Are we destined for a forever-war between two technological giants, whose battleground will be network control, rather than geography?

–DAVID E. SANGER

Managing the Fifth Generation: America, China, and the Struggle for Technological Dominance

David E. Sanger[1]

In February 2019, Secretary of State Mike Pompeo took a tour through Europe, issuing a dire warning to foreign officials every stop along his route.

In visits to Hungary and Poland, and later to Germany and Britain, he warned American allies that they faced a stark choice: They could reject the efforts of Chinese firms to build the next big thing in telecommunications networks (called 5G for "fifth generation") inside their borders and stay firmly within the American defense camp. Or they could take the Chinese technology and low-cost financing that comes with it—and, he threatened, lose access to sensitive American intelligence and perhaps American military bases.[2]

For many of the countries he visited, Pompeo's ultimatum seemed shocking: officials had been treating the building of new cellular networks largely as a procurement decision. While they had heard warnings that installing Chinese-made equipment in their networks could give Beijing a foothold to install "backdoors" that could allow intelligence agencies to read or divert digital traffic, the security issues had been considered background noise, not a festering national security crisis. Now, suddenly, the U.S. was presenting 5G as a loyalty test—a choice between staying in the Western alliance or placing at least one foot in the Chinese camp. The Trump administration was insisting that nations declare their allegiances.

Pompeo's demands were followed by quiet visits from American intelligence officials armed with a slide deck laying out the specific dangers that Washington was worried about. They described the 5G hardware as the leading edge of a broader Chinese effort to gain influence everywhere from Latin America to Africa to the former Soviet states—including some of the newer members of NATO. Those efforts, they warned, ranged from overt to covert: subsidizing universities and libraries (as the United States did in the 1950s and 1960s), using the Belt and Road Initiative to create trade dependencies, and providing "donations" to politicians. But American officials contended the 5G initiative was the most insidious. Their argument boiled down to this: if Chinese firms—led by Huawei, China's national telecommunications champion and the world's second-largest cell phone maker after it edged ahead of Apple in 2018—were allowed to install the hardware and software of the next-generation networks, the Chinese government would gradually amass an unprecedented amount of control over a vast array of infrastructure. "It's not just the communications,'' one of the officials who conducted those classified briefings warned. "It would be the gas pipelines, the water supplies, the factory floors, the 'smart cities' of the future." Under Chinese law, he argued, Huawei and other Chinese firms are required to comply with any request from Chinese intelligence services to create a "backdoor" into another nation's communications networks. This would allow them to spy or—more ominously—use that power in time of conflict to turn off the networks of their clients.

It was a dire picture—but an entirely speculative one, as the Europeans and others argued in response. So far, there was scant evidence that China had used Huawei for nefarious purposes. So by early summer 2019, the battle

to keep Chinese-made technologies out of allied 5G networks was not going well for the United States. Much of Europe was hedging its bets, not willing to give up the subsidized, low bids that Chinese manufacturers were offering. Other countries, including close U.S. military allies such as Bahrain, home of the Fifth Fleet, were either planning to incorporate Huawei into at least part of their network or refraining from making a public decision. The Philippines, once a centerpiece of American air and naval power in the Pacific, outright balked, announcing it would go with the Chinese system. India—one of the largest telecommunications networks—was sending mixed signals. As of July 2019, only Australia had formally announced that it would ban Huawei components in its 5G networks—though New Zealand and Japan were moving that way. By the fall, no new countries had announced a ban. Instead, Huawei steadily picked up more 5G contracts around the globe, announcing sixty contracts by October—just over half of which were with carriers in Europe. (However, most were for cell towers and radio components of the networks, rather than the core switching systems that are of particular concern to military and intelligence officials.)

The argument between Washington and its allies over 5G had run headlong into the always-difficult balancing act inherent in simultaneously treating China as an economic partner, an intelligence adversary, an intellectual-property thief, and a potential military foe. But the 5G problem went deeper. At a moment when America's influence around the globe appears waning, allies were essentially looking into the crystal ball and trying to discern which of the world's two largest economies would be more critical to their future. While they acknowledged the risks of putting Chinese firms at the core of their national networks, they were weighing that risk against the potential for job creation and the fear of Chinese retaliation if they sided with Washington. ("We sell five million cars to China every year," a senior German official said amid this debate. "What happens to that the year after we ban Huawei?")

Even inside the Trump administration, there was no unanimity on the issue. While a cluster of powerful China hawks, led by Pompeo, made the case that banning Huawei was non-negotiable, Treasury Secretary Steve Mnuchin led a camp arguing that, just as the trade relationship could be managed, so could Huawei's presence in Western networks. President Trump vacillated. For much of the spring of 2019, he described 5G networks as an issue of national security and went so far as to impose a ban on exporting sensitive American technology to Chinese manufacturers. (Although U.S. companies promptly discovered loopholes in the ban that permitted them to sell some products.[3]) Then, in June, he partially lifted the ban, saying it was a trade issue. One of his own senior advisers conceded that he had no idea whether the president might trade away America's long-range security concerns for a trade deal that included a Chinese purchase of billions of dollars in American soybeans.

The result, not surprisingly, has been confusion among American firms and American allies. And the absence of a clear administration strategy has contributed to a fear that the United States is falling behind not only in 5G but in the technologies it will enable, from artificial intelligence to advanced robotics to autonomous vehicles. All are considered the next technological battleground with a rising China.

A Core Debate: 5G and the Future of the Internet

Beyond the specific debate about whether to let Chinese firms build the telecommunications infrastructure of the Western and Asian allies of the United States lies competing visions of what the internet will look like in a few years—and how China's central role in 5G technology may shape the internet's future.

Those in one camp see the 5G networks inevitably leading to the creation of a new Berlin Wall—elements of which are already partly in place. While the analogy draws from the Cold War, this wall would be virtual, not physical. It would stretch around the globe and essentially divide the world into two internets. On one side

would be the familiar anarchy of the Western version of the internet, awash in constant commerce, largely free speech, and the inevitable abuses and chaos that come with a vast, unregulated space. On the other would lie a Chinese-controlled "authoritarianet." This second internet, in Pompeo's words, would be "based on the principles of an authoritarian, Communist regime." Inside the authoritarianet, content is controlled by the government, facial recognition is employed to tighten the ruling party's control, and artificial intelligence is deployed to sniff out dissent. And its traffic may pass over Chinese-provided undersea cables, to which the United States and its allies would, presumably, have limited access. It would, in essence, replicate elements of what China has created at home: an increasingly self-reliant network that uses Chinese search engines that filter inquiries for political correctness, Chinese social networks, and Chinese mobile payment systems. The appeal to a rising class of authoritarian leaders, from Hungary to Bolivia, is obvious. For insecure leaders looking for a bargain, it will all come in a subsidized surveillance-and-control package.

The alternative to this back-to-the-Cold-War view belongs to techno-realists. They note that China's control over a substantial portion of the world's networks is inevitable, just as China's rise is beyond America's control. But in their view, the two-internet system is a flawed concept. While China has been more successful than most could have imagined at walling off its own population from outside influences, stretching that wall beyond China's shores would interfere with Beijing's own ability to trade around the world. In this view, dividing the world into two internets defeats the grand political achievement of the digital age: the benefits of tying together billions of global citizens.

So in this view, even if there are "sovereign" corners of the internet, the world will still have to exchange data among them at blazing speeds. And that means your data will traverse free and authoritarian internets, and secure and less secure environments. As Sue Gordon, then deputy director of national intelligence, put it bluntly: "You have to presume a dirty network," and adjust accordingly. "We are going to have to figure out a way in a 5G world that we're able to manage the risks in a diverse network that includes technology that we can't trust."[4] Her meaning was clear: the nation that dominated the world of communications since Alexander Graham Bell, that built the internet and benefited from the fact that the most critical connections flowed through American territory, must accept the reality that we can no longer control our digital environment.

These two visions likely oversimplify how the next decade will unfold. If there is a lesson from the first three decades of the internet, it is that cyberspace is a messy place. It defies planning. That is especially true as the 5G networks are rolled out around the world. And there is no assurance that the American approach to developing these networks will prevail.

The Defense Innovation Board made a convincing case in 2019 that the United States cannot depend on stumbling its way to a lead merely by assuming that the wizards of Silicon Valley will stay ahead. "The country that owns 5G will own many of these [critical] innovations and set the standards for the rest of the world," the board concluded. "That country is currently not likely to be the United States."[5]

So it is no surprise that 5G has already become a political battlefield. Its deployment over the next few years has struck at one of America's existential fears: that once the West's digital communications are dominated by Chinese firms, Beijing will have more than just an innovation advantage; it will have the power to divert internet traffic at will or, with the flick of a switch, turn off the communications spine of the United States.

Are we destined for a forever-war between two technological giants, whose battleground will be network control, rather than geography? Or is there room for accommodation of a rising technological power—even in the West's networks—and the potential to craft rules of the road that might exempt the most critical communications networks from the daily, low-level cyber conflicts that major states are fighting every day?

How We Got Here

When the world embraced 3G and 4G technologies in the first decades of the twenty-first century, it was joining a system that was essentially designed, built, and controlled by the West. The technology was dominated by American makers: the wireless systems were heavily dependent on switching systems built by Cisco and wireless radio technology designed by Qualcomm, among others. Western allies and Japan invested heavily in deploying their networks first, and the Chinese were usually a few years behind. That meant the West was able to define the technical standards and promote their versions of devices and regulations, granting them a significant competitive advantage.

But the Chinese understood quickly that 5G was their moment to catch up—a revolution in manufacturing that would also create new opportunities in artificial intelligence, autonomous vehicles, and other technologies that are key components of their "Made-in-China" goals. They invested heavily in research and development, licensing some of the technology from American makers (though not always paying for it). Huawei, which began as a domestic telecommunications firm founded by the famously reticent former People's Liberation Army engineer Ren Zhengfei, became the symbol of China's global ambitions. By mid-2018 it held an estimated 28 percent share of the world's telecommunications equipment market.[6] And it dominated markets in Southeast Asia, Latin America, and Africa. Now it has begun using that market dominance to sign 5G contracts with dozens of countries worldwide, aided by low-cost financing provided by the Chinese government.[7] And it has begun to push back at American and European dominance of the key leadership roles on the international bodies responsible for setting the standards for 5G communications.[8] Today, roughly 10 percent of patents necessary for 5G are held by Chinese companies, including Huawei—though the leading technology, and the ability to integrate it into a network, still belongs to the U.S. and a smattering of European competitors.[9]

Senator Mark Warner, the ranking Democrat on the Senate Intelligence Committee and a former telecommunications executive, has described the change to his colleagues this way: "We are accustomed to a world in which America invented the internet, set the standards, and manufactured all the key parts. And that world is going away. It's not coming back."

Yet few in the United States saw this Chinese initiative coming. Huawei was founded in 1987, but it hardly seemed a threat for its first two decades, as it mostly focused on consolidating its market share in China and expanding to developing countries. But by the mid-2000s, the company's successes set off at least a few alarm bells in the ranks of the U.S. government. And by 2012, Huawei was frozen out of U.S. government supply chains following a congressional report warning that installing Huawei gear in the U.S. would be tantamount to letting the Chinese Communist Party wire up the country. While Huawei has always maintained that it is privately owned by its employees, public reporting on the company has revealed a very close relationship between Huawei and the Chinese government. It thrives largely because of a tight web of state-backed financing, government clientele, and a talent pool with overlap in the military and intelligence services. Yet the U.S. has never been able to prove—at least in the unclassified world—that Huawei is an instrument of the Communist Party, or of the People's Liberation Army, in which Zhengfei served as a young man. Even Operation Shotgiant, mounted by the National Security Agency (NSA) to reveal Huawei's secret connections, turned up little. And when the operation was exposed by Edward J. Snowden, the former NSA contractor now in exile in Russia, it merely convinced the Chinese that the United States was doing to China exactly what American officials charged Huawei would do to the United States.[10]

The absence of a smoking gun connecting Huawei to any direct spying has not halted American officials from warning of a danger to the West. Instead, they start with China's two-year-old national security laws, noting that Huawei officials are bound, by Chinese law, to give Chinese intelligence agencies any access they demand to networks where Huawei operates.[11] That fear is one reason a handful of acquisitions, mergers, and other deals between Huawei and U.S. companies have been blocked.

Finally, in 2018—with the advent of the first 5G networks now imminent—Congress formally banned much of Huawei gear from government use. And in December 2018, the chief financial officer of Huawei, Meng Wanzhou—Zhengfei's daughter—was arrested on charges of violating sanctions against Iran by shipping it Huawei technology. The Chinese cried foul, arguing that Meng was being held in Canada merely for leverage by President Trump. And Trump gave credence to the charge by suggesting she might be let go if there was a good enough trade deal—thus mixing trade, national security, and the integrity of the American justice system.

Promises and Reality

While dozens—if not hundreds—of recently published articles talk about the need for the U.S. to "win the race to 5G," the conversation rarely focuses on what 5G actually is, what it promises, or what a technological lead might look like. Many are tempted to view 5G as simply a faster version of 4G. It is true that speeds achievable with 5G technology dwarf 4G many times over—a Netflix movie that might take several minutes to download on an existing 4G cellular network will be downloaded in a flash. And latency—the lag time between a command or inquiry and the response—is greatly reduced, a necessity for autonomous vehicles, which have to decide in a split second whether to take an exit ramp. The networks also have vastly increased capacity, meaning they are not overwhelmed by huge amounts of data flowing simultaneously.

Yet the real promise of 5G lies not in its speed, but the future applications that speed allows—and the ability to exploit those for new technologies. (This is hardly a new phenomenon: Uber wouldn't have been possible without real-time mapping.) Previous generations of network connectivity were generally designed for consumers: the traffic was primarily calls and data. 5G is different: it is designed for machines talking to machines and will enable connections between the billions of sensors, robots, autonomous vehicles, and other devices that will continuously feed one another vast amounts of data in the coming years. It will continuously swap information through the cloud—and will update more frequently and autonomously than previous generations. The implications for industry, national security, and human welfare are clear and revolutionary in scope.

But the question of whether or not the U.S. is in a good position to collect on these benefits of 5G is hotly debated—and has been the subject of a number of meetings between key leaders in Congress, the executive branch, and private wireless carriers. Many of these are asking whether—Huawei aside—the U.S. is actually on track to deploy its networks in a competitive manner.

One of the biggest problems is that there is a disagreement over which segment of the electromagnetic spectrum should be used for 5G. China and a number of other countries seem to have settled on spectrum in the "sub-6" region—that is, below 6GHz. In the U.S., however, much of the key sub-6 spectrum is reserved for defense use, leaving industry to develop 5G technologies that will operate at a much higher band—between 24GHz and about 300GHz, so-called "mmWave." While faster, the higher frequencies can be more difficult to manage and don't cover as much area as the lower- to mid-range sub-6 spectrum. As a result, it will be more effective in cities and harder to deploy in already-underserved rural areas.

Most worrisome is the question of which spectrum will dominate globally: if the rest of the world mostly follows China into the sub-6 spectrum, the U.S. may have a high-speed network—but one with significant interoperability issues with other countries' networks. It's a problem that has a number of experts—from the Defense Innovation Board[12] to an FCC Commissioner[13]—highly concerned. And no one even knows for sure whether the great promise of this new architecture—that its blinding speeds for cellular communications will give birth to autonomous vehicles constantly communicating with the cloud, revolutionize manufacturing, and bring vast streams of data for farmers in the most distant, poorest nations—will yield the promised benefits. Even as billions of dollars are spent to construct it, 5G networks have become the digital Field of Dreams: build it, we are told, and they will come.[14]

Is It Too Late? Managing China, and Managing the 5G Future

If Russia has spent the past decade focused on disruption of the West, China, by contrast, is focused on its goal of dominating the technologies that make the world work. The way to get there, China's leadership has been convinced, is not with nukes or the world's largest navy, but with control of the world's servers, software, and undersea cables.

The United States woke up too late to the 5G challenge and to many of the issues associated with it. The fear of falling behind—on 5G and the advances it will help spur in artificial intelligence, robotics, autonomous vehicles, and weapons, among others—is now pervasive in Washington. But all is not lost, just as it was not lost in 1990, when American politicians feared that the U.S. was on the way to becoming a "techno-colony" of Japan.

So what would be the elements of a national 5G strategy? Here are some suggestions.

1) Threatening allies doesn't work. Devising a credible alternative might.

There are lessons in the apparent failure of Pompeo's pressure tactics to lock Huawei out of American allies' networks. The first is that, unsurprisingly, other governments don't like to be threatened, and many see resisting Washington on this point as a way of pushing back on an "America First" agenda. But the second is that NATO allies, and allies in Asia, seem more likely to respond to a positive incentive: an argument that they can profit by building a Western supply chain with the reach, effectiveness, and affordability of Huawei.

There are many ideas floating around about how to do this. One is to combine Nokia and Ericsson, two European suppliers that do not enjoy Huawei's market reach. A second is to combine them with an American partner. But whatever the corporate configuration, it is clear that the United States and its partners need a Western "champion" of their own: one that creates jobs, innovates, and may be the beneficiary of some Western industrial policy, much as Huawei benefits from Chinese industrial policy. Clearly the United States already recognizes the importance of keeping home-grown technology in American hands, because it has used CFIUS—the Committee on Foreign Investment in the United States—to prevent the foreign takeover of Qualcomm and other key technology providers.

Another critical question now is whether the U.S. is ready to go further than simply protecting companies from takeover to assure that the country's own technological base is not hollowed out. For decades, such "industrial policy" was a political issue that divided Democrats and Republicans. While the Manhattan Project is often cited as a prime example of government-sponsored innovation, it was driven by wartime necessity and the fear that Nazi Germany had both the talent to develop a nuclear bomb and the means to deliver it. Later efforts never quite matched that success. The Strategic Computing Initiative, designed by DARPA to take on Japan, never lived up to its hype. The Microelectronics and Computer Technology Corporation, a consortium of major American companies, was not responsible for the major breakthroughs that Americans associate today with the mobile-computing revolution. When a small Obama-era energy program failed to produce many results, there were objections in Congress to "picking winners." That may help explain why the U.S. underreacted at first to China's announcement of dedicated funding to a range of advanced technologies, many focused on artificial intelligence, alternative energy vehicles, and 5G.

Of course, the United States has never been as hands-off as it advertises. DARPA has long financed promising defense technologies. In-Q-Tel has long served as a small-scale venture capitalist for the intelligence community. Defense Innovation Unit (formerly Defense Innovation Unit-Experimental, or DIUx) has been particularly successful at finding commercial firms and products that could be useful for warfighters—and it has invested in a few. But all these have survived by flying under the radar. Their work has not been tied together as part of a

national strategy. The official Trump administration position is that none is needed—the competitive genius of Silicon Valley will always outperform China's step-by-step, incremental innovation. Maybe it will, but the early evidence in 5G, machine learning, AI, and autonomous vehicles suggest that scale and organization count.

The U.S. has to choose—it can pursue both paths, as long as government leaders understand that failure is a routine part of the process. So far, there is little evidence of a broader strategy.

2) Learn to live in a world of "dirty networks."

No one knows what the internet will look like in a decade. Yet even if the United States is wildly successful—if it keeps Huawei and other Chinese firms out of the core of its 5G networks, if it builds a Western "champion" of its own to compete—that won't be enough. China didn't need 5G to steal the plans for the F-35. It didn't need it to steal the most sensitive personal information of twenty-two million Americans—including our country's national security elite, military, top academics, and contractors—which was contained in security clearance files at the Office of Personnel Management.

Even if America learns to lock down its domestically held data, in a world of global communications and trade, sensitive American data will be running through networks dominated by China and other nations that also seek our intellectual property. In short, we will need to learn to live with dirty networks. Just as we don't get to choose other nations' political systems, we don't get to choose their communications infrastructure either.

What does that mean in practical terms? It requires developing a strategy for keeping the most sensitive defense data inside national networks—with better technologies for walling them off—and developing far more reliable encryption technologies for even routine communications going around the world. Such a policy, however, would require the administration to revise its views on encryption. After the Snowden revelations in 2013, a commission appointed by President Obama and composed of intelligence officials, industry executives, and academics called for the United States to greatly strengthen encryption—both to give assurance to foreigners that the NSA has not undermined the safety of American products and to assure Americans that their own data is safe. The commission insisted that the U.S. "not in any way subvert, undermine, weaken, or make vulnerable generally available commercial software" and that it "increase the use of encryption and urge U.S. companies to do so, in order to better protect data in transit, at rest, in the cloud, and in other storage."[15]

President Obama never acted on this recommendation. Under President Trump, Attorney General William Barr has argued that law enforcement agencies need to always maintain a legal "backdoor" to any encrypted system. He did not explain, however, how to manage the risk that any skilled foreign power—starting with China—would leap through that backdoor.

Barr's strategy is at odds with other parts of the administration. The Defense Innovation Board has already publicly recommended transitioning Defense Department networks to a "zero-trust" model that deemphasizes perimeter-based security in favor of encryption and resiliency.[16] Securing future networks—and the data moving through them—will increasingly require internal safeguards and the ability to prevent unauthorized entities from spreading from one system into another.

3) Exploiting national security issues for trade concessions is bound to backfire.

When President Trump hinted that he might intervene in the criminal case of Huawei's chief financial officer, Meng Wanzhou, if it would help him win trade concessions from China, it fed into the Communist Party's narrative that Meng's arrest was a political move designed to pressure Huawei. When he issued an export ban of sensitive U.S. technology to Huawei and then walked it back, he undercut not only his iterated rationale for having blocked the technology in the first place but turned national security into a pawn in the large trade game.

As former chairman of the Federal Communications Commission Tom Wheeler wrote in July 2019, "The Trump administration's focus on Huawei equipment is not a cybersecurity strategy, and by melding trade policy with cybersecurity, damages each."[17]

The division here should not be difficult. Trade deals are negotiable; national security considerations are, by and large, non-negotiable. Every presidential administration violates that precept to some degree. But President Trump opens himself—and the country—to a new set of dangers when he hints that Huawei's troubles might end in return for trade concessions. And the Chinese government is already exploiting that difference. It believes, perhaps rightly, that it can solve its long-term competitive issues by buying off the Trump administration. If so, we are in new territory.

4) Standards-setting and supply chains are boring. And they matter.

It is easy for national security officials to map China's expanding presence in the South China Sea: satellites record every newly created island, measure every landing strip, and count airplanes and munitions bunkers. But only recently did government officials begin to appreciate how Chinese engineers were flooding the zone of standards-setting meetings, looking to set the parameters of how internet-of-things (IoT) devices will communicate with 5G networks.

This is a new phenomenon: in the past, China rolled its networks out after the United States and Europe paved the way, meaning standards were set by the time they engaged with the technology. Chinese leaders learned from the mistake. In 5G, they expect China to have a major voice from the start. They are churning out patents, hoping that numbers alone will triumph over true breakthroughs. Their interest is understandable: China already makes a vast number of IoT devices. But the country that sets the standards has a clear advantage in developing intelligence strategies as well. For years, Washington benefited enormously from the fact that so many internet communications flowed through U.S. territory. Beijing is now moving to tilt the playing field in the other direction.

Maintaining U.S. technological leadership in global standards-setting won't be easy, and it will require the U.S. government to display both leadership and flexibility. But it is well worth the relatively small cost. The most immediate action should be to recommit to assertive diplomacy at the standards-setting bodies: that is, moving U.S. and allied representatives into key leadership positions and advocating strongly for U.S.-patented technologies to be adopted as standards.

Playing a big role in setting standards is only the first step; manufacturing the parts that fit those standards comes next. Here, the answer seems straightforward: building Western systems on a foundation of untrusted parts defeats the purpose of the exercise. Just as the U.S. has trusted suppliers for the F-35, it cannot depend on components, or software, of uncertain origin.

The battle over 5G is only a small part of the broader effort to manage the rise of China. But it has become both technologically and symbolically important. It gets to the heart of who will control the systems that make our societies tick. And it will be key to the perception of who holds the levers of global power. We have one last shot at getting it right.

David E. Sanger is a national security correspondent and a senior writer at *The New York Times.* In a 37-year reporting career, he has been on three *Times* teams that have won Pulitzer Prizes, most recently in 2017 for international reporting on Russia's cyber activities surrounding the 2016 presidential election. His newest book, *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*, examines the emergence of cyberconflict as the primary way large and small states are competing and undercutting each other, changing the nature of global power. He is also the author of two *Times* best sellers on foreign policy and national security: *The Inheritance: The World Obama Confronts and the Challenges to American Power,* published in 2009, and *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, published in 2012. Mr. Sanger has served as Tokyo bureau chief, Washington economic correspondent, White House correspondent during the Clinton and Bush administrations, and chief Washington correspondent. He was a leading member of the team that investigated the causes of the Challenger disaster in 1986, which was awarded a Pulitzer in national reporting the following year. A second Pulitzer, in 1999, was awarded to a team that investigated the struggles within the Clinton administration over controlling technology exports to China. A 1982 graduate of Harvard College, Mr. Sanger co-teaches "Central Challenges in American National Security, Strategy and the Press" with Graham T. Allison Jr. at the Kennedy School of Government. He is a member of the Aspen Strategy Group.

[1] My thanks to Mary K. Brooks, who conducted much of the research and reporting on the chapters dealing with 5G technology and the competition with China for the revised edition of *The Perfect Weapon: War, Sabotage and Fear in the Cyber Age*. Her reporting and editing were critical for this paper.

[2] Julian E. Barnes and Adam Satariano, "U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist," *New York Times,* March 17, 2019, https://www.nytimes.com/2019/03/17/us/politics/huawei-ban.html.

[3] Paul Mozur and Cecilia Kang, "U.S. Tech Companies Sidestep a Trump Ban, to Keep Selling to Huawei," *New York Times,* June 25, 2019, https://www.nytimes.com/2019/06/25/technology/huawei-trump-ban-technology.html.

[4] Zak Doffman, "Huawei May Have Claimed 5G Victory Over The U.S. But Is Now In A Street Fight," *Forbes*, April 5, 2019, https://www.forbes.com/sites/zakdoffman/2019/04/05/spy-games-huawei-claims-5g-victory-over-the-u-s-but-is-now-in-a-street-fight/#14ccc7ca4639.

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

[6] Milo Medin and Gilman Louie, *The 5G Ecosystem: Risks & Opportunities for DoD*, Defense Innovation Board, April 3, 2019, https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

[7] "Huawei Obtains 46 Commercial 5G Contracts in 30 Countries," XinhuaNet, June 6, 2019, http://www.xinhuanet.com/english/2019-06/06/c_138122365.htm.

[8] Todd Shields and Alyza Sebenius, "Huawei's Clout Is So Strong It's Helping Shape Global 5G Rules," *Bloomberg*, February 1, 2019, https://www.bloomberg.com/news/articles/2019-02-01/huawei-s-clout-is-so-strong-it-s-helping-shape-global-5g-rules.

[9] Raymond Zhong, "China's Huawei Is at Center of Fight Over 5G's Future," *New York Times*, March 7, 2018, https://www.nytimes.com/2018/03/07/technology/china-huawei-5g-standards.html.

[10] David E. Sanger and Nicole Perlroth, "N.S.A. Breached Chinese Servers Seen as Security Threat," *New York Times*, March 22, 2014, https://www.nytimes.com/2014/03/23/world/asia/nsa-breached-chinese-servers-seen-as-spy-peril.html.

[11] Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," *Lawfare*, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

[12] Milo Medin and Gilman Louie, *The 5G Ecosystem: Risks & Opportunities for DoD,* Defense Innovation Board, April 3, 2019, https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

[13] Jessica Rosenworcel, "Choosing the Wrong Lane in the Race to 5G," *Wired*, June 10, 2019, https://www.wired.com/story/choosing-the-wrong-lane-in-the-race-to-5g/.

[14] See *Secure 5G: The Eisenhower National Highway System for the Information Age*, as published in "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.

[15] Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire, *Liberty and Security in a Changing World,* Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, December 12, 2013, https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[16] Milo Medin and Gilman Louie, *The 5G Ecosystem: Risks & Opportunities for DoD*, Defense Innovation Board, April 3, 2019, https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

[17] Tom Wheeler, "5G in Five (Not So) Easy Pieces," Brookings, July 9, 2019, https://www.brookings.edu/research/5g-in-five-not-so-easy-pieces/.