

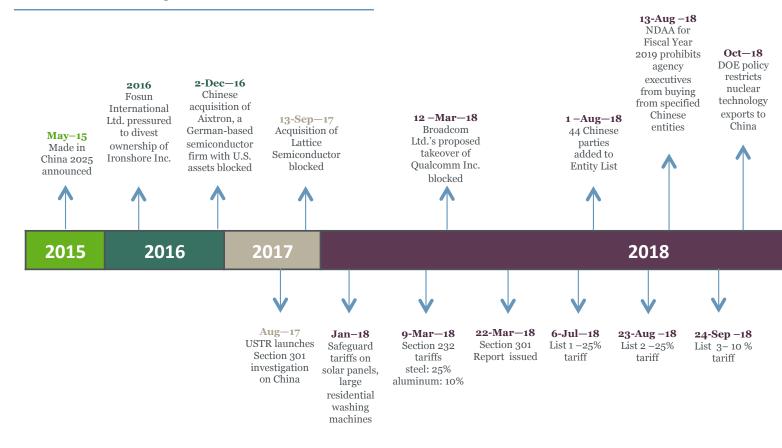
### With or without a trade deal, national security concerns regarding China are here to stay

Since President Trump took office, the U.S.-China trade relationship has been at the center of the administration's foreign policy agenda. While a broader trade deal may grant reprieve to the series of escalating tariffs between the two countries that have defined U.S.-China trade policy over the past year, the Trump administration is unlikely to wholly abandon its forceful approach to containing the growing influence of China in the global economy, which it sees as a direct threat to the national security of the United States.

Distinct from trade disputes of past administrations, President Trump has broadly mobilized the U.S. government to counter this perceived national security threat from China. Multiple government departments and agencies have taken or are considering a range of actions, including:

- Expanding restrictions on foreign investment in the United States from China and other countries on national security grounds.
- Expanding and enforcing restrictions on the transfer of strategic technology and items to China and Chinese persons.
- Designating individual Chinese companies for national security concerns.
- Barring the use of Chinese telecommunication and IT equipment in U.S. networks or by the U.S. government.
- Targeting Chinese companies that engage in intellectual property theft.

### Timeline of Selected China-Related National Security Measures

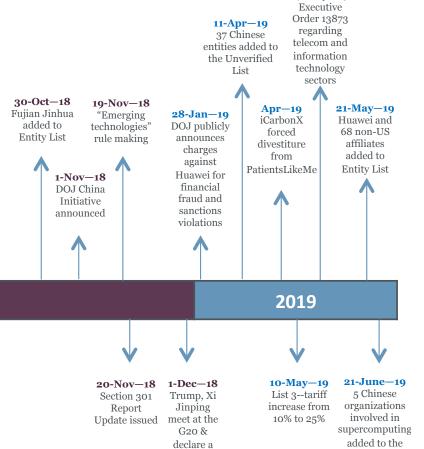


 Marshalling the broad trade powers of the U.S. government to counter Chinese influence based on national security concerns.

These actions are primarily aimed at preventing the Chinese government, companies, and individuals from obtaining technology, lawfully or through theft, to support China's development of strategic industries. China's concerted effort to increase its influence over the global economy was put on full display in May 2015 with the unveiling of its Made in China 2025 initiative. The purpose of the Made in China 2025 campaign is to rapidly achieve Chinese dominance in high-technology and advanced manufacturing by acquiring intellectual property from outside of China, subsidizing Chinese industry, and leveraging state-owned enterprises. The Trump administration has taken notice of China's plans to achieve dominance in key strategic industries, labeling the Made in China 2025 initiative as China's "most prominent industrial policy." Going even

17-May-19

Entity List



90-day truce to tariff escalation



further, United States Trade Representative Robert Lighthizer has stated that "China's government is aggressively working to undermine America's hightech industries and our economic leadership through unfair trade practices and industrial policies like 'Made in China 2025.'"<sup>2</sup>

Generally, there remains broad bipartisan support throughout the U.S. government for President Trump's robust approach to China, though some specific actions – such as the use of Section 232 tariffs based on national security grounds (discussed below) – have drawn criticism from Democrats and Republicans alike. Regardless of whether the Trump administration is able to strike a trade deal with China under renewed negotiations, national security concerns will remain, and the U.S. government will likely continue to expand restrictive measures against China and Chinese companies for the foreseeable future.

These actions are having a significant impact on U.S. and global companies that have customers in China or supply chains dependent on Chinese products, components, and technology. In particular, the expansion of restrictions on China could potentially lead to a decoupling of the U.S. and Chinese markets in certain industries (e.g., telecommunications, cybersecurity, and certain advanced technologies) – a significant challenge facing many global companies, including those operating in the aerospace, defense, and government services industry sector.

"China's government is aggressively working to undermine America's high-tech industries and our economic leadership through unfair trade practices and industrial policies like 'Made in China 2025."

United States Trade
 Representative Robert Lighthizer

This article sets forth below (1) a high-level summary of recent U.S. government actions against China based on national security grounds and (2) considerations that global companies should take into account when dealing with Chinese companies to remain compliant with complex U.S. legal restrictions.

## U.S. government assessment of the threat from Chinese acquisition of U.S. technology

The Trump administration, certain agencies of the U.S. government, and Congress have all sounded the alarm of the perceived national security threat from China. In particular, the U.S. government has blurred the lines between national security and economic espionage, specifically characterizing Chinese attempts to acquire U.S. technology through intellectual property theft and lawful technology transfers as national security threats.<sup>3</sup>

The Department of Defense's (DOD) 2018 National Defense Strategy found that "[i]nter-state strategic competition, not terrorism, is now the primary concern in U.S. national security." In particular, this report stated, "It is increasingly clear that China and Russia want to shape a world consistent with their authoritarian model – gaining veto authority over other nations' economic, diplomatic, and security decisions."

In a January 2018 report, the Defense Innovation Unit Experimental (DIUx), an organization within DOD (now known as the Defense Innovation Unit) which is responsible for evaluating emerging technologies for the DOD, released a report assessing the effects of technology transfers on national security. Among its principal conclusions, the DIUx study found the following:

- Technology transfer to China occurs in part through increasing levels of investment and acquisitions of U.S. companies. China participated in approximately 16 percent of all venture deals in 2015, up from 6 percent average participation rate during 2010-2015.
- Investments are only one means of technology transfer, which also occurs through the following licit and illicit vehicles where the cost of stolen

intellectual property has been estimated at US\$300 billion per year.

- The United States does not have a comprehensive policy or the tools to address this massive technology transfer to China. The Committee on Foreign Investment in the United States (CFIUS) is one of the only tools in place today to govern foreign investments, but it was not designed to protect sensitive technologies. CFIUS is only partially effective in protecting national security given its limited jurisdiction.
- The U.S. government does not have a holistic view of how fast this technology transfer is occurring, the level of Chinese investment in U.S. technology, or what technologies we should be protecting.<sup>6</sup>

In its March 2018 Section 301 report, the Office of the United States Trade Representative (USTR) accused China of using inbound foreign ownership restrictions, such as joint venture requirements and foreign equity limitations, as well as its administrative licensing and approval process, to coerce U.S. companies to transfer technology.<sup>7</sup> According to the White House, inadequate intellectual property (IP) protection in China leaves the U.S. economy and other developed economies at significant risk.<sup>8</sup>

Congress has also expressed consistent bipartisan concern over the national security threats posed by China, particularly in relation to supply chains and the telecommunications sector. The Senate Intelligence Committee has emphasized the "national security risks associated with the advent of a domestic 5G network," as well as "the advanced and critical technology transfer campaign that China continues to conduct at the expense of the U.S."9 Similarly, the House Appropriations Committee has noted its concern with the "PRC's [People's Republic of China] efforts to dominate the 5G global market," and committed to "a coordinated strategy with allies and partners to provide alternatives to Chinese-financed telecommunication technology."10 Such actions align with the U.S.-China Commission's recent warning that "technology transfers and IP theft threaten to undermine U.S. technological development and capabilities both now and in the future," noting with distinct concern that China's development of certain foundational technologies, in particular, could have lasting effects.<sup>11</sup>





Congress is not simply raising concerns but is also considering various legislative proposals to counter the threat of Chinese acquisition of U.S. technology. Several proposed appropriations bills would prohibit executive agencies from acquiring telecommunications equipment from certain Chinese telecommunications companies.<sup>12</sup> Other proposals would require the USTR to report on products produced with support of China's Made in China 2025 industrial policy,13 prohibit the export of "national security sensitive technology" or intellectual property subject to U.S. jurisdiction,<sup>14</sup> and prevent certain public funds from being used to purchase any equipment or services from certain Chinese telecommunications companies.<sup>15</sup> While many of these measures align with the prerogatives of the Trump administration, others show a broader bipartisan consensus aimed at containing the growing economic and political influence of China.

### CFIUS: Expansion of restrictions on foreign investment from China

One of the most significant developments affecting Chinese access to U.S. technology has been the expansion of the U.S. government's authority to capture for review certain non-controlling foreign investments in U.S. businesses, including Chinese investments in such businesses, that CFIUS had previously been unable to review. The Trump administration, as well as the Obama administration before it, has aggressively used the CFIUS process to curb investment from China in certain key technology sectors and related access to intellectual property and know-how. In particular, Congress passed legislation in 2018 expanding the jurisdiction of CFIUS and making filings with CFIUS mandatory for certain foreign government-backed investments.

The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), a bipartisan effort, expanded CFIUS' jurisdiction in a number of areas, including non-controlling foreign investments in U.S. firms involved with critical technologies, critical infrastructure, or personally identifiable information. <sup>16</sup> Notably, FIRRMA is the most significant reform to CFIUS in over a decade and was largely driven by China's previous acquisition of advanced U.S. technologies. In particular,

although a number of these provisions of FIRRMA await implementation, CFIUS launched a pilot program to cover investments in certain industries involving critical technology. Under this program, CFIUS now has authority to review certain non-controlling investments in so-called pilot program industries, which include, among others, aerospace/defense, nuclear power, petrochemical manufacturing, telecommunications, battery manufacturing, nanotechnology, biotechnology, and semiconductors.<sup>17</sup> Most notably, this new pilot program mandates the submission of a filing for any controlling or non-controlling investment in a pilot program U.S. business, with steep penalties – including up to the value of the transaction – for a failure to file.18 Previously, CFIUS had not mandated any filings.

Even before the expansion of CFIUS' jurisdiction, the U.S. government had taken proactive steps to block Chinese investment in American companies where national security concerns existed. President Obama ordered the Chinese-owned Ralls Corporation to divest certain U.S. wind farm project companies in September 201219 and blocked the proposed acquisition of the U.S. assets of the German semiconductor company Aixtron by Chinese investors in 2016.20 Other deals have been withdrawn in lieu of having a transaction blocked. For example, in 2016, China's Fosun International Limited was pressured by CFIUS to divest itself of U.S. property and casualty insurer Ironshore Inc. over concerns of how Fosun would operate as the liability coverage provider for U.S. government employees even after the acquisition was complete.21

Under the current administration, in September 2017, President Trump blocked the acquisition of Lattice Semiconductor Corporation by Canyon Bridge Capital Partners – a corporation ultimately controlled by Chinese investors – due to the acquisition's threat "to impair the national security of the United States."<sup>22</sup> On March 12, 2018, President Trump blocked the attempted hostile takeover by Broadcom Limited, a then-Singaporean company, of Qualcomm Incorporated, in part because of concerns that the transaction would allow Chinese companies to dominate the 5G-standard setting process.<sup>23</sup> More recently, CFIUS forced Shenzhen-based iCarbonX to divest its stake in U.S.-based health tech start-

up PatientsLikeMe, prompting alarm throughout the start-up community. <sup>24</sup> Heavy CFIUS scrutiny of Chinese investments and Chinese restrictions on outbound investment have led to a precipitous drop in Chinese investment in U.S. companies, a trend unlikely to abate anytime soon. <sup>25</sup>

# Export controls: Broad use of export control authorities to counter Chinese influence and acquisition of strategic technologies

One of the principal tools the U.S. government has used to target China is the dual-use export control regime, which is administered by the Department of Commerce under its Export Administration Regulations (EAR). The administration has specifically turned its attention to China's ability to obtain advanced technology from U.S. companies and universities and has taken or is considering measures, including amendments to the EAR, which would restrict China's ability to obtain not only advanced strategic technology, but also emerging technologies that are not currently controlled. In addition, the Department of Commerce is targeting individual Chinese companies with designations that prohibit nearly all exports of U.S. items to such companies, as well as focusing its enforcement resources on Chinese companies and Chinese nationals who seek to illicitly acquire U.S. technology.

### Emerging and foundational technologies

The U.S. government is working to implement significant new regulations that would expand

restrictions on the transfer of certain emerging and foundational technology to China and other countries that are viewed as national security threats. The impact of these new restrictions, when implemented, is likely to be far reaching, affecting technical collaboration and research and development between U.S. and Chinese companies and universities.

On August 13, 2018, President Trump signed the John S. McCain National Defense Authorization Act (NDAA) for fiscal year 2019 into law. The NDAA included the Export Control Reform Act, which directed the secretaries of Defense, Energy, and State - along with other federal agencies as appropriate to identify "emerging and foundational technologies" that are "essential to the national security of the United States."26 Subsequently, in November 2018, the Commerce Department issued an advanced notice of proposed rule-making (ANPRM) that sought public comment on "criteria for defining and identifying emerging technologies."27 While no final rules have been published, the interagency process will eventually result in proposed rules for new export control classification numbers (ECCNs) on the Commerce Control List (CCL) that will, at minimum, impose licensing requirements for exports to countries subject to a U.S. arms embargo, such as China. The Commerce Department has indicated that it is initially focused on the sectors set forth in Box 1.

While the November 2018 ANPRM focused only on emerging technologies, a separate rulemaking on foundational technologies is expected in the near future. The Commerce Department has not yet defined what constitutes foundational technology or how such technology differs from emerging technology.



#### Emerging technology sectors identified by the Commerce Department:

- · Biotechnology, such as
  - nanobiology
  - synthetic biology
  - genomic and genetic engineering
  - neurotech
- Artificial intelligence (AI) and machine learning technology, such as
  - neural networks and deep learning (e.g., brain modeling, time series prediction, classification)
  - evolution and genetic computation (e.g., genetic algorithms, genetic programming)
  - reinforcement learning
  - computer vision (e.g., object recognition, image understanding)
  - expert systems (e.g., decision support systems, teaching systems)
  - speech and audio processing (e.g., speech recognition and production)
  - natural language processing (e.g., machine translation)
  - planning (e.g., scheduling, game playing)
  - audio and video manipulation technologies (e.g., voice cloning, deepfakes)
  - AI cloud technologies
  - AI chipsets
- Position, navigation, and timing technology.
- Microprocessor technology, such as
  - systems-on-chip
  - stacked memory on chip
- · Advanced computing technology, such as
  - memory-centric logic
- Data analytics technology, such as
  - visualization
  - automated analysis algorithms
  - context-aware computing
- Quantum information and sensing technology, such as
  - quantum computing

- quantum encryption
- quantum sensing
- Logistics technology, such as
  - mobile electric power
  - modeling and simulation
  - total asset visibility
  - distribution-based logistics systems
- Additive manufacturing (e.g., 3D printing)
- · Robotics, such as
  - micro-drone and micro-robotic systems
  - swarming technology
  - self-assembling robots
  - molecular robotics
  - robot compilers
  - smart dust
- Brain-computer interfaces, such as
  - neural-controlled interfaces
  - mind-machine interfaces
  - direct neural interfaces
  - brain-machine interfaces
- Hypersonics, such as
  - flight control algorithms
  - propulsion technologies
  - thermal protection systems
  - specialized materials (for structures, sensors, etc.)
- · Advanced materials, such as
  - adaptive camouflage
  - functional textiles (e.g., advanced fiber and fabric technology)
  - biomaterials
- Advanced surveillance technologies, such as
  - Faceprint and voiceprint technologies
- Other general technology categories that warrant review to identify emerging technology that are important to U.S. national security.



#### Technology transfer to Chinese nationals

The U.S. government has significant concerns regarding the acquisition of export-controlled technology by Chinese nationals working or studying in the United States. The Commerce Department – as well as other agencies such as the Department of Homeland Security, Department of Justice, and Federal Bureau of Investigation (FBI) – is closely scrutinizing Chinese employees working, or seeking to work, for U.S. companies in certain industries, as well as Chinese students at U.S. universities, to identify unlawful transfers of technology.

In particular, U.S. companies are reporting that there has been a slowdown in the processing of authorizations from the Commerce Department for transfers of controlled technology to Chinese employees in the United States. <sup>28</sup> Under the EAR's so-called "deemed export" rule, a foreign person in the United States requires an export license from the Commerce Department to access controlled technology if an export license is required to export such technology to the foreign person's home country. <sup>29</sup> We understand that the Commerce Department is closely reviewing such "deemed export" license applications resulting in delays or outright denials.

The enforcement arms of the Commerce Department, the FBI, and the Department of Homeland Security are also engaged in outreach visits to companies and universities that have Chinese national employees and/or students. While the purported purpose of these visits is to educate industry and the academic community about threats from foreign persons attempting to unlawfully acquire sensitive U.S. technology, the combined impact of licensing delays and outreach visits, as well as scrutiny of visa applications, is having a chilling effect on the hiring and retention of Chinese nationals in the United States.

#### **Designation of Chinese companies**

There has been a substantial increase in additions of Chinese entities to the Bureau of Industry and Security's (BIS) Entity List and Unverified List, thereby greatly restricting the designated entities' ability to transact in U.S.-origin products or products containing more than a de minimis amount of U.S. content that render them subject to U.S. laws. Notable examples of designations include:

- August 2018 addition of 44 Chinese parties, including large state-owned enterprises and their subsidiaries and research institutes involved in the semiconductor industry to the Entity List.<sup>30</sup>
- October 2018 addition of state-owned semiconductor manufacturer Fujian Jinhua Integrated Circuit Company, Ltd. to the Entity List. <sup>31</sup>
- April 2019 addition of 37 entities, including prominent Chinese universities, to the Unverified List.<sup>32</sup>
- May 2019 addition of telecommunications giant Huawei and 68 of its non-U.S. affiliates in 26 destinations to the Entity List.<sup>33</sup>
- June 2019 addition of 5 Chinese organizations involved in supercomputing to the Entity List. 34

As the Trump administration continues to increase pressure against China, further additions are expected.

#### **Enforcement against Chinese companies**

Over the past several years, the Commerce Department and other agencies have actively increased enforcement against Chinese companies and individuals seeking to obtain export controlled items unlawfully. Several federal agencies have indicated that Chinese attempts to illicitly acquire U.S. technology are an enforcement priority, including:

- Secretary of Commerce Wilbur Ross, following the January 2019 indictment of Huawei and its CFO, stated, "For years, Chinese firms have broken our export laws and undermined sanctions, often using U.S. financial systems to facilitate their illegal activities. This will end. The Trump Administration continues to be tougher on those who violate our export control laws than any administration in history."35
- Department of Justice announced its China Initiative to combat threats to national security from Chinese state actors, as discussed below.<sup>36</sup>
- Department of Homeland Security has increased investment in technologies and public-private partnerships to combat Chinese cyber threats, and recently reorganized its cybersecurity division under the Cybersecurity and Infrastructure Security Agency.<sup>37</sup>

"For years, Chinese firms have broken our export laws and undermined sanctions, often using U.S. financial systems to facilitate their illegal activities. This will end. The Trump Administration continues to be tougher on those who violate our export control laws than any administration in history"

- Secretary of Commerce, Wilbur Ross

### Expansion of restrictions on nuclear exports to China

With around 46 operational nuclear power reactors and reportedly 11 more under construction, China is a major market for U.S. nuclear suppliers.<sup>38</sup> Despite the size of the Chinese nuclear market, the U.S. government has imposed new export control restrictions that are intended to significantly limit civil nuclear cooperation with China. These new restrictions involve the Department of Energy (DOE), which administers controls on the export of nuclear technology and assistance, including civil nuclear power reactor and nuclear fuel technology; and the U.S. Nuclear Regulatory Commission (NRC), which administers control of the export of tangible nuclear items, including civil nuclear power reactor components, equipment, and nuclear materials.

Prompted by "concerns about China's efforts to obtain nuclear material, equipment, and advanced technology from U.S. companies," in October 2018, DOE developed a new policy framework that restricts nuclear technology exports to China under 10 C.F.R. part 810.<sup>39</sup> Notably, the new framework establishes a "presumption of denial" of certain exports to China, including:

- Exports related to light water Small Modular Reactors.
- Non-light water advanced reactors.
- New technology transfers after January 1, 2018.
- Any transfer to China General Nuclear (CGN) and/or CGN subsidiaries or related entities.<sup>40</sup>

Based on the above policy, DOE will continue to authorize technology transfers to China to support projects that were authorized prior to 2018, but any new cooperation with China, including collaboration on advanced reactor development, will be denied. In addition, the NRC instituted a presumption of denial for licenses for any exports to China of nuclear reactor components, equipment, and nuclear materials that involve direct economic competition with the United States or that involve CGN and/or its subsidiaries.<sup>41</sup>

### Targeting Chinese involvement in the U.S. telecommunications system

As mentioned previously, in 2018 Congress passed the John S. McCain National Defense Authorization Act for Fiscal Year 2019 specifically banning the heads of executive agencies from procuring services and equipment from specified Chinese companies.<sup>42</sup> The legislation notably targets certain Chinese telecommunications companies (including Huawei), severely limiting the extent to which federal agencies can use their products and services. Specifically, section 889 prohibits executive agencies from using equipment or services provided by certain Chinese telecommunications companies, and from entering into contracts with entities that use equipment or services from such companies as "a substantial or essential component of any system, or as critical technology as part of any system."43 The Office of Management and Budget (OMB) has stated that it may take two years to implement the procurement ban, and is seeking approval from Congress to defer implementation of the ban on grants and subsidies to rural carriers for up to four years.44

More recently, in May 2019, the Trump administration issued a new executive order (EO) aimed at bolstering the government's efforts to combat "malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people." The EO specifically targets the information and communications sectors, permitting the government to bar the acquisition and use of equipment, software, and technology from certain "foreign adversaries." While the EO does not specifically mention China, it is widely understood that the EO is intended to target Huawei and possibly other Chinese companies.

The EO directs the Secretary of Commerce, in consultation with other agencies, to implement rules to prohibit transactions that involve "information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" and that pose one of the following undue risks:

1. Risk of "sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of

- information and communications technology or services in the United States."
- 2. Risk of "catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States."
- 3. A transaction that "otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons."<sup>47</sup>

These prohibitions broadly apply to "acquisition[s], importation, transfer[s], installation, dealing[s] in, or use of any information and communications technology or service" that are determined to pose risks to the national security or critical infrastructure of the United States.<sup>48</sup>

The Department of Commerce, in consultation with other agencies, is required to publish rules or regulations implementing the EO within 150 days of May 15, 2019, the date of the EO. The EO also directs all other agencies of the federal government to take all appropriate measures within their authority to carry out the provisions of the EO.<sup>49</sup>

### Department of Justice's initiative to counter Chinese intellectual property theft and enforce export controls

In November 2018, the DOJ launched its China Initiative to counter Chinese national security threats, including attempts by China to obtain U.S. export controlled technology and intellectual property. The press release announcing the initiative listed 10 primary components:

- 1. Identify priority trade secret theft cases, ensure that investigations are adequately resourced, and work to bring them to fruition in a timely manner and according to the facts and applicable law.
- 2. Develop an enforcement strategy concerning nontraditional collectors (e.g., researchers in labs, universities, and the defense industrial base) that are being coopted into transferring technology contrary to U.S. interests.

- 3. Educate colleges and universities about potential threats to academic freedom and open discourse from influence efforts on campus.
- 4. Apply the Foreign Agents Registration Act to unregistered agents seeking to advance China's political agenda, bringing enforcement actions when appropriate.
- 5. Equip the nation's U.S. Attorneys with intelligence and materials they can use to raise awareness of these threats within their districts and support their outreach efforts.
- 6. Implement the Foreign Investment Risk Review Modernization Act (FIRRMA) for DOJ (including by working with Treasury to develop regulations under the statute and prepare for increased workflow).
- 7. Identify opportunities to better address supply chain threats, especially ones impacting the telecommunications sector, prior to the transition to 5G networks.
- 8. Identify Foreign Corrupt Practices Act (FCPA) cases involving Chinese companies that compete with American businesses.
- 9. Increase efforts to improve Chinese responses to requests under the Mutual Legal Assistance Agreement (MLAA) with the United States.
- 10. Evaluate whether additional legislative and administrative authorities are required to protect our national assets from foreign economic aggression.<sup>50</sup>

The same day that the department announced this initiative, it also announced charges against stateowned Fujian Jinhua Integrated Circuit Company, Ltd. and Taiwan-based United Microelectronics Corporation (UMC), alleging theft of intellectual property from U.S.-based Micron Technology Inc. (DRAM technology).<sup>51</sup> The case is currently being litigated in the Northern District of California, and if convicted, each company faces forfeiture and a maximum fine of more than US\$20 billion. This criminal case followed on the heels of the Commerce Department placing Fujian Jinhua on the Entity List, denying the company access to U.S. goods, components, and technology. This case is notable because this appears to be the first time the Commerce Department has designated a company

on the Entity List for intellectual property theft. Such assertive measures further signal key efforts by the Trump administration to work across various departments and agencies to collectively confront what it views as the national security threat posed by China's economic rise and continued acquisition of vital U.S. technologies.

### Use of trade-related measures to counter Chinese influence

In addition to the measures described above, the Trump administration has made vigorous use of traditional trade measures, such as tariffs, to counter the perceived threat that China poses to the economic and national security of the United States. The use of these measures demonstrates the Trump administration's willingness to use all available trade and national security tools to pressure China.

Following instructions from the president, on August 18, 2017, USTR initiated an investigation under Section 301 of the Trade Act of 1974 (Section 301 Report) of China's acts, policies, and practices related to technology transfer, intellectual property, and innovation. During this same period, in January 2018, President Trump imposed his first round of safeguard tariffs under Section 202 of the Trade Act of 1974 on imported washing machines and solar cells and modules. Shortly thereafter in March 2018, the administration implemented tariffs on steel and aluminum imports under Section 232 of the Trade Expansion Act of 1962, finding that continued unabated imports would impair the national security of the United States.

On March 22, 2018, USTR issued its 301 Report findings, concluding that certain "acts, policies, and practices [of the Chinese government] related to technology transfer, intellectual property, and innovation" were "unreasonable or discriminatory and burden or restrict U.S. commerce."<sup>54</sup>

Specifically, the Section 301 Report highlighted China's conduct in four main areas:

1. Use of "foreign ownership restrictions, such as joint venture (JV) requirements and foreign equity limitations, and various administrative review

- and licensing processes, to require or pressure technology transfer from U.S. companies."
- 2. Use of "technology regulations forces U.S. companies seeking to license technologies to Chinese entities to do so on non-market based terms that favor Chinese recipients."
- 3. Facilitation of "systematic investment in, and acquisition of, U.S. companies and assets by Chinese companies to obtain cutting-edge technologies and intellectual property and generate the transfer of technology to Chinese companies."
- 4. Support of "unauthorized intrusions into, and theft from, the computer networks of U.S. companies to access their sensitive commercial information and trade secrets."

In response, President Trump issued a memorandum calling for swift action against China "to address the acts, policies, and practices of China that are unreasonable or discriminatory and that burden or restrict U.S. commerce." <sup>56</sup> The memorandum directed USTR to publish a proposed list of products and any intended tariff increases and to pursue dispute settlement in the World Trade Organization (WTO), while directing the Secretary of the Treasury to address concerns about investment in the United States directed or facilitated by China in industries and technologies deemed important to the United States.

Over the following months, the USTR proposed and implemented three series of tariff increases:

- "List 1" items, worth approximately US\$35 billion, imposed an additional 25 percent duty of specified Chinese goods and went into effect on July 6, 2018.<sup>57</sup>
- "List 2" items, worth approximately US\$16 billion, subjected certain specified goods to an additional 25 percent tariff and went into effect on August 23, 2018.<sup>58</sup>
- "List 3" items, worth approximately US\$200 billion, subjected certain specified goods to an additional 10 percent duty that went into effect September 24, 2018, with an increase to 25 percent originally scheduled for January 1, 2019. This tariff increase was initially delayed following a meeting between President Trump and President

Xi on the sidelines of the G20 summit in December 2018. However, after trade talks began to stall in the first half of 2019, the Trump administration reinstituted the increase on May 10, 2019.<sup>59</sup>

Despite the ongoing dialogue between the United States and China and growing concern over the economic impact that such tariffs may have on the U.S. economy, the administration has shown few signs of easing its approach of using tariffs to pressure China.

### Considerations for global companies moving forward

The U.S. government's robust approach to countering China is having wide-ranging impacts on global companies, including on global supply chains, technology transfers involving China, sales to China, and investment from Chinese companies. Taken together, the patchwork of various national security measures against China, implemented by multiple agencies under different legal authorities, represents a significant compliance challenge for global companies. When approaching business relationships with Chinese entities, companies should be mindful of not only current regulatory requirements, but also the potential future measures involving China that could further restrict business activities. We set forth below a number of considerations for global companies doing business in China or with Chinese companies.

 Closely monitor export control, trade, and CFIUS developments related to China. It is critical that companies closely monitor U.S. government announcements and actions related to China to identify any national security measures that could affect their global operations. Given the ongoing trade negotiations with China and efforts of various agencies within the federal government, as well as proposed legislation in Congress to target Chinese companies, the legal and regulatory landscape is evolving rapidly and is prone to abrupt change. Companies should establish processes to regularly assess and address risks to their global operations from new or proposed national security measures against China. This can be implemented both at the board of directors

- level and/or at the management level using risk committees and other structures.
- Carefully assess any proposed investment from or joint ventures with Chinese companies. Companies should carefully consider any proposed investment from or joint ventures with companies ultimately owned by Chinese interests. Companies should assess well in advance of concluding agreements with Chinese companies whether any U.S. or non-U.S. legal restrictions or requirements would apply to the agreements or related activities, including CFIUS and export control requirements, and whether it makes commercial sense to pursue such agreements in light of current and potential new restrictions. This is particularly true given that certain filings with CFIUS are now mandatory and need to be filed 45 days in advance of closing. In addition, any technology transfers or access to technology under the agreement should be vetted carefully. Companies should consider ways to expand the involvement of export control compliance personnel or attorneys in the consideration of agreements or partnerships with Chinese companies as early as possible to avoid wasting time and resources on transactions that ultimately cannot proceed or are unlikely to be successful.
- Implement robust diligence measures regarding business relationships with Chinese companies, including supply, purchase, distribution, and research and development agreements. Companies should implement robust due diligence practices with regard to transactions involving Chinese companies, such as thoroughly assessing affiliations with restricted parties, including companies or organizations on the Entity List and other lists; identifying any operations or transactions in sanctioned countries involving the Chinese partner; determining whether the transaction involves export-controlled items including controlled technology; assessing cybersecurity threats; and confirming the Chinese company's understanding of and commitment to compliance with U.S. export control and economic sanctions laws.



- Include strong trade compliance provisions in agreements with Chinese companies.
  - Companies should negotiate robust trade compliance provisions in agreements with Chinese companies, including prohibiting diversion to sanctioned countries or restricted parties and confirming that Chinese partners are not themselves restricted parties or owned or controlled by restricted parties. Companies should also include language in contracts to permit immediate termination in the event of designation as a restricted party. Additionally, companies should consider including provisions for audit rights in contracts with potential Chinese partners (and should exercise such audit rights periodically) to confirm compliance with applicable export control and economic sanctions laws.
- Carefully review all exports, reexports, or transfers of commodities, software, and technology to Chinese companies. Given the U.S. government scrutiny on China-related transactions, it is imperative that global companies comply with U.S. export control and economic sanctions laws when dealing with Chinese companies. Companies should confirm that any China-related transactions are subject to effective and verifiable export control and sanctions-related compliance policies and procedures. They should also prioritize their China-related transactions and operations for trade compliance assessments and trainings. Specifically, companies should consider questions such as:
  - Have all of the items and technology involved in the transaction been classified for export control purposes?

- Do the activities at issue require export licenses or other authorizations?
- Has the company built in enough lead time for a license application if required?
- Is the company vulnerable to potential new controls on emerging technology?
- Does the transaction raise any reputational and political sensitivities in the United States or other countries?
- Review company's cybersecurity plan specifically with regard to interactions with Chinese partners to protect IP. Companies should periodically assess their cybersecurity plans and confirm that they are adequate in light of their interactions with Chinese partners. Companies should have a clear protocol for addressing any cybersecurity incidents that occur, including a plan for reviewing, remediating, and possibly disclosing to relevant authorities any exfiltration of export-controlled technology by Chinese threat actors.

#### Conclusion

While it remains to be seen whether or not the broader U.S.-China trade negotiations will produce a new trade regime that eases bilateral tensions, the Trump administration has made clear through myriad avenues that it does not intend to lessen economic pressure on China any time soon. By intertwining national security concerns with traditional trade and intellectual property protection measures, the Trump administration has positioned itself to forcefully counter growing Chinese influence through a variety of measures.

#### **Authors and contacts**



**Ajay Kuntamukkala**Partner, Washington, D.C.
T: 1 202 637 5552
ajay.kuntamukkala@hoganlovells.com



Chris R. Mullen Associate, Washington, D.C. T: 1 202 637 6687 chris.mullen@hoganlovells.com

#### **Endnotes**

- \* Special thanks to Andrea Fraser-Reid and Greg Hawkins for their contributions to this piece.
- 1. Office of the U.S. Trade Representative, Update Concerning China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation 7 (Nov. 20, 2018), available <a href="here">here</a> [hereinafter USTR REPORT UPDATE]. Specifically, USTR found industrial sectors including "aerospace, information and communications technology, robotics, industrial machinery, new materials, and automobiles" contributed to or directly benefited from the Made in China 2025 policy. Id. See also 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 (Mar. 22, 2018), available <a href="hereinafter SECTION">here [hereinafter SECTION 301 REPORT]</a> (explaining USTR's initial investigation findings).
- Press Release, Office of the U.S. Trade Representative, USTR Issues
   Tariffs on Chinese Products in Response to Unfair Trade Practices
   (June 15, 2018) (quoting United States Trade Representative Robert Lighthizer), available <a href="here">here</a>.
- 3. SECTION 301 REPORT, *supra* note 1 (quoting Memorandum of August 14, 2017 Addressing China's Laws, Policies, Practices, and Actions Related to Intellectual Property, Innovation, and Technology, 82 Fed. Reg. 39,007, 39,007 (Aug. 14, 2017)) ("China has implemented laws, policies, and practices and has taken actions related to intellectual property, innovation, and technology that may encourage or require the transfer of American technology and intellectual property to enterprises in China or that may otherwise negatively affect American economic interests.").
- Department of Defense, Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge 1 (2018), available <a href="here">here</a>.
- 5. Id. at 2.
- Defense Innovation Unit Experimental (DIUX), China's Technology
   Transfer Strategy: How Chinese Investments in Emerging Technology
   Enable a Strategic Competitor to Access the Crown Jewels of U.S.
   Innovation 3-4 (Jan. 2018) (emphasis removed), available <a href="here">here</a>.
- 7. See SECTION 301 REPORT, supra note 1, at 19.
- 8. See White House Office of Trade and Mfr. Policy, How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World 6-8 (2018), available <a href="here">here</a>; see also European Chamber, China Manugacturing 2025: Putting Industrial Policy Ahead of Market Forces 24 (2017), available <a href="here">here</a>.
- 9. S. REP. NO. 116-20, at 11-12 (2019).
- 10. H.R. REP. NO. 116-78, at 111 (2019).

- Sean O'Connor, U.S.-China Econ. & SEC. Review Comm'n, How Chinese Companies Facilitate Technology Transfer from the United States 11 (2019), available <a href="here">here</a>.
- 12. See, e.g., H.R. 21, 116th Cong. § 432 (2019); H.R. 264, 116th Cong. § 632 (2019); H.R. 266, 116th Cong. § 432 (2019); H.R. 267, 116th Cong. § 420 (2019).
- 13. S. 2, 116th Cong. § 101 (2019).
- 14. Id. at § 102.
- 15. S. 1625, 116th Cong. § 4 (2019).
- 16. See CFIUS Legislation Takes Final Form, Moves Closer to President's Desk, Hogan Lovells 3 (July 30, 2018), available <a href="here">here</a>.
- 17. Determination and Temporary Provisions Pertaining to a Pilot Program to Review Certain Transactions Involving Foreign Persons and Critical Technologies, 83 Fed. Reg. 51,322, 51,322-34 (Oct. 11, 2018) [hereinafter CFIUS Pilot Program]; see CFIUS Legislation Takes Final Form, Moves Closer to President's Desk, supra note 16, at 3.
- 18. CFUIS Pilot Program, *supra* note 17, at 51,332-33; *see New Regulations Expand CFIUS' Jurisdiction and Mandate Filings*, Hogan Lovells 1 (Oct. 12, 2018), available <a href="here">here</a>.
- 19. Order of September 28, 2012 Regarding the Acquisition of Four U.S. Wind Farm Project Companies by Ralls Corporation, 77 Fed. Reg. 60,281, 60,281-83 (Oct. 3, 2012).
- 20. Order of December 2, 2016 Regarding the Proposed Acquisition of a Controlling Interest in Aixtron SE by Grand Chip Investment GmbH, 81 Fed. Reg. 88,607, 88,607-08 (Dec. 7, 2016).
- 21. See Greg Roumeliotis, RPT-INSIGHT-U.S. Watchdog Expands Scrutiny to More Chinese Deals, Reuters (Oct. 11, 2016), available here.
- 22. Order of September 13, 2017 Regarding the Proposed Acquisition of Lattice Semiconductor Corporation by China Venture Capital Fund Corporation Limited, 82 Fed. Reg. 43,665, 43,665-66 (Sept. 13, 2017).
- 23. Order of March 12, 2018 Regarding the Proposed Takeover of Qualcomm Incorporated by Broadcom Limited, 83 Fed. Reg. 11,631, 11,631-32 (Mar. 15, 2018).
- 24. See Christina Farr & Ari Levy, The Trump Administration Is Forcing This Health Start-Up that Took Chinese Money into a Fire Sale, CNBC (Apr. 4, 2019), available here.
- 25. E.g., Jodi Xu Klein, *Chinese Acquisitions of US Companies Plunge* 95 Per Cent in 2018 Amid Trade War, S. China Morning Post (Jan. 8, 2019), available here.
- 26. See H.R. 5515, 115th Cong. § 1758 (2018).
- Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201, 58,201 (Nov. 19, 2018).

- 28. See Wendy Wu, Casualties of Trade War: Chinese in US Denied
  Licences to Work with Sensitive Technologies, S. China Morning Post,
  (Mar. 12, 2019), available <a href="here">here</a>.
- 29. 15 C.F.R. § 734.13(b) (2019).
- 30. Addition of Certain Entities; and Modification of Entry on the Entity List, 83 Fed. Reg. 37,423, 37,423-33 (Aug. 1, 2018).
- 31. Addition of an Entity to the Entity List, 83 Fed. Reg. 54,519, 54,519-21 (Oct. 30, 2018).
- 32. Revisions to the Unverified List (UVL), 84 Fed. Reg. 14,608, 14,608-14 (Apr. 11, 2019).
- 33. Addition of Entities to the Entity List, 84 Fed. Reg. 22,961, 22,961-67 (May 21, 2019). Note that BIS has issued a Temporary General License, permitting some exports, reexports, and transfers to Huawei for a limited period. *See* Temporary General License, 84 Fed. Reg. 23,468, 23,468-71 (May 22, 2019).
- 34. Addition of Entities to the Entity List and Revision of an Entry on the Entity List, 84 Fed. Reg. 29,371, 29,371-75 (June 24, 2019).
- 35. Press Release, Department of Justice, Chinese Telecommunications Conglomerate Huawei and Huawei CFO Wanzhou Meng Charged with Financial Fraud (Jan. 28, 2019), available <a href="here">here</a>.
- 36. Press Release, Department of Justice, Deputy Assistant Attorney General Adam S. Hickey of the National Security Division Delivers Remarks at the Fifth National Conference on CFIUS and Team Telecom (Apr. 24, 2019), available here.
- 37. Center for New American Security, China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses (Dec. 12, 2018), available <a href="here">here</a>.
- 38. Power Reactor Information System: China, People's Republic of, IAEA (June 9, 2019), available <a href="here">here</a>.
- 39. Press Release, Department of Energy, DOE Announces Measures to Prevent China's Illegal Diversion of U.S. Civil Nuclear Technology for Military or Other Unauthorized Purposes (Oct. 11, 2018), available here.
- 40. U.S. Policy Framework on Civil Nuclear Cooperation with China, Department of Energy (Oct. 11, 2018), available <a href="here">here</a>.
- 41. See id.
- 42. H.R. 5515, 115th Cong. § 889 (2018).
- 43. Id.
- 44. Letter from Russell T. Vought, Acting Dir., Office of Mgmt. & Budget to Honorable Michael R. Pence, President of the Senate (June 4, 2019), available <a href="https://example.com/here/bence/">here</a>.

- 45. Exec. Order 13873 of May 15, 2019 Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22,689, 22,689 (May 17, 2019).
- 46. Id.
- 47. Id. at 22,690.
- 48. Id. at 22,689.
- 49. Id. at 22,690-92.
- 50. Press Release, Department of Justice, Attorney General Jeff Session's [sic] China Initiative Fact Sheet (Nov. 1, 2018), available here.
- 51. Press Release, Department of Justice, PRC State-Owned Company, Taiwan Company, and Three Individuals Charged with Economic Espionage (Nov. 1, 2018), available <a href="here">here</a>.
- 52. Proclamation 9693 of January 23, 2018 To Facilitate Positive Adjustment to Competition From Imports of Certain Crystalline Silicon Photovoltaic Cells (Whether or Not Partially or Fully Assembled Into Other Products) and for Other Purposes, 83 Fed. Reg. 3541, 3541-51 (Jan. 23, 2018) (describing solar cells and modules tariffs); Proclamation 9694 of January 23, 2018 To Facilitate Positive Adjustment to Competition from Imports of Large Residential Washers, 83 Fed. Reg. 3553, 3553-62 (Jan. 25, 2018).
- 53. Proclamation 9705 of March 8, 2018 Adjusting Imports of Steel into the United States, 83 Fed. Reg. 11,625, 11,626 (Mar. 15, 2018) (imposing steel tariffs); Proclamation 9704 of March 8, 2018 Adjusting Imports of Aluminum into the United States, 83 Fed. Reg. 11,619, 11,620 (Mar. 15, 2018) (imposing aluminum tariffs).
- 54. SECTION 301 REPORT, supra note 1, at 17.
- 55. USTR REPORT UPDATE, *supra* note 1, at 3-4; see also SECTION 301 REPORT *supra* note 1 (detailing alleged Chinese conduct).
- 56. Presidential Memorandum on the Actions by the United States Related to the Section 301 Investigation (March 22, 2018), available <u>here</u>.
- 57. Notice of Action and Request for Public Comment Concerning Proposed Determination of Action Pursuant to Section 301: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation, 83 Fed. Reg. 28,710, 28,710-56 (June 20, 2018).
- 58. Notice of Action Pursuant to Section 301: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation, 83 Fed. Reg. 40,823, 40,823-37 (Aug. 16, 2018).
- 59. Notice of Modification of Section 301 Action: China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation, 83 Fed. Reg. 20,459, 20,459-60 (May 9, 2019).

Alicante

Amsterdam

Baltimore

Beijing

Birmingham

Boston

Brussels

Budapest\*

Colorado Springs

Denver

Dubai

Dusseldorf

Frankfurt

Hamburg

Hanoi

Ho Chi Minh City

Hong Kong

Houston

Jakarta \*

Johannesburg

London

Los Angeles

Louisville

Luxembourg

Madrid

Mexico City

Miami

Milan

Minneapolis

Monterrey

Moscow

Munich

New York

Northern Virginia

Paris

Perth

Philadelphia

Riyadh\*

Rome

San Francisco

São Paulo

Shanghai

Shanghai FTZ\*

Silicon Valley

Singapore

Sydney

Tokyo

Ulaanbaatar\*

Warsaw

Washington, D.C.

Zagreb\*

Associated offices\*

Legal Services Center: Berlin

### www.hoganlovells.com

"Hogan Lovells" or the "firm" is an international legal practice that includes Hogan Lovells International LLP, Hogan Lovells US LLP and their affiliated businesses.

The word "partner" is used to describe a partner or member of Hogan Lovells International LLP, Hogan Lovells US LLP or any of their affiliated entities or any employee or consultant with equivalent standing. Certain individuals, who are designated as partners, but who are not members of Hogan Lovells International LLP, do not hold qualifications equivalent to members.

For more information about Hogan Lovells, the partners and their qualifications, see www. hoganlovells.com.

Where case studies are included, results achieved do not guarantee similar outcomes for other clients. Attorney advertising. Images of people may feature current or former lawyers and employees at Hogan Lovells or models not connected with the firm.

© Hogan Lovells 2019. All rights reserved. 04953