Seizing Core Technologies: China Responds to U.S. Technology Competition

by Adam Segal

Chinese analysts and policy makers have interpreted U.S. efforts to prevent the flow critical technologies through limits on investment, blocks on the operations of Huawei and other Chinese telecom companies in the U.S. and other markets, and new export control laws, as part of a strategy of containment designed to slow China's rise as a science and technology power. In response, a newly emerging strategy consists of: a doubling down on indigenous innovation and developing "core technologies"; protection of supply chains; diversification of access to foreign technology; diplomatic efforts that stress the shared benefits of Chinese technology development; and continued cyber-enabled theft of intellectual property. Even though both sides are likely to lose the efficiencies that came from the globalization of innovation, such a strategy may also energize American and Chinese policy makers to mobilize even greater resources for scientific competition.

While the Trump administration has caused a fair degree of uncertainty in Beijing about its ultimate strategic and economic objectives through an unconventional policy process, shifting personnel, and conflicting messages emanating from the President's tweets, there is a widespread consensus among Chinese policy makers and analysts about the motivations of U.S. technology policy. Officials and academics are convinced that Washington is pursuing a strategy of containment, designed to slow China's rise as a science and technology power, or, as Fudan University Professor Zhou Wen argues, "The United States' real intention is to suppress the development of China's high-tech industries."[1]

To be sure, over the last several years both China and the United States have acted to reduce vulnerabilities created by the interconnectedness of their science and technology systems. President Xi Jinping has continued to implement the techno-nationalist policies introduced by his predecessors. The 2017 National Cybersecurity Law and Made in China 2025 as well as large investments in artificial intelligence, semiconductors, and quantum computing are the most recent efforts to free China from dependence on the West for critical technologies. Washington, anxious about China's rising technological capabilities and its program of military-civil fusion, has limited Chinese investment in U.S. technology sectors, blocked Chinese telecommunications companies from doing business in the United States and other markets, and tightened controls on the sale of technologies.

The long-term effects of the decoupling of the U.S. and Chinese technology systems are uncertain. While both sides are likely to lose the efficiencies that came from the globalization of innovation, such decoupling may also energize American and Chinese policy makers to mobilize even greater resources for scientific competition. It is, however, too early to know whether the costs of eliminating the vulnerabilities created by interdependence outweigh the potential innovation gains of competition.

In the short term, it is possible to identify an emerging Chinese strategy in reaction to U.S. pressure consisting of: doubling down on indigenous innovation and developing "core technologies"; protecting supply chains; diversifying access to foreign technology; making diplomatic efforts that stress the shared benefits of Chinese technology development; and continuing cyber-enabled theft of intellectual property.

U.S. Strategy

The Trump administration has placed Chinese technology policy front and center as a danger to U.S. economic and national security, and in response it has rolled out a fourfold policy response.[2] First, the United States levied tariffs on products benefiting from "Made in China 2025," Beijing's initiative to upgrade its manufacturing sector, placing a 25 percent tariff on 1,300 industrial technology, transport, and medical products.

Second, Congress has limited Chinese investment in U.S technology sectors, and the Commerce Department is revising the export control laws so as to block the flow of critical technologies to Chinese end-users. In August 2018, Congress passed the Foreign Investment Risk Review Modernization Act, enabling the Committee on Foreign Investment in the United States (CFIUS) to investigate additional investments, for instance minority positions or overseas joint ventures. The legislation also added new national security criteria to CFIUS decisions. The Trump administration has blocked the sale of the Lattice Semiconductor to a group that included a Chinese venture capital firm; barred Broadcom's US$121 billion offer for Qualcomm; prevented Ant Financials acquisition of MoneyGram; and demanded that Beijing Kunlun Tech give up its control of Grindr, a gay dating app.

In addition, the 2018 Export Control Reform Act includes new controls on the export of "emerging and foundational technologies." The Commerce Department, which is responsible for overseeing such restrictions, has published a list of technologies that might be controlled, including computer vision, speech recognition, and natural language understanding.[3]

Third, Trump officials have made it more difficult for Huawei and other Chinese telecom companies to do business in the United States. Congress has prohibited the Pentagon from buying network equipment from either Huawei or ZTE, and security concerns reportedly were behind AT&T's and Verizon's decisions not to distribute Huawei smartphones. The Federal Communications Commission has proposed making it more difficult for smaller carriers to use the Universal Service Fund to pay for future purchases of telecom equipment from Huawei and ZTE, and in April 2019 the FCC opposed China Mobile's application to provide telecommunications services in the United States.[4]

In addition, U.S. officials have pressured Australia, Canada Japan, the European Union, and other allies and friends not to use Huawei for 5G infrastructure. Whereas Germany and the UK have suggested they can manage the risk of using Chinese suppliers, Secretary of State Mike Pompeo has threatened to stop sharing intelligence with allies, telling an interviewer, "If a country adopts this [Huawei equipment] and puts it in some of their critical information systems, we won't be able to share information with them, we won't be able to work alongside them."[5] Others, such as Bahrain, Iceland, Saudi Arabia, Latin America, and the United Arab Emirates,

have ignored Washington's warnings and have recently signed deals to deploy Huawei's 5G equipment.[6]

Fourth, the Department of Justice has pursued a number of high-level indictments against Chinese companies for theft of intellectual property. In November 2018, Trump officials charged Fujian Jinhua with the theft of DRAM—dynamic random-access memory technology— from Micron. The Commerce Department subsequently put Fujian Jinhua on a list of entities that cannot purchase components, software, and technology goods from U.S. firms. In January 2019, the Justice Department unsealed indictments claiming that Huawei stole technology from T-Mobile and that Huawei had a formal policy of awarding bonuses to employees who stole confidential information from competitors.[7]

The Trump administration has also responded to the return of Chinese hackers after the brief downturn in activities in the wake of a September 2015 agreement between President Xi and President Obama in which both sides pledged not to become involved in cyber-enabled theft of intellectual property for competitive advantage. In November 2017, the Justice Department indicted three Chinese nationals employed by the Chinese cybersecurity firm Boyusec, charging them with hacking into the computer systems of Moody's Analytics, Siemens AG, and global positioning system developer Trimble Inc. In November 2018, then Attorney General Jeff Sessions announced a China initiative to identify priority Chinese trade theft cases, pool FBI and Department of Justice resources to combat Chinese economic espionage and evaluate whether additional legislative and administrative authorities would be required to protect U.S. assets from foreign economic espionage. Finally, in December 2018 the United States, in coordination with Canada and the United Kingdom, indicted two Chinese citizens for hacking more than forty-five technology companies in at least one dozen U.S. states.[8]

Technology Containment

Chinese analysts are clear about the goals and motivations of U.S. technology strategy. In short, they argue that Washington is pursuing policies designed to slow China's rise as a science and technology power. Or, as Li Zheng of the China Institute of Contemporary International Relations, has put it, "The United States views technology as the 'last barrier' to constrain China's challenge." Li continues that U.S. actions have "risen to the strategic level," seeking to "systematically and comprehensively curb the rapid rise of China's technology industry."

Moreover, Zhou Xiaoming, a former Chinese diplomat, argues that the containment policies are here to stay: "The containment of the United States against China will be a normal state, and it will intensify. We must learn to adapt."[9] These "containment" policies, according to most analysts, are not a response to Beijing's industrial policies or theft of intellectual property, but rather they stem from a decline in U.S. power and prestige and a "panic" about China's rise in technologies, such as 5G and artificial intelligence.[10]

Analysts and policy makers have used the blockade of ZTE as clear evidence of Washington's intentions and China's vulnerabilities. In April 2018, the United States announced a seven-year ban on American firms from selling parts and software to ZTE after the company violated an agreement that was reached when it was caught illegally shipping U.S. goods to Iran.[11] Even

though the ban was eventually overturned after the company paid a US$1 billion fine, the ban threatened ZTE's survival and clearly demonstrated China's dependence on U.S. technology, especially semiconductors.

In a series of speeches after the ZTE ban, Xi Jinping highlighted China's need for innovation and technological self-determination. In an April 20, 2018 speech on cyberspace and information technologies, Xi focused on indigenous innovation and for the first time described "core technologies" as "important instruments of the state" (**核心技**术是国之重器). (Xi's 2016 speech on cyberspace also stressed the centrality of "gaining breakthroughs in core technology as quickly as possible," but it did not use the phrase "instrument of the state.")[12]

In May 2018, at a joint annual conference of the Chinese Academy of Sciences and the Chinese Academy of Engineering, Xi exhorted the gathered scientists and engineers to redouble their efforts, stating: "Self-determination and innovation is the unavoidable path ... to climb to the world's top as a leading player in technology." [13] Xi returned to the same themes in July 2018, telling the Central Financial and Economic Affairs Committee that "China must improve innovation capabilities for key and core technologies and keep a firm hold on the initiative in the development of science and technology to offer a strong technological guarantee for China's development." [14]

In September, during a visit to Heilongjiang, President Xi argued that "rising unilateralism and trade protectionism" was pushing Chinese companies to adopt a "self-reliance" strategy, which, he said, was "not a bad thing."[15] Days after the Commerce Department sanctioned Fujian Jinhua in November, Xi called for acceleration of the development of artificial intelligence, telling a Politburo study group that China must "control" the technology and make sure it is "securely kept in our own hands."[16]

China's Response

In the face of U.S. pressure, Beijing has adopted a five-part response. First, although China is likely to make some concessions at the margins of its industrial policy as part of any trade deal, it is equally expected that it will follow Xi's repeated calls to double down on efforts to reduce dependence on the West for semiconductors and other critical technologies. In a March 2019 speech to the National People's Congress (NPC), Li Keqiang made no reference to "Made in China 2025," but he stated the government would promote advanced manufacturing in the same areas covered by Made in China 2025.[17] Similarly, the 2019 draft plan of the National Development and Reform Commission submitted to the NPC states that it "will prioritize and strongly develop a number of clusters of strategic emerging industries in key fields such as next-generation IT, high-end equipment, biotechnology, and new materials."[18]

At the same meeting, Chinese lawmakers passed a new foreign investment law that is intended to stop the forced transfer of technology from foreign companies. There are, however, serious questions about enforcement of the law, and there is, in any case, no evidence that Chinese policy makers have abandoned deeply held beliefs about the need for technological self-reliance.[19]

China will continue to promote advances in semiconductors with huge investments in new fabs and technology. In 2018, China's chip imports broke US$300 billion, rising from US$270 billion in the previous year.[20] Hu Weiwu, a Chinese Academy of Science scholar and the engineer behind the Loongson CPU, believes that the ZTE incident is a chance for the "domestic chip industry to turn a crisis into an opportunity."[21] He suggested that the Chinese government should take advantage of this opportunity to promote the commercial application of domestic chips and build China's own information and communication technology ecosystem. During the last several years, Beijing has mobilized US$100–US$150 billion in public and private funds to build an indigenous industry. Local governments have ramped up investment projects and the central government has designated a number of companies as national champions in manufacturing and chip design. China has the most fab projects in the world, with thirty new facilities or lines either in construction or in the planning stages.[22]

China will also pursue other avenues for computer and chip design, for example designating a quantum-computing "megaproject." The government is reportedly investing US$1 billion to build the National Laboratory for Quantum Information Sciences in Hefei, and in 2017 Chinese companies filed twice as many patents for quantum computing as did American companies.[23]

Chinese technology companies have signaled that they will follow the government's lead. As Alibaba's CEO Jack Ma said, "Big enterprises have an important responsibility. If we do not master the core technologies, we will be building roofs on other people's walls and planting vegetables in other people's yards."[24] Baidu released its smart chip, Kunlun, in July; Huawei unveiled a 7nm microchip in August; and Alibaba launched its semiconductor division Pingtouge in September. This new business will develop artificial intelligence chips for cloud computing and Internet-connected devices. Huawei also announced that it has built its own operating systems for smartphones and laptops in case it is unable to use Google or Microsoft software in the case of another round of U.S. sanctions, and in April 2017 the company announced it will establish an Institute of Strategic Research and invest US$300 million each year for the next five to ten years to fund research in basic science and technology.[25]

Second, Chinese technology companies will make efforts to protect their supply chains from U.S. sanctions. After the arrest of CFO Meng Wanzhou for allegedly violating sanctions on Iran, Huawei's leaders feared they would face a fate similar to that of ZTE. Huawei boosted purchases of capacitors, integrated circuits, flash memory and camera-related parts from Japanese suppliers, stockpiling components in case of a potential ban on U.S. sales.[26] Huawei reportedly asked Taiwan's ASE Technology Holding and King Yuan Electronics, its top chip packaging and testing providers, to relocate most production to sites in mainland China. The company also spoke with Taiwan Semiconductor Manufacturing Co. about moving some chip production to Nanjing.[27]

Third, Chinese firms and investors are diversifying and looking for new technology-investment opportunities beyond U.S regulations. In 2016, China invested US$18.7 billion in 107 U.S. tech firms. In 2018, because of increased CFIUS scrutiny the total dropped to US$2.2 billion for eighty deals. As investment in the United States has fallen, there have been some notable technology acquisitions in Europe, such as Tencent's US$8.6 billion purchase of Finnish gaming

company Supercell and CSC Group's multimillion-dollar investment in the London-based accelerator Founders Factory.[28] European governments are, however, updating or introducing foreign-investment screening regimes, and for the first time a Chinese acquisition was blocked when the German government vetoed the takeover of a machine tool company.[29]

In addition, Chinese investors are looking at the Israeli technology sector, where Chinese investment has grown from US$274 million in 2016 to US$325 million in the third quarter of 2018.[30] Chinese funders supplied at least US$20 million in all seventeen financing rounds for Israeli start-ups during the first three quarters of 2018.[31] In response to these investments as well as Chinese investments in Israeli infrastructure, the Trump administration has reportedly told Israeli officials they must establish a CFIUS process for dual-use technologies and they also risk harming intelligence-sharing between the United States and Israel if the infrastructure projects move forward.[32]

Fourth, Chinese diplomatic efforts are likely to stress the global benefits of Chinese scientific and technological development and the threats to trade and security emanating from the United States. For example, during his 2019 Davos speech Wang Qishan called for countries to "work together to shape the global architecture in the age of the fourth industrial revolution with the vision to create a better future for all mankind." He warned, however, that it is "imperative to respect national sovereignty and refrain from seeking technological hegemony, interfering in other countries' domestic affairs, and conducting, shielding, or protecting technology-enabled activities that undermine other countries' national security. We need to respect the independent choices of model technology management and of public policies made by countries, and their rights to participate as equals in the global technological governance system."[33]

Chinese diplomacy is also likely to echo the public relations campaign that Huawei has mounted in the face of U.S pressures, casting aspersions on those who question the security of Huawei's products. In an op-ed piece in the *Financial Times* and in a speech at the Mobile World Congress in Barcelona, Guo Ping, chairman of Huawei, drew attention to U.S. intelligence capabilities. Explaining why Washington was trying to block the company, Guo argued that Huawei equipment was more difficult for the National Security Agency (NSA) to hack because the agency maintained cooperative relations with U.S. telecoms. Since Chinese firms were unlikely to cooperate if U.S. intelligence wanted "to modify routers or switches in order to eavesdrop," Guo concluded, Huawei "hampers U.S. efforts to spy on whomever it wants."[34]

The Foreign Ministry made a similar pivot with Australia's new encryption bill, which requires tech companies to provide law enforcement and security agencies access to encrypted communications. Asked whether Australia was engaged in a double standard since it had banned Huawei from its 5G roll-out because it did not want companies in their networks that were beholden to another government, Foreign Ministry Spokesperson Lu Kang noted "Forcing companies to install 'backdoors' through legislation means protecting one's own security and interests at the expense of other countries' security and their people's privacy." Lu further claimed, "It is baffling how the country concerned could whip up 'security threats' posed by other countries or companies with trumped-up charges under the facade of cyber security, while they themselves are engaged in acts that endanger cyber security.[35]

Fifth, Chinese hackers will continue their campaign of cyber-enabled theft of intellectual property. CrowdStrike, FireEye, PwC, Symantec, and other cybersecurity companies reported new Chinese computer attacks on U.S. companies in 2017 and 2018. Rob Joyce, a senior official in the NSA and former White House cybersecurity coordinator, stated in November 2018 that "it's clear that they [China] are well beyond the bounds today of the agreement that was forged between our countries."[36]

Chinese hackers may have reinstated their cyber-enabled theft of intellectual property for two reasons.[37] First, Beijing may have never intended for the pause to be long term, but instead saw it as an opportunity to gain diplomatic advantage for a planned restructuring of its cyber forces that independently would create a temporary downturn in activity. The purpose of this reorganization, which involved the creation of the Strategic Support Forces and the shifting of espionage to more skilled hackers in the Ministry of State Security (MSS), was to allow the People's Liberation Agency (PLA) to focus on warfighting and to reduce the chances that Chinese hackers would be called out by Washington. In effect, Beijing did not intend to give up hacking over the long term; it simply wanted to stop being caught so often.

Second, the return of hacking may be a reaction to increased pressure from Washington. If Chinese policy makers believe the United States has adopted a technology containment strategy, they are also likely to believe they have little to gain from honoring the 2015 agreement between Xi and Obama.

No matter the reason, and it may actually be some combination of the two, China possibly believes it can reach a stable equilibrium of espionage with the United States, in which the MSS deploys a level of tradecraft equivalent to the hacking conducted by the NS.. A high level of relatively "noisy" activity (for which they were likely to get caught and be called out on) is being replaced by a smaller number of more professional hacks who nevertheless provide China access to U.S. assets.[38]

Conclusion

There is also another possible direction that Beijing could take. Chinese leaders could embrace openness and an innovation strategy, a more bottom-up effort to create an environment supporting technological innovation rather than continuing down the road of market barriers and top-down, state-directed efforts to develop specific technologies. There is a long debate in Chinese technology policy about the best means to achieve the objectives of technological autonomy, and parts of the bureaucracy believe that it is possible for China to raise its technological capabilities through more market-friendly policies. The 2006 Guidelines on the National Medium- and Long-term Program for Science and Technology Development, for example, introduced the idea of indigenous innovation (*zizhu chuangxin*) and eighteen science and engineering "megaprojects" also draw on the experience of Silicon Valley and introduce policies that deal with university-industry collaboration, venture capital, and small-start-ups. At least eight provisions either directly or indirectly focus on small and medium-sized technology businesses.[39]

There are hints of this thinking in some of the analysis of what is called the U.S. technology containment strategy. While analysts do not question the legitimacy of the ultimate goal of developing and controlling core technologies, they also introduce a range of reforms necessary to improve China's innovation capabilities. These include reforming the education system, limiting the impact of political factors in funding and personnel evaluations, and recruiting foreign talent.

These voices were clearly in the minority even before the current U.S.-China technology war, and they are unlikely to gain significant policy traction during the technology war. Instead, the stark vulnerability in core technologies that has been exposed by U.S. actions will accelerate efforts to eliminate such dependencies. Beijing is likely to continue with heavy state support for R&D, especially for semiconductors, AI, and other frontier technologies; to coordinate with technology companies on the development of these same technologies; to diversify investment opportunities; and to direct a campaign on cyber-enabled industrial espionage.

Although Washington should maintain efforts to push back against Beijing's market distorting policies and cyber theft, U.S. policy makers should work more closely with their counterparts in Europe and Asia to create a more multilateral effort. The European Commission's March 2019 review of the EU's relations with China, for example, criticizes Beijing for preserving "its domestic markets for its champions, shielding them from competition through selective market opening, licensing and other investment restrictions; [and] heavy subsidies to both state-owned and private sector companies."[40] Such efforts may take some of the heat out of the tech war, making it less a U.S. containment strategy and more a broader conflict between China's development model and the norms of the more open economies.

Both sides will incur costs from a technology cold war. Global challenges, such as addressing climate change and stopping pandemics, require collaboration, and all will benefit from breakthroughs in clean energy, carbon capture, and new vaccinations against influenza. Chinese and American policy makers will need to distinguish between competition over technologies with national security implications and more cooperative approaches to targeted technologies that could be the basis for a reconsidered U.S.-China science relationship.

Adam Segal is the Ira A. Lipman chair in emerging technologies and national security and director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations

[1] Zhou Wen, "Huawei Incident is the US Political Pursuit of China's High-tech Enterprises" (华为事件是美国对中国高科技企业的政治追杀), at https://mp.weixin.qq.com/s/_qudPfUS9qhVTCgcl0uBNw

[2] Office of the U.S. Trade Representative, *Findings of the Investigation* into *China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation, under Section 301 of the Trade Act of 1974*, March 22, 2018, at https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF; White House Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*, June 2018, at https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf

[3] Cade Metz, "Curbs on A.I. Exports? Silicon Valley Fears Losing Its Edge," *New York Times*, January 1, 2019, at https://www.nytimes.com/2019/01/01/technology/artificial-intelligence-export-restrictions.html

[4] Cecilia Kang, "F.C.C. Chair Plans to Block China Mobile From U.S. Market," *New York Times*, April 17, 2019, at https://www.nytimes.com/2019/04/17/business/fcc-china-mobile-block.html

[5] "Mike Pompeo: Been Making Sure Countries Understand the Risk of Putting Huawei Technology into their IT Systems," *Fox Business News*, February 21, 2019, at https://video.foxbusiness.com/v/6005194321001/#sp=show-clips

[6] Jeremy Horwitz, "Huawei Racks Up 5G Network Deals at MWC 2019 Despite U.S. Pressure," *VentureBeat*, February 27, 2019, at https://venturebeat.com/2019/02/27/huawei-racks-up-5g-network-deals-at-mwc-2019-despite-u-s-pressure/

[7] U.S. Department of Justice, "Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction of Justice," January 28, 2019, at https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade

[8] U.S. Department of Justice, "Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information," December 20, 2018, at https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

9 "U.S. Technology Blockade Against Chinese Firms Seeks to Contain China High Tech Development and Innovation" (美国对中国企业技术封锁 想遏制中国高科技发展和创新) *Gucheng*, August 6, 2018, at https://finance.gucheng.com/201808/3482211.shtml

[10] "Discussing China's Breakthroughs in Core Technological Innovation within the Context of U.S. Technological Containment Strategy" (前沿 | 透过美国对华科技遏制谈我国核心技术创新突破), *China Infosec*, April 1, 2019, at https://mp.weixin.qq.com/s?__biz=MzA5MzE5MDAzOA==&mid=2664117218&idx=2&sn=fc617d34adecbe0943dabcb9abdb5fce&chksm=8b5e311bbc29b80d6b0f94f370583e577273743a736dc8e798ec4da60764e4478438e5e586f2&scene=0&xtrack=1#rd

[11] US Department of Commerce, "Secretary Ross Announces Activation of ZTE Denial Order in Response to Repeated False Statements to the U.S. Government," April 16, 2018, at https://www.commerce.gov/news/press-releases/2018/04/secretary-ross-announces-activation-zte-denial-order-response-repeated

[12] Xi Jinping, "Speech at the Work Conference for Cybersecurity and Informatization," translated by *China Copyright and Media*, April 19, 2016, at https://chinacopyrightandmedia.wordpress.com/2016/04/19/speech-at-the-work-conference-for-cybersecurity-and-informatization/

[13] Kinling Lo, "Xi Jinping Urges China to Go All in on Scientific Self-reliance After ZTE Case Exposes Hi-tech Gaps," *South China Morning Post*, May 28, 2018, at https://www.scmp.com/news/china/economy/article/2148189/xi-jinping-urges-china-go-all-scientific-self-reliance-after-zte

[14]"Xi Stresses Improving Innovation Capabilities for Key, Core Technologies," Xinhua, July 14, 2018, at http://www.xinhuanet.com/english/2018-07/14/c_137322614.htm

[15] Xu Wei, "Xi Stresses Nation's Self Reliance," *China Daily*, September 27, 2018, http://www.chinadaily.com.cn/a/201809/27/WS5babed9aa310c4cc775e8414.html

[16] Anna Fifield, "As China Settles in for Trade War, Leader Xi Emphasizes 'Self Reliance,'" *Washington Post*, November 2, 2018, at https://www.washingtonpost.com/world/asia_pacific/as-china-settles-in-for-trade-war-leader-xi-emphasizesself-reliance/2018/11/01/2961b2b2-d8de-11e8-9559-712cbf726d1c_story.html

[17] Lingling Wei, "Beijing Drops Contentious 'Made in China 2025' Slogan, but Policy Remains," *Wall Street Journal*, March 5, 2019, at https://www.wsj.com/articles/china-drops-a-policy-the-u-s-dislikes-at-least-in-name-11551795370

[18] "Report on the Implementation of the 2018 Plan for National Economic and Social Development and on the 2019 Draft Plan for National Economic and Social Development," at http://www.xinhuanet.com/english/2019-03/17/c_137901686.htm

[19] Austin Lowe, "China's Foreign Investment Law Fails to Address U.S. Concerns," *Lawfare*, March 7, 2019, at https://www.lawfareblog.com/chinas-foreign-investment-law-fails-address-us-concerns

[20] "China's Chip Imports Break $300 Billion, According to the General Manager of China's National IC Fund" (芯片进口总额突破 3000 亿美元，中国芯及 AI 芯片要强大缺什么？) *LeiPhone*, April 11, 2019, at https://www.leiphone.com/news/201904/n3z1Mu1chbtZuuKT.html

[21] "The U.S. Banning ZTE from Buying U.S. Chip Technology Fuels Debate about Whether 'Chip Sickness' Requires a 'Chip Cure'" (中兴被美国禁用芯片引热议 "芯病"还需"芯药"医), *China Youth Daily*, April 19, 2018, at http://it.people.com.cn/n1/2018/0419/c1009-29935507.html

[22] Mark Lapedus, "China's Foundry Biz Takes Big Leap Forward," *SemiEngineering*, January 28, 2019, at https://semiengineering.com/chinas-foundry-biz-takes-big-leap/

[23] Susan Decker and Christopher Yasiejko, "Forget the Trade War. China Wants to Win Computing Arms Race," *Bloomberg*, April 8, 2018, at https://www.bloomberg.com/news/articles/2018-04-08/forget-the-trade-war-china-wants-to-win-the-computing-arms-race

[24] "Alibaba's Jack Ma on Developing Core Technologies post-ZTE," *Shanxi Evening News*, April 24, 2018, http://baijiahao.baidu.com/s?id=1598613211326939453&wfr=spider&for=pc

[25] Arjun Kharpal, "Huawei Built Software for Smartphones and Laptops in Case it Can't Use Microsoft or Google Products," *CNBC*, March 15, 2019, at https://www.cnbc.com/2019/03/15/huawei-has-built-its-own-operating-system-for-smartphones-laptops.html; "Huawei Commits 300 Million USD Annually to Basic S&T research," Xinhua, April 17, 2019, at http://www.xinhuanet.com/english/2019-04/17/c_137984843.htm

[26] Naoki Watanbe, "Huawei Boosts Japan Parts Orders, Hedging US Risks," *Nikkei Asian Review*, March 7, 2018, at https://asia.nikkei.com/Business/China-tech/Huawei-boosts-Japan-parts-orders-hedging-US-risks

[27] Lauly Li, Cheng Ting-Fang, and Coco Liu, "Huawei Tells Suppliers to Move Production to China as US Ban Looms," *Nikkei Asian Review*, January 30, 2019, at https://asia.nikkei.com/Business/China-tech/Huawei-tells-suppliers-to-move-production-to-China-as-US-ban-looms

[28] Ji Bo, "Amid Trade War, Foreign Startups May Spot Opportunity in China," *Venturebeat*, March 16, 2019, at https://venturebeat.com/2019/03/16/amid-trade-war-foreign-startups-may-spot-opportunity-in-china/

[29] "Chinese Takeover of German Firm Leifeld Collapses," BBC, August 1, 2018, at https://www.bbc.com/news/world-europe-45030537

[30] Rami Blachman, "Amid Trade War Crossfire, Israel-China Tech Courtship Presses On," *Technode*, February 28, 2019, at https://technode.com/2019/02/28/amid-trade-war-crossfire-israel-china-tech-courtship-presses-on/

[31] Nisha Gopalan, "For China, Israel Loses its Promised Land Allure," February 22, 2019, at https://www.bloomberg.com/opinion/articles/2019-02-23/scrutiny-of-china-tech-deals-via-israeli-cfius-hurts-both-sides

[32] Stuart Winer, "Chinese Investment in Israel Could Harm Intelligence Ties, US Official Warns," *Times of Israel*, January 16, 2019, at https://www.timesofisrael.com/chinas-investments-in-israel-could-harm-intelligence-ties-us-official-warns/

[33] Full Text of Chinese Vice President's Speech at 2019 WEF Annual Meeting, January 24, 2019, at http://www.xinhuanet.com/english/2019-01/24/c_137771279.htm

[34] Guo Ping, "The US Attacks on Huawei Betray its Fear of Being Left Behind," *Financial Times*, February 27, 2019, at https://www.ft.com/content/b8307ce8-36b3-11e9-bb0c-42459962a812

[35] Foreign Ministry Spokesperson Lu Kang's Regular Press Conference on April 10, 2019, at https://www.fmprc.gov.cn/mfa_eng/xwfw_665399/s2510_665401/t1653187.shtml

[36] "U.S. Accuses China of Violating Bilateral Anti-Hacking Deal," Reuters, November 8, 2018, at https://ca.reuters.com/article/topNews/idCAKCN1NE02E-OCATP

[37] Lorand Laskai and Adam Segal, "A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage," Council on Foreign Relations, December 6, 2018, at https://www.cfr.org/report/threat-chinese-espionage

[38] Adam Segal et al., "Hacking for Ca$h: United States," Australian Strategic Policy Institute, September 25, 2018, at https://www.aspi.org.au/report/hacking-cash

[39] Adam Segal, "Chinese Technology Policy and American Innovation," testimony before US China Security Review Commission, June 15, 2011, at https://www.cfr.org/report/chinese-technology-policy-and-american-innovation

[40] European Commission, "EU-China – A Strategic Outlook," March 12, 2009, at https://ec.europa.eu/commission/sites/beta-political/files/communication-eu-china-a-strategic-outlook.pdf