fas.org/irp/doddir/dod/jp6_0.pdf.
48. Mike Burgess, speech to the ASPI National Security Dinner, Canberra, Australia, October 29, 2018, https://www.asd.gov.au/publications/speech-ASPI-national-security-dinner.
49. Griff Witte and Luisa Beck, "When hunger for fast Internet collides with U.S. concerns about Chinese spying," *Washington Post*, April 23, 2019, https://www.washingtonpost.com/world/europe/when-hunger-for-fast-internet-collides-with-us-concerns-about-chinese-spying/2019/04/22/20bf17f6-5d29-11e9-98d4-844088d135f2_story.html.
50. Office of Senator Ted Cruz, "Sen. Cruz: Huawei Decision Will Endanger National Security of Britain, United States, and Our Allies, for Generations to Come," January 28, 2020, https://www.cruz.senate.gov/?p=press_release&id=4898.
51. Lake, "The U.S.-U.K. Alliance Could Soon Get Much Weaker."
52. Richard Tanter, "The 'Joint Facilities' revisited – Desmond Ball, democratic debate on security, and the human interest," Nautilus Institute for Security and Sustainability, December 12, 2012, 31, http://nautilus.org/wp-content/uploads/2012/12/The-_Joint-Facilities_-revisited-1000-8-December-2012-2.pdf.
53. U.S. Department of Justice, "Attorney General China Initiative Fact Sheet," July 12, 2019, https://www.justice.gov/opa/press-release/file/1179321/download.
54. U.S. Department of Commerce, Bureau of Industry & Security, "Entity List Additions of Huawei and 69 non-US Affiliates in Effect," May 16, 2019, https://www.bis.doc.gov/index.php/documents/regulations-docs/2395-effective-date-of-huawei-and-affiliates-entity-list-rule/file.
55. Stacie Hoffmann, Samantha Bradshaw, and Emily Taylor, "Networks and Geopolitics: How great power rivalries infected 5G," Oxford Information Labs, August 22, 2019, 4, https://oxil.uk/publications/geopolitics-of-5g/.
56. "Westlessness: Munich Security Report 2020," Munich Security Conference, n.d., 6, https://securityconference.org/assets/user_upload/MunichSecurityReport2020.pdf.
57. Kadhim Shubber and Kiran Stacey, "Barr urges US stakes in Nokia and Ericsson to stall Huawei," *Financial Times*, February 6, 2020, https://www.ft.com/content/1aa61918-48fc-11ea-aeb3-955839e06441.
58. "Secure 5G: The Eisenhower National Highway System for the Information Age."
59. Shayerah Ilias Akhtar and Marian L. Lawson, "BUILD Act: Frequently Asked Questions About the New U.S. International Development Finance Corporation," Congressional Research Service, January 15, 2019, 4, https://fas.org/sgp/crs/misc/R45461.pdf.
60. Office of Senator Tom Cotton, "Cotton Introduces Bill Banning Intelligence Sharing With Countries Using Huawei," January 8, 2020, https://www.cotton.senate.gov/?p=press_release&id=1288.
61. Office of Senator Ben Sasse, "Sasse Statement on United Kingodm's Huawei Decision," January 28, 2020, https://www.sasse.senate.gov/public/index.

cfm/2020/1/sasse-statement-on-united-kingdom-s-huawei-decision.
62. Robert Kagan, Of Paradise and Power (New York: Vintage Books, 2004), 3.
63. Bob Davis and Drew FitzGerald, "U.S. Pushing Effort to Develop 5G Alternative to Huawei," *Wall Street Journal*, February 4, 2020, https://www.wsj.com/articles/u-s-pushing-effort-to-develop-5g-alternative-to-huawei-11580831592?redirect=amp#click=https://t.co/tSyVtQ0ccT.
64. Yawen Chen and Se Young Lee, "China slams U.S. blacklisting of Huawei as trade tensions rise," Reuters, May 16, 2019, https://www.reuters.com/article/us-usa-trade-china-huawei/china-slams-u-s-blacklisting-of-huawei-as-trade-tensions-rise-idUSKCN1SM0NR.
65. Guy Faulconbridge and Paul Sandle, "UK's Johnson says Huawei critics need to suggest alternatives," Reuters, January 14, 2020, https://www.reuters.com/article/us-britain-usa-huawei/uks-johnson-says-huawei-critics-need-to-suggest-alternatives-idUSKBN1ZD0UY.
66. William Booth, Jeanne Whalen, and Ellen Nakashima, "Britain, resisting U.S. pressure, to allow some Huawei equipment in 5G networks," *Washington Post*, January 28, 2020, https://www.washingtonpost.com/world/europe/britain-resisting-us-pressure-to-allow-some-huawei-equipment-in-5g-networks/2020/01/28/52e708b4-4145-11ea-99c7-1dfd4241a2fe_story.html.
67. "Attorney General China Initiative Fact Sheet."
68. Jay Bellamy, "The Zimmerman Telegram," *Prologue Magazine* 48, no. 4 (Winter 2016), https://www.archives.gov/publications/prologue/2016/winter/zimmermann-telegram.
69. U.S. Central Intelligence Agency, "The Enigma of Alan Turing," April 10, 2015, https://www.cia.gov/news-information/featured-story-archive/2015-featured-story-archive/the-enigma-of-alan-turing.html.
70. Phillip Knightley, "Gervase Cowell: British spymaster behind Oleg Penkovsky, whose disclosures sparked the Cuban missile crisis," *Guardian* (London), May 15, 2000, https://www.theguardian.com/news/2000/may/16/guardianobituaries.
71. James Cox, "Canada and the Five Eyes Intelligence Community," Canadian Defense & Foreign Affairs Institute, December 2012, 6, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.357.5576&rep=rep1&type=pdf; See also Jeffrey T. Richelson, *The U.S. Intelligence Community* (Boulder: Westview Press, 1999), 293. Additionally, see Jeffrey T. Richelson and Desmond Ball, *The Ties That Bind: Intelligence Cooperation between the UKUSA Countries – the United Kingdom, the United States of America, Canada, Australia, and New Zealand* (Cambridge: Unwin Hyman, 1990), 174.

AMERICAN FOREIGN POLICY COUNCIL

DEFENSE TECHNOLOGY PROGRAM BRIEF

March 2020 | No. 19

ABOUT THE DEFENSE TECHNOLOGY PROGRAM

A revolution is taking place in the nature of warfare. The proliferation of ballistic missiles and weapons of mass destruction has given rogue states and terrorist groups unprecedented access to potentially devastating capabilities, while space and cyberspace have emerged as distinct new arenas of strategic competition. The American Foreign Policy Council's (AFPC) work in these areas is aimed at helping U.S. offcials understand and respond to this new, and increasingly complex, threat environment.

For more information about the program, please contact Richard Harrison, Director of Operations and Defense Technology Programs at Harrison@afpc.org.

ABOUT AFPC

For close to four decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies. AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

AFPC MISSION STATEMENT

The American Foreign Policy Council seeks to advance the security and prosperity of the United States by:

- providing primary source information, as well as policy options, to persons and organizations who make or influence the national security and foreign policies of the United States;
- arranging meetings and facilitating dialogue between American Statesmen and their counterparts in other countries; and
- fostering the acceptance and development of representative institutions and free market economies throughout the world in a manner consistent with the Constitution, the national interest, and the values of the United States.

AMERICAN FOREIGN POLICY COUNCIL
509 C Street NE, Washington, D.C. 20002 | Telephone: 202.543.1006 | Fax: 202.543.1007 | www.afpc.org