Tech Wars: National Security-Based Restrictions on Foreign Access to U.S. Technology

By Hdeel Abdelhady | October 19, 2018 | Published in Law360

Amidst the myriad trade confrontations, realignments, and rules reconfigurations between the United States and China, the European Union, Mexico, Canada, Japan, South Korea, and others, the links—clear and tenuous—between national security, trade, and business have become more apparent.

Relative to its predecessors, the Trump Administration appears to have fewer discernible qualms about invoking "national security' to justify retaliatory or preemptive trade measures—namely tariffs—to remediate "unfair" trade practices or direct trade outcomes.[1] This has not gone without challenge. In response to steel and aluminum tariffs, an industry group filed suit in the United States Court of International Trade challenging the constitutionality of Section 232 of the Trade Expansion Act of 1962.[2] And, some of the President's co-partisans in Congress have called for legislation limiting the President's national security-based tariffs authority.[3]

But in other areas, in particular the maintenance of the United States' global technological edge, there is agreement between and among the Executive Branch and Congress that measures to restrict foreign access to U.S. technology are necessary and appropriate on national security grounds. Cutting-edge and critical technologies are of acute interest to the Administration, Congress members, and policy influencers. These technologies include artificial intelligence (perhaps of foremost concern), technology that has clear or expected military applications, and "emerging technologies critical to economic growth and security" as identified in the Trump Administration's inaugural National Security Strategy (**NSS**), including: "autonomous technologies, gene editing, new materials, nanotechnology, [and] advanced computing technologies."[4]

In this environment, the technology industry—which has operated in a fairly light touch regulatory climate owing in no small part to the basic inability of the law to keep pace with technological innovation—is now at the center of legal and policy measures designed to protect U.S. technology from foreign access and influence, particularly where such foreign access would threaten U.S. technology dominance or otherwise serve foreign strategic aims.

Measures to curb foreign access to U.S. technology have taken and will likely take various forms that will cut across industries and legal disciplines. Among them, as discussed below, are restrictions on foreign access to and influence on U.S. technology through (1) foreign investment, (2) supply chain exclusions, (3) limits on participation in academic and other research, (4) legal or

political curbs on U.S. technology access or transfers through third countries, and (5) countermeasures against foreign control of raw materials essential to technological manufacturing and innovation.

(1) Restrictions on Foreign Investment in U.S. Technology

Enacted on August 13, 2018, the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (**NDAA**) includes measures to curb foreign access to and influence on U.S. technology.[5] Key among them are the Foreign Investment Risk Review and Modernization Act of 2018 (**FIRRMA**), the FIRRMA-related Export Control Reform Act of 2018 (**ECRA**), and other provisions that effect, among other outcomes, the supply chain exclusions discussed below.

FIRRMA, which has been covered fairly extensively in legal and business publications (and is therefore treated cursorily here), expands the jurisdiction of the Committee on Foreign Investment in the United States (**CFIUS**) to, on national security grounds, review and potentially block foreign direct and indirect investment in "critical technologies," as well as "emerging and foundational" technologies to be defined later pursuant to the ECRA.[6]

(2) Supply Chain Exclusions Through Federal Procurement Prohibitions

The NDAA contains provisions that effectively leverage the procurement power of the federal executive branch to freeze out certain foreign entities from participating in public and private sector technology supply chains in the United States. For example, the NDAA prohibits executive agencies from directly or indirectly procuring telecommunications and video surveillance equipment and services produced by certain named companies (all Chinese) and entities that use the same equipment or services "as a substantial or essential component of any system, or as critical technology as part of any system."[7]

With the prohibition on indirect procurement of certain foreign company provided equipment and services, the NDAA potentially excises targeted foreign firms from private sector supply chains, as companies that will want to do business with federal executive agencies (or their providers) will be required to exclude foreign targeted firms from some or all of their provider pipelines.[8]

Beyond the named Chinese firms, the NDAA provides scope for further prohibitions on procurement with or involving equipment or services provided by additional firms (Chinese or other), as the Secretary of Defense, in consultation with the Director of National Intelligence or the Director of the FBI, may identify for restriction equipment or services provided by entities that he or she "reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a foreign country."[9]

(3) Limits on Foreign Student and Corporate Participation in Academic and Other Research

Several reports this year have indicated that the Trump Administration is seeking to limit foreign participation in scientific research in academic and perhaps other settings, including through visa restrictions and export controls. For example, the New York Times reported in April that the

Related MassPoint Publications

- U.S. Law as Trade War Weapon
- U.S.-China Trade and Tech War on Three Fronts
- ZTE: Was the Export Ban the Right Penalty?
- Threat of Sanctions for Chinese Firms Shows Tech Company Human Rights Accountability Risks
- Critical Minerals: Where National Security, Trade and Environmental Laws Will Meet
- Glencore FCPA Investigation, a Canary in the Cobalt Mine
- Proposals to Curb Foreign Investment in the United States Gaining Steam After the U.S. Election
- After Election 2016: 5 Legal and Business Issues to Watch in 2017
- U.S. Senators Raise National Security Concerns About Foreign Investment in U.S. Real Estate

Administration was considering restrictions on Chinese researchers over "espionage concerns."[10] According to the report, the White House discussed "whether to limit the access of Chinese citizens [excluding permanent residents and asylum grantees] . . . by restricting certain types of visas" and adopting measures to "clamp down on collaboration in advanced materials, software and other technologies at the heart of Beijing's [Made in China 2025] plan to dominate cutting-edge technologies like advanced microchips, artificial intelligence, and electric cars." In addition to visa restrictions, the Trump Administration was reportedly considering expanding the scope of goods and services that would be subject to deemed export controls, effectively requiring U.S. companies and universities to "obtain special licenses for Chinese nationals."

Such measures would be consistent with the Trump Administration's policy pronouncements. The National Security Strategy states that the "United States will review visa procedures to reduce economic theft by non-traditional intelligence collectors . . . [and] consider restrictions on foreign STEM students from designated countries to ensure that intellectual property is not transferred to our competitors."[11] Relatedly, in a May 2018 statement, the White House reported that the "United States will continue efforts to protect domestic technology and intellectual property . . . [including by stopping] noneconomic transfers of industrially significant technology and intellectual property to China."[12] The White House statement does not define "noneconomic transfers," but the term would appear to potentially encompass technology transfers to foreign nationals through research in academic or other settings.[13]

In addition, lawmakers have sounded alarms on foreign corporate affiliations with university research. For example, in June, 26 members of Congress urged the Secretary of Education to, among other actions, "immediately request (and require) information from . . . [over 50] U.S. universities involved in [research partnerships with Huawei Technologies], especially those receiving any federal research funding . . . to gather information related to whether any such funding is involved in a Huawei partnership, and whether any research personnel (including Chinese nationals . . .) are involved in these efforts."[14]

The potential for restrictions on foreign individual and corporate participation in academic or other research should be monitored, including because concerns about "academic espionage" exist

outside of (and predate) the Trump Administration, including among some Congress members and policy influencers.

(4) Curbs on U.S. Technology Access or Transfers Through Third Countries, Formalized Cooperation With Allies on Foreign Investment

Just this month, Senators Marco Rubio and Mark Warner—both members of the Senate Select Committee on Intelligence (Senator Warner is the Ranking Member)—sent a letter to Canadian Prime Minister Trudeau to express "grave concerns about the possibility that Canada might include Huawei Technologies or any other Chinese state-directed telecommunications company in its fifth generation (5G) telecommunications network infrastructure."[15] Owing to the United States and Canada's "strong alignment" in spectrum management and membership in the "Five Eyes" intelligence alliance (with Australia, New Zealand, and the United Kingdom) Canada's potential inclusion of Chinese "state-directed firms" in its 5G networks has, according to the senators, implications for U.S. security.

Beyond ad hoc efforts to influence third country decisions on foreign involvement in technology architecture, FIRRMA directs the Treasury Secretary (as chair of CFIUS) to "establish a formal process for the exchange of information . . . with governments of countries that are allies or partners of the United States . . . to protect the national security of the United States and those countries."[16] Thus, FIRRMA's impact is likely to be felt, through a more formalized process, globally.[17]

(5) Countermeasures to Foreign Influence on U.S. Technology Through Control of Essential Industrial Inputs

On December 20, 2017, the President issued Executive Order 13817, entitled "A Federal Strategy To Ensure Secure and Reliable Supplies of Critical Minerals," finding that the United States' heavy reliance on certain mineral commodities imports "vital to the Nation's security and economic prosperity" constituted a "strategic vulnerability for both [the U.S.] economy and military."[18] In May, pursuant to EO 13817, the Department of Interior published the Final Critical Minerals list, which enumerates 35 mineral commodities deemed "vital to the Nation's security and economic prosperity." Among the listed inputs are minerals essential to technology development and manufacturing, such as cobalt (used in electric vehicle batteries) and rare earth elements (used in batteries and consumer electronics).

The publication of the Critical Minerals list and additional actions (taken and expected) are designed to reduce the United States' reliance on foreign (and unstable) sources critical nonfuel minerals. Actions toward this end may include, in addition to measures to green light critical minerals mining in the United States, national security-based reviews of foreign-source minerals, including under national security provisions of trade laws.[19]

Considerations and Takeaways

In a recent "60 Minutes" interview, the President took issue with the description of the U.S.-China tariff confrontation as a "trade war." "I consider it a skirmish," he said.[20] Whether back and forth tariffs between the U.S. and China rise to the level of trade war can be debated. What is clearer is that, compared to the unfolding race for future technology dominance, issues concerning tariffs are of lesser complexity and long-term strategic importance.

While China is and likely will remain for the foreseeable future the focus of U.S. measures to maintain technological dominance, other countries may, as future events require, become the subject of the same or similar policy concerns currently focused on China.

Finally, while the Trump Administration—owing to its substantive policies, actions, and style—has brought issues of foreign access to U.S. technology to the fore, interested parties should bear in mind that the concerns addressed by the measures outlined above are held by policy and lawmakers outside the Administration and existed well before the Trump Administration (or the Trump candidacy) came into being. Accordingly, national security-based measures to control or restrict foreign access to U.S. technology, in some shape or form, are likely to outlast the Trump Administration.

In the meantime, Trump Administration's willingness to use U.S. law creatively to achieve international trade and economic goals introduces an element of unpredictability for parties seeking to monitor, anticipate, and make sense of developments.[21] This environment counsels in favor of holistic methods to identify and synthesize legal, regulatory, and policy events, free from the substantive constraints and inefficiencies of siloed legal practice area or single industry approaches.

***

Hdeel Abdelhady is Principal at MassPoint Legal and Strategy Advisory PLLC. She teaches a law school course in Regulation of Foreign Access to U.S. Technology.

NOTES

[1] Bloomberg provides a useful table of "notable" (and few) Section 232 investigations conducted by prior administrations that resulted in protective measures (per Department of Commerce data): Thomas Biesheuvel et al., *Trade as National Security Issue? Here's What the U.S. Law Says, Bloomberg*, May 24, 2018 (updated July 10, 2018), at https://www.bloomberg.com/news/articles/2018-05-24/trade-as-national-security-issue-here-s-the-u-s-law-quicktake.

[2] In June, the American Institute for International Steel and two of its member companies challenged, in the United States Court of International Trade, the constitutionality of Section 232 as an over-broad delegation of discretionary authority by Congress to the President. *See, e.g.*, *American Institute for International Steel Files Lawsuit Challenging Constitutionality of Section 232 steel tariffs*, June 27, 2018, at http://www.aiis.org/2018/06/american-institute-for-international-steel-files-lawsuit-challenging-constitutionality-of-section-232-steel-tariffs/.

[3] *See, e.g.*, Jenny Leonard et al., *Senate Considers Ways to Limit Trump's Authority on Tariffs*, Bloomberg, June 26, 2018, at https://www.bloomberg.com/news/articles/2018-06-26/senate-considers-ways-to-limit-trump-s-national-security-tariffs.

[4] White House, National Security Strategy, Dec. 2017, 20 (discussing, as part of "Pillar II: Promote Economic Prosperity," the Administration's plans to "maintain . . . [the United States'] competitive advantage"). On the strategic significance of artificial intelligence, there is widespread agreement and a sense of urgency. As the Russian President stated: "Artificial intelligence is the future . . . for all humankind . . . Whoever becomes the leader in this sphere will become the ruler of the world." Gregory C. Allen, *Putin and Musk are right: Whoever masters AI will run the world*, Sept. 5, 2017, at https://www.cnn.com/2017/09/05/opinions/russia-weaponize-ai-opinion-allen/index.html.

[5] John S. McCain National Defense Authorization Act for Fiscal Year 2019, P. Law No. 115-232 (Aug. 13, 2018).

[6] Foreign Investment Risk Review and Modernization Act of 2018, §§ 1701-28 of the NDAA, at § 1703(a)(6).

[7] NDAA at § 889. The named companies are, in the telecommunications category, Huawei and ZTE (and their subsidiaries and affiliates) and, in video surveillance category, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company (and their subsidiaries and affiliates). The probation on direct procurement takes effect one year from the date of the NDAA's enactment and the prohibition on indirect procurement takes effect two years from the NDAA's enactment. *Id.*

Notably, some Congress members have recently called for the imposition of Global Magnitsky Sanctions on Hikvision and Dahua, for their alleged provision to the Chinese government of surveillance equipment used by the Chinese government to carry out abuses of Uighur and other minority groups in China's Xinjiang Province. *See, e.g.*, MassPoint Legal and Strategy Advisory PLLC, *Threat of Sanctions for Chinese Firms Shows Tech Company Human Rights Accountability Risks*, Aug. 30, 2018, at https://masspointpllc.com/world-wide-web-of-tech-supply-chain-risk/.

[8] The relevant NDAA provisions allow for limited waivers. Heads of executive agencies may, on a "one-time basis" waive for up to two years the NDAA's indirect procurement prohibitions "with respect to an entity that requests such a waiver," subject to certain waiver eligibility requirements. In addition, the Director of National Intelligence may provide a waiver, only after the NDAA prohibitions take effect, if he or she determines that waiver is "in the national security interests of the United States." NDAA at § 889(d).

[9] *Id.* at § 889(f)(3)(D).

[10] Ana Swanson and Keith Bradsher, *White House Considers Restricting Chinese Researchers Over Espionage Fears*, N.Y. Times, April 30, 2018, at https://www.nytimes.com/2018/04/30/us/politics/trump-china-researchers-espionage.html.

[11] NSS at 22.

[12] White House, *Statement on Steps to Protect Domestic Technology and Intellectual Property from China's Discriminatory and Burdensome Trade Practices*, May 29, 2018, at https://www.whitehouse.gov/briefings-statements/statement-steps-protect-domestic-technology-intellectual-property-chinas-discriminatory-burdensome-trade-practices/.

[13] A more recent report stated that "White House hawks" recently "encouraged" the President to "stop providing visas to Chinese nationals." The President reportedly demurred. But opponents of the proposal were, according to the same report, "worried that the president might return to the issue, particularly as he takes an increasingly tough line on China over everything from trade to cyber security." Demitri Sevastopulo and Tom Mitchell, *US considered ban on student visas for Chinese nationals*, Financial Times, Oct. 2, 2018, https://www.ft.com/content/fc413158-c5f1-11e8-82bf-ab93d0a9b321.

[14] Release, Office of Senator Marco Rubio, *Rubio, Banks Raise Concerns of Chinese Espionage Through University Partnerships with Huawei*, June 20, 2018, at https://www.rubio.senate.gov/public/index.cfm/2018/6/rubio-banks-raise-concerns-of-chinese-espionage-through-university-partnerships-with-huawei. The Congress members also urged DeVos to arrange for a classified FBI and Director of National Intelligence briefing "on Huawei and Chinese technology acquisition modalities in general" and "immediately convene a senior-level working group to understand how the People's Republic of China attempts to gather U.S. technology on U.S. university and college campuses and to develop recommendations . . . for protecting the U.S. technology advantage."

[15] Release, Office of Senator Marco Rubio, *Rubio, Warner Urge Canadian Prime Minister Trudeau To Reconsider Huawai* [sic] *Inclusion in Canada's 5G Network*, Oct. 12, 2018, at https://www.rubio.senate.gov/public/index.cfm/press-releases?id=EBDC659C-93D6-4620-B3B8-E17F82A80A2A.

[16] FIRRMA at § 1713(3).

[17] FIRRMA's import in this regard is the formalization of cooperation with allied countries. Before FIRRMA, the United States had influence on foreign investment in third countries. For example, in 2016 President Obama blocked a Chinese company's proposed acquisition of German chip maker Aixtron (which had a U.S. subsidiary and engaged in interstate commerce in the United States).

[18] *See, e.g.*, MassPoint PLLC, *Critical Minerals: Where National Security, Trade and Environmental Laws Will Meet*, August 15, 2018.

[19] *Id.*

[20] CBS News, *President Trump on Christine Blasey Ford, his relationships with Vladimir Putin and Kim Jong Un and more*, Oct. 15, 2018, at https://www.cbsnews.com/news/donald-trump-full-interview-60-minutes-transcript-lesley-stahl-2018-10-14/.

[21] *See, e.g.*, Hdeel Abdelhady, *US Law As Trade War Weapon*, Law360, May 21, 2018, at https://www.law360.com/articles/1045372/us-law-as-trade-war-weapon.