CHAPTER 51

The Assault on Huawei

"I call it the spyway," President Trump explained to the hosts of *Fox & Friends*, one of his favorite TV programs, when asked about Huawei. "We don't want their equipment in the United States because they spy on us.... They know everything." It was hardly a revelation that tech infrastructure could be used to pilfer confidential information. After former National Security Agency emplo yee Edward Snowden defected to Russia in 2013 while releasing many of the agency's most closely held secrets, news of American cyber sleuths' capabilities were regularly discussed in the world's newspapers. China's impressive hacking capabilities were also well known after a string of high-profile breaches of ostensibly secret U.S. government data.

Within the Pentagon and the NSC, Huawei was seen less as an espionage challenge—though U.S. off icials had little doubt the company would support Chinese spycraft—than as the first battle in a long struggle for technological dominance. Matt Turpin, a Pentagon official who'd worked on the military's new offset strategy, saw Huawei as symptomatic of a broader problem in the U.S. tech industry: Chinese firms "were effectively inside the system with the United States," given that they designed chips with U.S. software, produced them using U.S. machinery, and often plugged them into devices built for American consumers. Given this, it was impossible "for the United States to 'out-innovate' China and then deny them the fruits of that innovation." Huawei and other Chinese firms were assuming central roles in tech subsectors that the U.S. thought it needed to dominate to retain a technological advantage over China, militarily and strategically. "Huawei became really a proxy for everything we had done wrong with our tech competition with China," another senior Trump administration official put it.

Concern about Huawei wasn't confined to the Trump administration or the United States. Australia had banned Huawei from 5G networks after its security services concluded the risk simply couldn't be mitigated, even if Huawei turned over access to all its software source code and hardware. Australian prime minister Malcolm Turnbull had at first been skeptical of an outright ban. According to Australian journalist Peter Hartcher, Turnbull bought himself a 474-page-book titled *A Comprehensive Guide to 5G Security* to study the topic so that he could ask better questions of his tech experts. Eventually he was convinced he had no choice but to ban the firm. Australia became the first country to formally cut Huawei's equipment from its 5G networks, a decision that was soon followed by Japan, New Zealand, and others.

Not every country had the same threat assessment. Many of China's neighbors were skeptical of the company and unwilling to take risks with network security. In Europe, by contrast, several traditional American allies looked warily at the Trump administration's pressure campaign to convince them to ban Huawei. Some close American allies in Eastern Europe openly banned the company, like Poland, which also in 2019 arrested a former company executive on espionage charges. France also quietly imposed strict restrictions. Other big European countries tried to find a middle ground. Germany, which exports large quantities of cars and machinery to China, was warned by the Chinese ambassador of "consequences" if it banned Huawei. "The Chinese government will not stand idly by," the Chinese diplomat threatened.

Ultimately the Trump administration expected pushback from Germany, which it saw as a free-riding ally on a range of issues. The bigger surprise was Britain, which despite its "special relationship" with the United States was spurning U.S. requests to ban Huawei from the UK's 5G networks and, instead, buy equipment from alternative suppliers like Sweden's Ericsson or Finland's Nokia. In 2019, the UK government's National Cyber Security Centre concluded the risk of Huawei systems could be managed without a ban.

Why did Australian and British cybersecurity experts differ in their assessment of Huawei risk? There's no evidence of technical disagreements. UK regulators were quite critical of deficiencies in Huawei's cybersecurity practices, for example. The debate was really about whether China should be stopped from playing an ever-larger role in the world's tech infrast ructure. Robert Hannigan, former head of the UK's signals intelligence agency, argued that "we should accept that China will be a global tech power in the future and start managing the risk now, rather than pretending the west can sit out China's technological rise." Many Europeans also thought China's technological advance was inevitable and therefore not worth trying to stop.

The United States government didn't agree. The issue with Huawei went far beyond the debate over whether the company helped tap phones or pilfer data. Huawei executives' admission that they'd violated U.S. sanctions on Iran angered many in Washington but was ultimately a sideshow. The real issue was that a company in the People's Republic of China had marched up the technology ladder—from, in the late 1980s, simple phone switches to, by the late 2010s, the most advanced telecom and networking gear. Its annual R&D spending now rivaled American tech giants like Microsoft, Google, and Intel. Of all China's tech firms, it was the most successful exporter, giving it detailed knowledge of foreign markets. It not only produced hardware for cell towers, it also designed cutting-edge smartphone chips. It had become TSMC's second biggest customer, behind only Apple. The pressing question was: Could the United States let a Chinese company like this succeed?

Questions like this made many people in Washington uncomfortable. For a generation, America's eli te had welcomed and enabled China's economic rise. The United States had also encouraged technology companies across Asia, providing market access to Japanese firms like Sony during the years of Japan's rapid growth and doing the same for South Korea's Samsung several decades later. Huawei's business model wasn't much different from that of Sony or Samsung when they first won a major position in the world's tech ecosystem. Wasn't a bit more competition a good thing?

On the National Security Council, however, competition with China was now seen primarily in zero-sum terms. These officials interpreted Huawei not as a commercial challenge but as a strategic one. Sony and Samsung were tech firms based in countries that were allied with the U.S. Huawei was a national champion of America's primary geopolitical rival. Viewed through this lens, Huawei's expansion was a threat. Congress wanted a tougher, more combative policy, too. "The United States needs to strangle Huawei," Republican senator Ben Sasse declared in 2020. "Modern wars are fought with semiconductors and we were letting Huawei use our Amer ican designs."

The point was less that Huawei was directly supporting China's military than that the company was advancing China's overall level of chip design and microelectronics know-how. The more advanced elec tronics the country produced, the more cutting-edge chips it would buy, and the more the world's semiconductor ecosystem would rely on China, at the expense of the United States. Moreover, targeting China's highest-profile tech fir m would send a message worldwide, warning other countries to prepare to take sides. Hobbling Huawei's rise became a fixation of the administration.

When the Trump administration first decided to turn up its pressure on Huawei, it prohibited the sale of U.S.-made chips to the company. This restriction alone was devastating, given that Intel chips are ubiquitous and many other U.S. companies manufacture all-but-irreplaceable analog chips. Yet after decades of offshoring, far less of the semiconductor production process took place in the United States than previously. For example, Huawei produced the chips that it designed not in the U.S.—which lacked facilities capable of building advanced smartphone processors—but at Taiwan's TSMC. Restricting the export of U.S.-made goods to Huawei would do nothing to stop TSMC from fabricating advanced chips for Huawei.

One might have expected the offshoring of chipmaking to have reduced the U.S. government's ability to restrict access to advanced chip fabrication. It would certainly have been easier to cut off Huawei if all the world's advanced chipmaking was still based on U.S. soil. However, the U.S. still had cards to play. For example, the process of offshoring chip fabrication had coincided with a growing monopolization of chip industry choke points. Nearly every chip in the world uses software from at least one of three U.S.-based companies, Cadence, Synopsys, and Mentor (the latter of which is owned by Germany's Siemens but based in Oregon). Excluding the chips Intel builds in-house, all the most advanced logic chips are fabricated by just two companies, Samsung and TSMC, both located in countries that rely on the U.S. military for their security. Moreover, making advanced processors requires EUV lithography machines produced by just one company, the Netherlands' ASML, which in turn relies on its San Diego subsidia ry, Cymer (which it purchased in 2013), to supply the irreplaceable light sources in its EUV lithography tools. It's far easier to control choke points in the chipmaking process when so many essential steps require tools, materials, or software produced by just a handful of firms. Many of these choke points remained in American hands. Those that didn't were mostly controlled by close U.S. allies.

Around this time, two academics, Henry Farrell and Abraham Newman, noticed that international political and economic relations were increasingly impacted by what they called "weaponized interdependence." Countries were more intwined than ever, they pointed out, but rather than defusing conflicts and encouraging cooperation, interdependence was creating new venues for competition. Networks that knit together nations had become a domain of con flict. In the financial sphere, the U.S. had weaponized other countries' reliance on access to the banking system to punish Iran, for example. These academics worried that the U.S. government's use of trade and capital flows as political weapons threatened globalization and risked dangerous unintended consequences. The Trump administration, by contrast, concluded it had unique power to weaponize semiconductor supply chains.

In May 2020, the administration tightened restrictions on Huawei further. Now, the Commerce Department declared, it would "protect U.S. national security by restricting Huawei's ability to use U.S. technology and software to design and manufacture its semiconductors abroad." The new Commerce Department rules didn't simply stop the sale of U.S.-produced goods to Huawei. They restr icted any goods made with U.S.-produced technology from being sold to Huawei, too. In a chip industry full of choke points, this meant almost any chip. TSMC can't fabricate advanced chips for Huawei without using U.S. manufacturing equipment. Huawei can't design chips without U.S.-produced so ftware. Even China's most advanced foundry, SMIC, relies extensively on U.S. tools. Huawei was simply cut off from the world's entire chipmaking infrastructure, except for chips that the U.S. Commerce Department deigned to give it a special license to buy.

The world's chip industry quickly began implementing the U.S. rules. Even though the U.S . was trying to eviscerate its second-largest customer, TSMC's chairman, Mark Liu, promised not only to abide by the letter of the law but also its spirit. "This is something that can be solved not solely through the interpretation of the rules, but also has to do with the intentions of the U.S. government," he told journalists. Since then, Huawei's been forced to divest part of its smartphone business and its server business, since it can't get the necessary chips. China's rollout of its own 5G telecoms network, which was onc e a high-profile government priority, has been delayed due to chip shortages. After the U.S. restrictions took place, other countries, notably Britain, decided to ban Huawei, reasoning that in the absence of U.S. chips the company would struggle to service its products.

The assault on Huawei was followed by blacklisting multiple other Chinese tech firms. After discussions with the United States, the Netherlands decided not to approve the sale of ASML's EUV machines to Chinese firms. Sugon, the supercomputer company that AMD described in 2017 as a "strategic partner," was blacklisted by the U.S. in 2019. So, too, was Phytium, a company that U.S. officials say has designed chips for supercomputers that were used to test hypersonic missiles, accord ing to a report in

the *Washington Post*. Phytium's chips were designed using U.S. software and produced in Taiwan at TSMC. Access to the semiconductor ecosystem of America and its allies enabled Phytium's growth. However, the company's reliance on foreign software and manufacturing left it critically vulnerable to U.S. restrictions.

Ultimately, though, the American assault on China's tech firms has been a limited strike. Many of China's biggest tech companies, like Tencent and Alibaba, still face no specific limits on their purchases of U.S. chips or their ability to have TSMC manufacture their semiconductors. SMIC, China's most advanced producer of logic chips, faces new restrictions on its purchases of advanced chipmaking tools, but it has not been put out of business. Even Huawei is allowed to buy older semiconductors, like those used for connecting to 4G networks.

Nevertheless, it's surprising that China's done nothing to retaliate against the hobbling of its most global tech firm. It has repeatedly threatened to punish U.S. tech firms but never pulled the trigger. Beijing said it was drawing up an "unreliable entity list" of foreign companies that endanger Chinese security, but it doesn't appear to have added any firms to the list. Beijing has evidently calculated that it's better to accept that Huawei will become a second-rate technology player than to hit back against the United States. The U.S., it turns out, has escalation dominance when it comes to severing supply chains. "Weaponized interdependence," one former senior official mused after the strike on Huawei. "It's a beautiful thing."