Expert Analysis

What Academia Must Know About DOJ's China Initiative

By **Hdeel Abdelhady**
January 28, 2019, 4:01 PM EST

"China wants the fruits of America's brainpower to harvest the seeds of its planned economic dominance. Preventing this from happening will take all of us ... across the U.S. government, and within the private sector."

—Assistant Attorney General for National Security John Demers[1]

"No country presents a broader, more severe threat to our ideas, our innovation and our economic security than China."

—FBI Director Christopher Wray[2]

Hdeel Abdelhady

The confrontation between the United States and China is not just a traditional "trade war" centered on tariffs. More consequentially, the two countries are in the early stages of a tech war: a race to develop or dominate emerging technologies deemed critical to future economic, industrial and military positioning and leadership. These emerging technologies include artificial intelligence, robotics, nanotechnology and advanced computing.[3]

On national security grounds, the United States is developing and implementing a whole-of-government approach to maintain the country's technological edge through legal and policy measures to restrict Chinese access to U.S. technology and intellectual property, including by: (1) limiting or prohibiting certain foreign investment and commercial transactions; (2) adopting export controls on emerging technologies; (3) instituting supply chain exclusions; (4) curbing participation in academic and other research; and (5) combating cyber intrusions and industrial and academic espionage.[4] Additionally, concerns about Chinese government influence have spurred proposals to regulate the activities of entities viewed as Chinese government influence operators.

While the Trump administration has raised the temperature on relevant economic and national security issues, the whole-of-government approach reflects concerns across the executive branch, within Congress and among policy influencers that predate the Trump administration.

DOJ China Initiative: Objectives and Working Group, Jeff Sessions' Departure

The U.S. Department of Justice recently launched an initiative to "combat Chinese

economic espionage." Announced on Nov. 1, 2018, by then-Attorney General Jeff Sessions, the China Initiative, according to a DOJ fact sheet, acts on the Trump administration's previous findings "concerning China's practices" and "reflects the Department's strategic priority of countering Chinese national security threats and reinforces the President's overall national security strategy."[5]

The China Initiative is led by the DOJ's National Security Division, which "is responsible for countering nation state threats to the country's critical infrastructure and private sector."[6] The DOJ Criminal Division will "aggressively investigate Chinese companies and individuals for theft of trade secrets."[7] In addition to the Federal Bureau of Investigation, five U.S. attorneys are original members of the China Initiative Working Group: from Massachusetts, the Northern District of Alabama, the Northern District of California, the Eastern District of New York and the Northern District of Texas.

The involvement of U.S. attorneys for Massachusetts and the Northern District of California is not surprising, given that Boston and Northern California, for example, are significant technology and IP centers.[8] The membership of the U.S. attorneys for the Eastern District of New York and the Northern District of Texas is more interesting, and likely harnesses those districts' experience in enforcement against Chinese technology giants ZTE, in the Northern District of Texas, and Huawei, in the Eastern District of New York.[9]

As the China Initiative is part of a whole-of-government approach to deemed national security threats posed by China, the departure of Jeff Sessions is unlikely to slow or diminish the initiative.

China Initiative Components: Enforcement, Regulation and Private Sector Engagement

The China Initiative is composed of 10 "components," some of which are outward-facing and others of which are inward-facing (i.e., capacity building within the DOJ). Broadly, the outward-facing components are of three types: (1) enforcement actions, (2) regulation and monitoring and (3) engagement with the private sector, including academia. Three components of the China Initiative most relevant to academic and research institutions are discussed here.

Academic and Industrial Espionage Countermeasures: Nontraditional Collectors

The DOJ will "develop an enforcement strategy concerning nontraditional collectors (e.g., researchers in labs, universities and the defense industrial base) that are being co-opted into transferring technology contrary to U.S. interests."[10] The "co-opted" language here is noteworthy for its ambiguity and potentially wide scope. For example, a plain reading of the language suggests that a "co-opted" "nontraditional collector" need not knowingly engage in "espionage" or technology transfers in a manner that is illicit or contrary to U.S. interests.

This prong of the China Initiative appears to respond largely to concerns about "academic

espionage," which have been raised for years but appear to have gained steam in 2017 and 2018. For example, the Trump administration's National Security Strategy, published in December 2017, identifies countering academic espionage as a priority.[11] The same concerns have gained currency among Congress members and those who influence them.[12]

The Trump administration has sought to curb foreign participation in U.S. academic research by indirect means, such as by imposing or proposing limits on foreign student (particularly Chinese) visas.[13] Universities, research institutions and others affected by the DOJ's focus on nontraditional collectors should seek clarification as to the scope of nontraditional collector targets and underlying premises. For example, would Chinese students whose studies are funded by the Chinese government be considered "co-opted" or so susceptible to being co-opted that they could be, presumptively, targets? Or is a broader premise at work?

Similar questions might apply to non-Chinese nationals who engage in paid or nonpaid work or collaboration with or on behalf of Chinese government or government-affiliated entities, such as those who participate in the Thousand Talents Plan (which has come under scrutiny, with some also suggesting that participants be required to register as foreign agents under the Foreign Agents Registration Act).

"Threats to Academic Freedom and Open Discourse From Influence Campaigns"

The China Initiative seeks to "educate colleges and universities about potential threats to academic freedom and open discourse from influence efforts on campus."[14] Targets of this prong of the initiative might include, for example, entities like the Confucius Institute, as well as Chinese companies that are, or are believed to be, state-owned or acting on behalf of the Chinese government.

Chinese government influence on U.S. academia has been highlighted as a national security threat. Corporate sponsorship of university research by Chinese companies (which are believed by some to be acting on behalf of the Chinese government, even if not government-owned) has been flagged as a national security challenge, as have nonprofit and educational institutions affiliated with the Chinese government.[15] As indicated above, an example is the Confucius Institute (understood to be present at over 100 university locations the United States), which lawmakers and others want to have registered as a foreign agent under FARA (including as part of legislation introduced in Congress).

Apply the Foreign Agents Registration Act to "Unregistered Agents Seeking to Advance China's Political Agenda"

Enacted in 1938 to regulate Nazi propaganda and related activities in the United States, FARA requires, inter alia, natural and legal persons acting or purporting to act on behalf of foreign principals — government and private — in "political" or "quasi-political" capacities to register with the DOJ as foreign agents. FARA's text is expansive enough to apply to

activities that do not or may not appear to be “political” or “quasi-political” (including potentially certain business and advocacy activities).

FARA has gained visibility since the 2016 presidential election, as persons affiliated with the Trump campaign have been accused of or prosecuted for being unregistered foreign agents. FARA’s higher profile has resulted in efforts to apply the law to a wide range of actors, such as to nonprofit organizations engaged in international environmental advocacy and to Chinese government and associated parties.[16]

Academic institutions, research institutes and other parties that host or engage with the Confucius Institute on campus or otherwise, have faculty or personnel who engage or collaborate with the Chinese government or entities perceived to arms of the Chinese state, and those engaged in research and technological development (such as incubators and accelerators) should, as a starting point, educate and train their leadership and relevant personnel on FARA and proposals to potentially apply the law to their environments.

Recommended Action for Academic and Research Institutions

The DOJ’s China Initiative is understood to advance national security objectives of high priority to the U.S. government. Given the United States’ focus on preserving its technological edge, including by curbing Chinese access to U.S. IP and technology (in cases of illicit and lawful access, such as by investment), the reasons for the DOJ China Initiative’s applicability to academic and research environments that birth and nurture technological innovation are clear.

Academic and research institutions should take steps to understand the China Initiative in the context of broader U.S.-China dynamics, seek clarification and develop compliance and other response plans that consider its potential interplay with and implications for, inter alia, academic freedom and privacy in light of applicable law, academic policies and institutional culture. As appropriate at the institutional level, such efforts should involve administrative, legal, research integrity/export controls and other relevant personnel at leadership and other levels.

More proactive measures — such as the development of advocacy strategies to inform the content and tone of legal and policy measures — might be more appropriate for entities that engage (at the institutional level or through faculty and students) with China and Chinese parties; host or collaborate with the Confucius Institute or other entities deemed influence operators; receive corporate or other support from Chinese companies or other entities; or enroll or host students or researchers who are Chinese nationals.

Given the importance of international cooperation and foreign student enrollment — including Chinese student enrollment — to many U.S. colleges and universities, the reasons for proactive engagement by academia are compelling.[17]

Hdeel Abdelhady is principal attorney at MassPoint Legal and Strategy Advisory PLLC, and teaches a course on regulation of foreign access to U.S. technology at The George Washington University Law School.

[1] Department of Justice, Attorney General Jeff Sessions's China Initiative Fact Sheet, Nov. 1, 2018 ("Fact Sheet").

[2] Id.

[3] See, e.g., MassPoint PLLC, Commerce Begins Rulemaking on Emerging Technologies Essential to National Security, Nov. 27, 2018 ("Commerce Emerging Technologies"), and U.S.-China Trade and Tech War on Three Fronts, May 21, 2018.

[4] See, e.g., Hdeel Abdelhady, Trade Wars: Restricting Foreign Access To US Technology, Law360, Oct. 19, 2018, at https://www.law360.com/tax-authority/articles/1093803/trade-wars-restricting-foreign-access-to-us-technology (explaining that as to "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") ("Abdelhady") and Commerce Emerging Technologies.

[5] Fact Sheet.

[6] Id.

[7] Id.

[8] The Northern District of California is involved in a trade secret theft case against a Taiwanese company, a Chinese state-owned firm and three individuals accused of, among other things, stealing the trade secrets of Micron Technology Inc., a U.S. company.

[9] See, e.g., DOJ Release, ZTE Corporation Agrees to Plead Guilty and Pay Over $430.4 Million For Violating U.S. Sanctions By Sending U.S.-Origin Items to Iran, at https://www.justice.gov/usao-ndtx/pr/zte-corporation-agrees-plead-guilty-and-pay-over-4304-million-violating-us-sanctions (detailing that, inter alia, ZTE entered a guilty plea to sanctions violations and other offenses in the Northern District of Texas) Mar. 7, 2017; Emily Rauhala, Huawei executive wanted by U.S. faces fraud charges related to Iran

sanctions, could face 30 years in prison, Washington Post, Dec. 7, 2018, at https://www.washingtonpost.com/world/the_americas/huawei-executive-wanted-by-us-scheduled-for-bail-hearing-in-canada/2018/12/07/0a08c602-fa31-11e8-863a-8972120646e0_story.html?utm_term=.101d5c48e8ac. Separately, it should be noted that Huawei has been under investigation for sanctions violations for years, and will likely face enforcement involving multiple U.S. agencies (particularly by the DOJ, the Office of Foreign Assets Control and the Department of Commerce) at the corporate level in the foreseeable future. For more on the ZTE case and discussionof the Trump Administration's approach to sanctions enforcement, 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.

[10] Fact Sheet.

[11] See, e.g., Abdelhady ("The National Security Strategy states that the 'United States will review visa procedures to reduce economic theft by nontraditional intelligence collectors ... [and] consider restrictions on foreign STEM students from designated countries to ensure that intellectual property is not transferred to our competitors.' 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] For example, in April 2018, two subcommittees of the House Committee on Science, Space, and Technology held a joint hearing entitled "Scholars or Spies: Foreign Plots Targeting America's Research and Development," the purposes of which were to, inter alia, "explore foreign nationals' exploitation of U.S. academic institutions for the purposes of accessing and engaging in exfiltration of valuable science and technology research and development." House Committee on Science, Space, and Technology, Hearing Charter, Oversight Subcommittee and Research and Technology Subcommittee joint hearing, April 4, 2018, available at https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-115-SY21-20180411-SD001.pdf.

[13] See, e.g., Commerce Emerging Technologies, Nov. 27, 2018, at https://masspointpllc.com/emerging-technologies-export-controls-rulemaking/ (indicating that the Department of Commerce's early proposed rulemaking as to potential export controls on "emerging technologies" excludes fundamental research and noting that other methods for restricting fundamental research may be pursued).

[14] Fact Sheet.

[15] See, e.g., Abdelhady, discussing objections by U.S. senators to Chinese corporate sponsorship of U.S. university research, particularly by Huawei. Concerns about Huawei's and other Chinese companies' "espionage" and/or links to the Chinese government (particularly Chinese intelligence) have affected academic institutions outside of the United

States. Earlier this month, for example, Oxford University announced that it would "'not pursue new funding opportunities'" with Huawei, "'in the light of public concerns raised in recent months surrounding UK partnerships with Huawei.'" BBC News, Oxford University suspends Huawei donations and sponsorships, Jan. 17, 2019, at https://www.bbc.com/news/business-46911265.

[16] For example, in July 2018, the House Committee on Natural Resources sent letters to two U.S.-based nonprofit organizations — the Natural Resources Defense Council and the Center for Biological Diversity — questioning whether their foreign activities and relationships require registration under the Foreign Agents Registration Act.

[17] It was reported recently, for example, that a U.S. university has secured insurance against declines in Chinese student enrollment. See, e.g., MassPoint PLLC, US-China Risks to American Academia Are So Real They Are Insurable, Dec. 27, 2018.