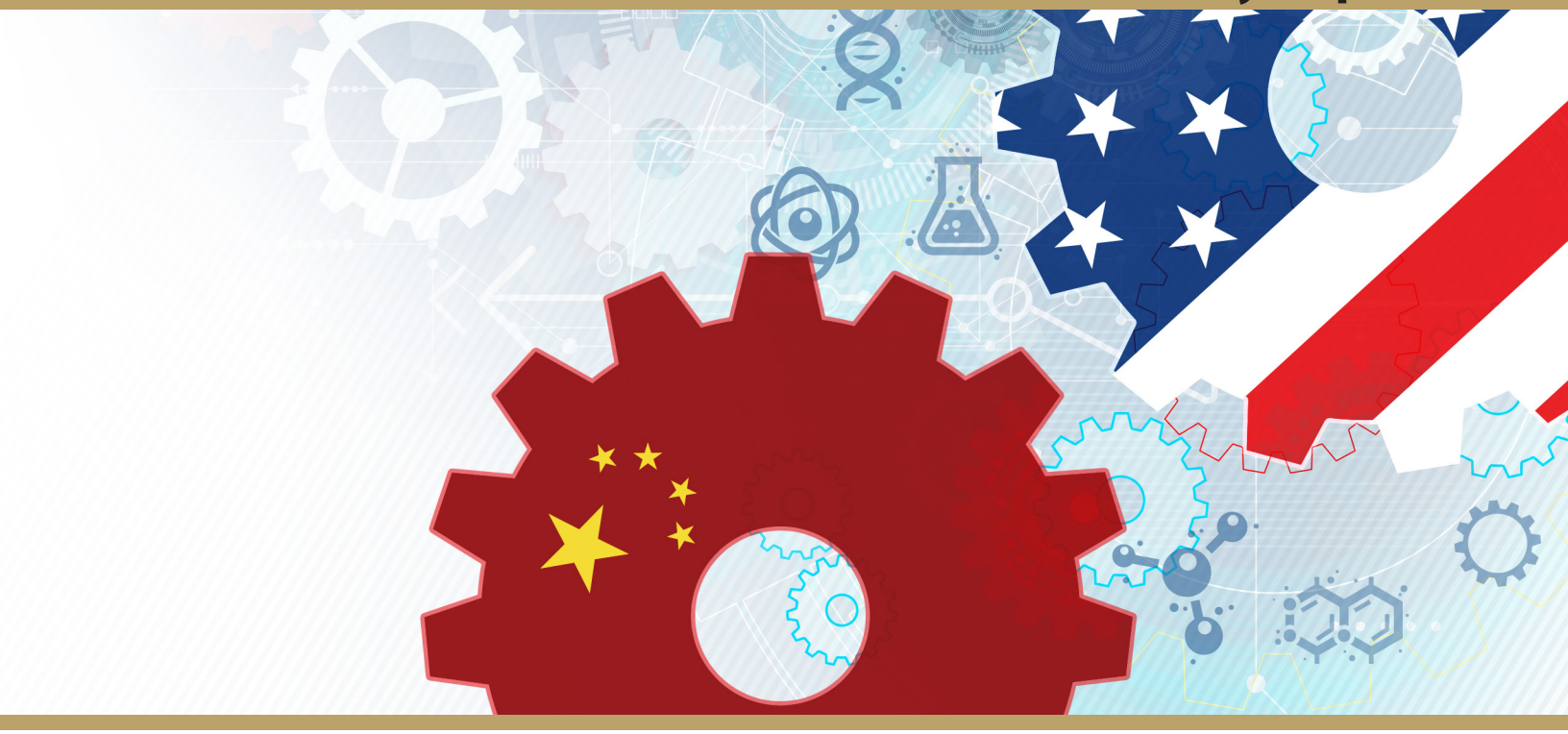
ADDRESSING THE CHINA CHALLENGE FOR AMERICAN UNIVERSITIES

National Security Report



Rory Truex

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

ADDRESSING THE CHINA CHALLENGE FOR AMERICAN UNIVERSITIES

Rory Truex

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY

The views in this document reflect the opinions of the author alone and do not represent any institutional position held by APL.

NSAD-R-20-062

Contents

Tables

Foreword

This paper is part of the "Measure Twice, Cut Once: Assessing Some China–US Technology Connections" research series sponsored by the Johns Hopkins University Applied Physics Laboratory.

As competition has intensified between the United States and China, actions to disengage their technology establishments from one another have also intensified. The two countries' systems for research and development, production, and sale of cutting-edge technologies have been substantially, though by no means uniformly, commingled. More recently, there have been concerted efforts by both nations' governments to reverse some or all of that commingling. Policymakers' priorities include perceived risks to national security, worry about economic disadvantage from proliferation, and concern about uses of technologies that intentionally or indifferently may harm civil liberties or the environment.

To explore the advisability and potential consequences of decoupling, the Johns Hopkins University Applied Physics Laboratory commissioned papers from experts in specific technology areas. In each of these areas, the authors have explored the feasibility and desirability of increased technological separation and offered their thoughts on a possible path forward. Other papers in this series include:

- *Two Worlds, Two Bioeconomies: The Impacts of Decoupling US–China Trade and Technology Transfer* by Rob Carlson and Rik Wehbring
- *The History and Future of US–China Competition and Cooperation in Space* by Matthew Daniels
- *Symbiosis and Strife: Where Is the Sino–American Relationship Bound? An Introduction to the APL Series "Measure Twice, Cut Once: Assessing Some China–US Technology Connections"* by Richard Danzig and Lorand Laskai
- *An Entwined AI Future: Resistance Is Futile* by Christine Fox
- *Cutting off Our Nose to Spite Our Face: US Policy toward Huawei and China in Key Semiconductor Industry Inputs, Capital Equipment, and Electronic Design Automation Tools* by Douglas B. Fuller
- *The Telecommunications Industry in US–China Context: Evolving toward Near-Complete Bifurcation* by Paul Triolo
- *US–China STEM Talent "Decoupling": Background, Policy, and Impact* by Remco Zwetsloot

Summary

Members of the US government have expressed concern that the Chinese government is targeting American researchers and labs for espionage and theft of information with commercial, military, and intelligence value. There are also separate concerns about inappropriate relationships between US researchers and Chinese institutions and the flow of human capital from US research institutions back to China.

This paper—one of two commissioned on science, technology, engineering, and mathematics (STEM) issues—argues that there is insufficient evidence that academic/economic espionage by Chinese nationals is a widespread problem at US universities. After 20 months of ongoing investigations, the "China Initiative"—a Department of Justice (DOJ) effort—has brought formal charges at only ten US universities or research institutions, and only three cases involved any evidence of espionage, theft, or transfer of intellectual property. Given about 107,000 Chinese citizens in STEM at US universities at the graduate level or above, current DOJ charges imply a criminality rate in this population of .0000934, less than 1/10,000. Given this evidence, we can consider ways to enhance research security at US universities but should be especially wary of overcorrections. Current solutions, which rely on mass visa restrictions and heightened monitoring of Chinese researchers, are counterproductive and will harm American science and national security in the long term.

Efforts to improve research security should proceed from these principles: First, no policy should foster systematic discrimination against a population based on its ethnicity or nation of origin. Second, policies must recognize the importance of foreign-born researchers—and Chinese researchers in particular—to the US economy and US universities, which are themselves of strategic importance. Third, we must acknowledge that our model of science has unavoidable vulnerabilities with respect to plagiarism, economic espionage, and other forms of theft. Within this framework, US universities and the government can cooperate in addressing security threats from China in a way that is mutually beneficial and consistent with academic values.

In particular, these policy solutions would enhance research security while maintaining a welcoming environment for Chinese researchers and minimizing the possibility of discrimination.

(1) **A No Dual-Salary Rule:** No full-time employee of an American university should receive salary or substantial compensation from the government or military of, or a university or firm in, a country of high strategic concern.

(2) **Centralized Disclosure:** The US government should work with universities to create a standardized, centralized disclosure system for faculty professional activities and conflicts of interest. The system can include an audit component conducted by the National Science Foundation.

(3) **Pretravel Counterintelligence Training:** US citizens traveling to China as part of an academic exchange should receive pretravel training from the US government on issues relating to Chinese espionage and elicitation practices.

(4) **The No Surveillance Rule:** US universities and their employees should not be expected to engage in monitoring or surveillance on behalf of the law enforcement community.

The paper will proceed in five parts. First, I will briefly overview the components of the Open Science Model, a set of principles that guide the conduct of research in the natural and social sciences at top US research universities. Second, I will outline the challenges posed by scientific collaboration between the United States and China, specifically threats to US national security and technological supremacy. This section also includes an assessment of the severity of the research security problem. Third, I will outline a set of principles that should govern policymaking on this issue. Fourth, I will review recent policy developments in this area. Fifth, I will propose four policy ideas that could protect US interests while remaining consistent with American and academic values.

The Open Science Model and US Science

Research and development (R&D) in the United States occurs in a range of sectors. This report focuses on universities, which spent $75 billion on R&D in 2018. This represents about 13 percent of total R&D expenditures in the United States ($580 billion in 2018). About 73 percent of US R&D occurs in the private sector, with the remaining research occurring in federal, state, and local governments (about 10 percent) and nonprofits (4.2 percent).

R&D activities can be categorized as basic research, applied research, and development. Basic research aims to "acquire new knowledge of the underlying foundations of a phenomena," while applied research focuses on a "specific practical aim or objective." Development is research directed at improving products or processes.[1] Universities are the engines of basic research in the United States, while the private sector conducts the vast majority of applied research and development. See Table 1, which is reproduced from Sargent (*U.S. Research and Development*).

Most STEM faculty in US universities focus on basic research, and they conduct their research in accordance with the Open Science Model. In Box 1, I summarize key features of Open Science.

The primary alternative to the Open Science Model is classified research, where access to research output and materials is restricted to certain personnel who have been vetted by the US government.[2] The research is not produced for public consumption, not widely disseminated in the scholarly community, not open for replication, and not subject to double-blind peer review. Many top universities—Stanford, UC Berkeley, Princeton, and Harvard, to name a few—do not allow faculty to conduct classified research on their campuses.[3] Research can also be subject to intellectual property protections, nondisclosure agreements, and other barriers to the dissemination of knowledge short of full classification.

Open Science is derived from the scientific method itself and is essential to the scientific enterprise. This model is the key driver of technological innovation at American universities, which remain the

[1] Sargent, *U.S. Research and Development*.

[2] One possible approach is to erect "intermediate-level boundaries" around certain research areas, such as using designations like "Controlled Unclassified Information" (CUI). This category was established in 2008 to replace a range of other informal, intermediate designations ("For Official Use Only [FOUO]," etc.), but it has yet to be systematically delineated for academic research and is not reconciled with National Security Decision Directive 189 (NSDD-189; JASON, *Fundamental Research Security*). I agree with the recommendations of the JASON report that research should have either high barriers (classified) or no barriers at all (open) and that the creation of intermediate categories would cause confusion and be counterproductive. The recently proposed Secure Campus Act creates such a category—"sensitive research"—that does not map well to the standards of NSDD-189.

[3] The existing model accords with what former Defense Secretary Robert Gates has termed a "small yard, high fence" approach—we should be selective in choosing technologies that merit protection, and we should be aggressive in protecting them (Laskai and Sacks, "America's Innovation Advantage").

Table 1. US R&D Performance by Sector and Character (2018) (Current Dollars, in Billions)

	Basic Research		Applied Research		Development		Total	
	Dollars	Percent	Dollars	Percent	Dollars	Percent	Dollars	Percent
Federal government	11.1	11.5	20	17.4	27.1	7.3	58.2	10.0
Nonfederal government	0.1	0.1	0.5	0.4	0.0	0.0	0.6	0.1
Business	26.2	27.2	65.6	57.0	330.3	89.6	422.1	72.8
Higher education	46.6	48.3	20.8	18.1	7.3	2.0	74.7	12.9
Other nonprofit	12.5	12.9	8.0	7.0	3.9	1.0	24.3	4.2
Total	**96.5**	**100**	**115**	**100**	**368.5**	**100**	**580**	**100**

Reproduced from Table 2 in Sargent (*U.S. Research and Development*).

top research institutions in the world.[4] The Reagan administration endorsed this model of inquiry in National Security Decision Directive 189 (NSDD-189),[5] which was released in 1985 in response to intelligence gathering efforts by Eastern bloc countries at American laboratories and universities. The directive states that "our leadership position in science and technology is an essential element in our economic and physical security" and affirms that American science requires "an environment in which the free exchange of ideas is a vital component."[6] According to existing regulations, where possible, fundamental research produced in US universities, labs, and other research institutions is to remain unrestricted. Proprietary research can be classified or otherwise restricted where appropriate.[7]

Under the Open Science Model, preventing citizens of a certain country from accessing research is effectively impossible. This would require, among other measures, restricting graduate and postdoctoral admissions based on country of origin; restricting conference attendance based on citizenship or instituting background checks; not publishing research or working papers; and not posting replication materials. Such measures are either illegal, harmful to the American innovation system, or both.

As described in the 2019 report by JASON—an independent advisory group of elite scientists—many of the security threats emanating from China can be considered violations of norms of research integrity.

The Open Science Model carries inherent vulnerabilities. Some degree of plagiarism or theft of intellectual property is inevitable, as there is little—other than research integrity and reputational sanctions—preventing a researcher from stealing ideas. This is a risk each researcher bears when circulating early-stage work, collaborating with students and postdoctoral researchers, and posting replication materials. The National Institutes of

[4] McKiernan et al., "Point of View"; and Woelfle, Olliaro, and Todd, "Open Science."

[5] White House, *National Security Decision Directive 189*.

[6] White House, *National Security Decision Directive 189*, 1.

[7] "'Fundamental research' means basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons" (White House, *National Security Decision Directive 189*).

Box 1. Features of the Open Science Model

Open Access—Research output is published and posted for public consumption. Readers can access reports for free or by paying a small fee.

Replication—Where possible, underlying materials (data sets, code, etc.) are made publicly available to facilitate replication and future research.

Peer Review—Research is published after peer review, where editors can send a submitted working paper or grant application to any other academic for anonymous review without knowledge of the authors.

Early-Stage Collaboration—Early-stage research and working papers are circulated and presented widely. Conferences are often open to anyone willing to pay a registration fee.

Nondiscrimination—Admission to labs, conferences, and PhD programs is determined on merit, without consideration of the citizenship or ethnicity of the researcher.

Health (NIH) has noted examples of its early-stage grants being downloaded and distributed to foreign governments/researchers during the peer-review process,[8] a clear violation of peer-review principles. As described in the 2019 report by JASON—an independent advisory group of elite scientists—many of the security threats emanating from China can be considered violations of norms of research integrity.[9] Universities can address many of the issues stemming from the Chinese government by focusing on protecting key academic norms: intellectual honesty, research integrity, and academic freedom.[10]

Research activity at US universities is relatively concentrated among a small group of institutions. According to indicators published by the National Science Foundation, research expenditures at US colleges and universities totaled $71.8 billion in 2016. Expenditures by the 131 "R1 universities" (as defined by the Carnegie Classifications of Institutions of Higher Education) totaled $51.2 billion, or 70 percent of overall expenditures.[11] For the purposes of this paper, the policy suggestions outlined below should be applied to R1 institutions. For other institutions, the policies may be less relevant or too burdensome.

Components of the Problem

Increasingly, members of the US government have expressed concern that scientific collaborations between American and Chinese citizens have strengthened technological innovation in China. This is particularly worrisome in areas of research that have national security and military implications.

There are three separate but interrelated issues that confront US universities as they engage in scientific collaboration with Chinese counterparts: ***espionage and theft***, ***compromising relationships***, and ***human capital outflow***. These three issues are often conflated, preventing the academic and security communities from developing optimal solutions. Importantly, policies to address one problem may exacerbate another.

Espionage and Theft

There have been several well-documented incidents of espionage and theft committed by Chinese researchers studying or visiting at US research universities. In its report, *China: The Risk to Academia*, the Federal Bureau of Investigation (FBI) describes the case of a Chinese researcher at a midwestern medical school who stole several containers of a patented cancer research compound and deleted proprietary information about the

[8] Tabak and Wilson, "Foreign Influences on Research Integrity."

[9] JASON, *Fundamental Research Security*; and Tollefson, "Keep US Research Open."

[10] JASON, *Fundamental Research Security*; and Truex, "Stand up to China."

[11] National Science Board, *Science and Engineering Indicators*.

compound from university servers. In instances like these, the Chinese citizen seeks to provide stolen intellectual property to a Chinese commercial or government entity. There is a direct cost to the university, the researcher, and, by extension, the US government, which funds the research.[12]

In other cases, espionage is not always clear-cut and is difficult to prove definitively. Chinese entrepreneur Ruopeng Liu was trained at the lab of Duke University professor David Smith, an expert on metamaterials and inventor of the so-called invisibility cloak. After working closely with Smith, Liu brought two Chinese colleagues to visit the lab. The colleagues subsequently took photographs of lab projects when Smith was not present. Liu then replicated the cloak at one of his own labs in China and now has a technology company valued at $6 billion. Liu insists that there was no theft or wrongdoing, saying that Smith's work fell into the category of fundamental research.[13]

Cases like Liu's highlight the national security implications of espionage and theft at American campuses. Professor Smith's metamaterials research has security applications and was funded in part by the US military. Investigators believe Liu met with Chinese government officials and operatives while studying in the United States, and that Smith's research was part of a larger "shopping list of intelligence and technology that they target every year." Such technologies can be fed directly to the Chinese military, or as in Liu's case, they can jumpstart new Chinese firms that become competitors to American technology companies.[14]

The Chinese government continues to employ cyber-espionage to target American intellectual property, and cyberattacks may be facilitated by access to the physical and social networks of US campuses.

In-person intelligence collection is only part of the problem. As FBI Director Christopher Wray recently stated in remarks to the Center for Strategic and International Studies, the threat from China is "diverse and multi-layered . . . in techniques, in actors, and in targets."[15] The Chinese government continues to employ cyber-espionage to target American intellectual property,[16] and cyberattacks may be facilitated by access to the physical and social networks of US campuses.

Compromising Relationships

In the process of conducting research, American professors and students may develop relationships with Chinese entities. These relationships might include appointments at Chinese universities, partnerships with Chinese firms, or personal relationships with Chinese counterparts in government. Many of these relationships are benign, but some have the potential to become conflicts of interest or, worse, mechanisms for illicit intelligence relationships. This can be especially concerning if the researcher is simultaneously funded by the US and Chinese governments. In its report, the FBI describes the case of a Chinese professor who contributed to a classified Department of Defense (DoD) project. The professor was a member of China's Thousand Talents Program and provided a

[12] According to a 2017 report by the US Trade Representative, the annual cost to the US economy of counterfeit goods, pirated software, and theft of trade secrets is $225–600 billion (Office of the US Trade Representative, "Special 301 Report"). Note that it is unclear what portion of this number can be attributed to the activities of Chinese espionage at US universities.

[13] McFadden, Nadi, and McGee, "Education or Espionage?"

[14] McFadden, Nadi, and McGee, "Education or Espionage?"

[15] Wray, "Chinese Economic Espionage Threat."

[16] Laskai and Segal, "A New Old Threat"; and Wray, "Chinese Economic Espionage Threat."

Chinese institute with research that resembled his DoD work.[17]

The case of Charles Lieber, former chair of Harvard's Department of Chemistry and Chemical Biology, is another well-known example. While funded by the NIH and DoD, Lieber received $50,000 per month from Wuhan University of Technology and failed to disclose his membership in China's Thousand Talents recruitment plan.[18] Lieber's offense did not involve espionage or the illicit transfer of technology but simply a failure to report his relationships with Chinese entities as a recipient of US government grants.

Recent data published by the Center for Security and Emerging Technology suggests that most Chinese graduate students aspire to live, work, and potentially pursue citizenship in the United States.

In other instances, members of the Chinese intelligence apparatus have sought to cultivate ties with American professors and students studying abroad or visiting China, potentially to facilitate espionage or the sharing of illicit information. The Glenn Duffie Shriver case is the most famous example. Shriver was an undergraduate studying in Shanghai when he began interacting with Chinese intelligence officers who pretended to be city government officials. The officers asked Shriver to return to the United States and gain employment with the government. Shriver complied and maintained contact with the Chinese intelligence officials, accepting $70,000 from them while working for the State Department and Central Intelligence Agency.

American academics visiting China are vulnerable to becoming intelligence targets of the Chinese state. They also carry sensitive information on their phones and laptop computers, which can be easily compromised during travel to China.

Human Capital Outflow

Espionage in academic settings must be distinguished from human capital outflow. Many Chinese citizens who are educated in US universities decide to return home to China and use their knowledge to assist the Chinese government or commercial entities in developing new technologies. The fact that they had access to leading US labs, technology, and professors might give them an advantage that they would not have otherwise had, and by extension, reduce the relative technological advantage of the United States. Dan Coats, a senior official in the Office of the Director of National Intelligence, summarizes the issue:

> In a world where technology is available, where we are training their scientists and engineers, and their scientists and engineers were already good on their own, we are just making them able to not have to toil for the same amount of time to get capabilities that will rival or test us.[19]

Recent data published by the Center for Security and Emerging Technology suggests that most Chinese graduate students aspire to live, work, and potentially pursue citizenship in the United States. According to 2017 survey data from the National Science Foundation, 85–90 percent of Chinese PhD graduates in the United States across all STEM fields intend to stay in the United States.[20] This rate was as high as 90–98 percent in 2001. The downward trend reveals an increasing pull from China and push from the United States.[21]

[17] FBI, *China: The Risk to Academia*.

[18] Department of Justice, "Harvard University Professor."

[19] "U.S. Intelligence Warns," CNN.

[20] Zwetsloot et al., *Keeping Top AI Talent*.

[21] JASON, *Fundamental Research Security.*

A fourth issue, which is not discussed in depth in this paper, relates to ***academic freedom***.[22] The Chinese government, often through intermediary organizations like Chinese Students and Scholars Associations, routinely places pressure on US universities and individual academics to avoid research or speakers that relate to sensitive topics.[23] US scholars can face repression and intimidation when traveling to China.[24] Chinese students also increasingly feel that they are being monitored by their government or classmates, and this can hamper classroom discussion. These problems have been exacerbated by China's new National Security Law, which has provisions that criminalize speech about China outside of Chinese borders.[25] The academic freedom issue is outside the scope of this paper, but it also affects the tenor of collaboration between US and Chinese academics and institutions.

On the Severity of the Problem

The severity of the research security problem at US universities remains unclear. As of June 2020, the FBI had about two thousand ongoing investigations into attempted theft of United States–based technology across all fifty-six of its field offices. This represents a 1,300 percent increase in economic espionage investigations related to China relative to a decade ago.[26] Roughly 80 percent of all economic espionage cases brought by the DOJ are related to China in some way.

But it is important to note that investigations are not arrests, and they cannot be taken in and of themselves as evidence of systematic wrongdoing. Since Attorney General Jeff Sessions announced the China Initiative in the fall of 2018, the DOJ has been under substantial pressure to find and prosecute cases of Chinese espionage. In an interview, Assistant Attorney General John Demers stated that DOJ headquarters wanted each of the country's ninety-four US attorney districts to bring China cases—one or two per year.[27] This has the appearance of a quota system, and it implies that investigations are being initiated not because of the severity of the problem but because of top-down bureaucratic pressure. It is unsurprising that we have seen two thousand investigations given these incentives.

After nearly two years of investigations on university campuses, only a handful of actual charges have been produced, and most center on grant, wire, or tax fraud—which are not espionage.

Beyond the high-level figure, the FBI does not provide a breakdown of its two thousand ongoing investigations by crime, sector, or geography. We only observe case information through the DOJ when an individual is charged.

As of July 2020, the China Initiative has led to about forty arrests on an array of charges of various degrees of severity over the span of about twenty months.[28] Within that group, there have been cases at precisely ten US universities or research institutions: the University of Arkansas; Emory University; West Virginia University; University of Tennessee, Knoxville; Harvard University; Boston University; University of Kansas; the Cleveland Clinic Foundation; The Ohio State University; and Beth Israel Deaconess Medical Center. Of those ten cases, eight centered on allegations of wire fraud, false claims, or tax fraud, usually where the researcher failed to

[22] Hoover Institution, *Chinese Influence and American Interests.*

[23] Truex, "Stand up to China."

[24] Greitens and Truex, "Repressive Experiences."

[25] Clarke, "Hong Kong's National Security Law."

[26] Wray, "Chinese Economic Espionage Threat"; and Perano, "Wray: FBI Has over 2,000 Investigations."

[27] Swan, "Inside DOJ's Nationwide Effort."

[28] Department of Justice, "Department of Justice's China Initiative."

disclose a relationship with a Chinese university or China's Thousand Talents Program. Only three cases involved any evidence of espionage, theft, or transfer of intellectual property. Chinese national Zaosong Zheng allegedly stole twenty-one vials of biological research from Beth Israel Deaconess Medical Center in Boston. Yanqing Ye, also a Chinese citizen, failed to disclose her ongoing military service at the National University of Defense Technology and completed People's Liberation Army (PLA) intelligence assignments while studying physics and engineering at Boston University. Song Guo Zheng, a rheumatology professor at The Ohio State University, used $4.1 million in grant money from the NIH "to develop China's expertise in the areas of rheumatology and immunology" while a member of a Chinese talent program.[29]

As of this writing in July 2020, it is my opinion that there is insufficient evidence that academic/economic espionage from Chinese nationals is a widespread problem at US universities. After nearly two years of investigations on university campuses, only a handful of actual charges have been produced, and most center on grant, wire, or tax fraud—which are not espionage. The private sector does appear more vulnerable, and the FBI and DOJ have found more evidence of economic espionage committed against US firms.

From a social science perspective, we should be concerned about the cognitive tendency to generalize from small samples. At this point, we have a few well-cited cases of misconduct among Chinese citizens in university settings, but the actual incidence of wrongdoing among that population is unknown. Current estimates suggest there are 41,000 master's students, 36,000 doctoral students, and 38,000 postdoctoral/visiting scholars of Chinese citizenship currently in STEM fields at US universities, about 107,000 in total. Based on current DOJ charges, this implies a criminality rate in this population of .0000934, less than 1/10,000.

To date, the United States has benefited tremendously from human capital flows from Asia.

First Principles

While we should still consider ways to enhance research security at US universities, we should also be wary of overcorrections to a problem of limited scope. In addressing these issues, we should begin with the following principles.

First, no policy approach should be adopted that fosters systematic discrimination against a population based on its ethnicity or nation of origin. Racial profiling is illegal.[30] Simply by raising the issue of espionage by Chinese academics at US universities, we run the risk of stigmatizing the entire group, the overwhelming majority of whom are valuable contributors to American society and the economy. The Committee of 100, a nonprofit organization comprising prominent Chinese Americans, has found recent language from the FBI on Chinese espionage to be "disturbing and prejudicial" and accused the FBI of going against "the fundamental American ideals of the presumption of innocence, due process and equal protection for all."[31] In another statement, the Committee of 100 argues, "The loyalties of Chinese Americans are being unfairly questioned, and the community is being severely maligned by overreaching prosecutions and rush to judgment."[32]

There is also an economic cost to fostering xenophobia and anti-Chinese sentiment. There

[29] Department of Justice, US Attorney's Office, Southern District of Ohio, "Researcher Charged."

[30] Department of Justice, *Guidance for Federal Law Enforcement Agencies*.

[31] Committee of 100, "Broad Brush Stereotyping and Targeting."

[32] Committee of 100, "Legal Defense and Education Fund."

is evidence that Chinese and Chinese American professors in the United States increasingly feel unwelcome, and there has been a rise in hate crimes committed against members of these groups.[33] If such trends continue, talented Chinese academic researchers might be more inclined to return home, contributing to the human capital outflow problem.

Second, any policy approach must recognize the importance of foreign-born researchers to American universities and technology firms. To date, the United States has benefited tremendously from human capital flows from Asia. As described in the JASON report, as of 2019, sixteen US Nobel Prize winners were scientists of Asian descent, including eight Chinese Americans. Roughly 30 percent of US Nobel laureates were scientists born on foreign soil.[34]

By itself, the United States does not produce sufficient numbers of scientists and engineers—graduate programs in the sciences increasingly recognize this fact. In US universities, citizens of foreign countries now comprise the majority of graduate students in most engineering fields—electrical, civil, mechanical, industrial, chemical, and petroleum engineering, for example.[35] The majority of these students intend to stay in the United States and contribute to the American economy.

The presence of highly skilled immigrants is a boon to the US economy and is politically popular across the ideological spectrum.[36] In a recent report, the Cato Institute condemned measures to scale back the Optional Practical Training (OPT) program, which allows recent foreign graduates to work in the United States and can potentially be a path to citizenship.[37] According to a recent study

Some degree of espionage is inevitable given the open nature of scientific inquiry at US universities, but this does not mean the research model is flawed.

from the University of Maryland, "scaling back OPT would cause the unemployment rate to rise 0.15 percentage points by 2028."[38] Highly skilled immigrants innovate and create jobs for American workers. The National Foundation for American Policy found that of American start-ups valued at $1 billion or more, nearly a quarter had founders who entered the United States as international students.[39]

Third, we must recognize that the Open Science Model carries inherent vulnerabilities. Espionage by foreign, authoritarian governments on US university campuses is not a new phenomenon, and it is not limited today to the activities of the People's Republic of China (PRC).[40] Some degree of espionage is inevitable given the open nature of scientific inquiry at US universities, but this does not mean the research model is flawed. Reducing espionage to zero would require a fundamental shift in American academic culture—the banning of all Chinese students or high levels of monitoring/surveillance—that would be counterproductive. Policy solutions must strike a balance between addressing the espionage issue while preserving Open Science.

Fourth, US universities and the government can cooperate in addressing security threats from China in a way that is mutually beneficial. One of the unique legacies of the Cold War is the close cooperation between the US government and universities on a range of natural science,

[33] Chen, "China's Brain Drain."

[34] JASON, *Fundamental Research Security.*

[35] JASON, *Fundamental Research Security.*

[36] Hainmueller and Hiscox, "Attitudes toward Highly Skilled and Low-Skilled Immigration."

[37] Bier, "Facts about Optional Practical Training."

[38] Bier, "Facts about Optional Practical Training."

[39] Bier, "Facts about Optional Practical Training."

[40] FBI, "Higher Education and National Security."

engineering, and social science issues, in both classified and unclassified settings. Today, at some universities, cooperation with the US government is seen as a threat to university independence and academic values. This does not need to be the case. A closer relationship between leading research universities and the US government can foster trust, enhance national security, and help set appropriate boundaries between government and academia.

Recent Policy Developments

Under the Trump administration, we have seen a number of regulatory and enforcement measures designed to promote research security in the context of the China threat. This section outlines some of the core developments as of July 2020.

The ***Secure Campus Act***, proposed in 2020 by Senator Tom Cotton (R-Arkansas), Senator Marsha Blackburn (R-Tennessee), and Representative David Kustoff (R-Tennessee), would bar all PRC citizens from receiving student or research visas to the United States for graduate or postgraduate studies in STEM fields. There are waivers and exceptions available for "members of religious or ethnic groups systematically oppressed by the CCP," and the prohibition does not apply to citizens of Hong Kong or Taiwan. The bill also targets China's foreign talent recruitment programs. It prohibits all participants in China's foreign talent recruitment programs—including US citizens—from receiving federal research grants in STEM fields. Participants in talent programs would also be required to register under the Foreign Agents Registration Act.[41] Universities that receive federal research funding would be required to attest that they do not knowingly employ talent program participants.

In 2019, several bills aimed to address security risks on US campuses. Most notably, the Protect Our Universities Act, introduced by Senator Josh Hawley (R-Missouri), would require students from China, Iran, and Russia to undergo background screening before participating in "sensitive research projects." The bill has not advanced and was criticized for ignoring existing mechanisms in place to protect research, namely the classification system. It would have required background checks for individuals working on fundamental research, which contradicts the spirit of NSDD-189.[42] The Securing American Science and Technology Act, proposed by Representative Mikie Sherrill (D-New Jersey), called for the establishment of an interagency working group to coordinate activities in defense of federally funded research. It was enacted as part of the National Defense Authorization Act of 2020.

The Trump administration recently announced a round of ***planned visa cancellations*** targeted at Chinese graduate students and other researchers in the United States who have relationships with the PLA and universities/institutions in China with close ties to the military. According to some estimates, the proposed change would affect some three thousand Chinese students, and it would affect students currently in the process of completing their degrees. The visa cancellations will be based on academic ties, not specific evidence of wrongdoing by the individual student.[43] This builds on ***visa restrictions*** introduced in 2018, which limited visas for Chinese graduate students in certain fields to one year, with the possibility of renewal. Such students could hold five-year visas under the Obama administration.[44] Relatedly, the Trump administration is considering new

[41] Cotton, "Bill to Restrict Chinese STEM Graduate Student Visas."

[42] Redden, "Bills Target Academic Espionage."

[43] Wong and Barnes, "U.S. to Expel Chinese Graduate Students." Note that this is distinct from the recently proposed Immigration and Customs Enforcement regulations, which would ban foreign students with an F-1 visa from entering the United States and prohibit current students from remaining in the country if their classes are fully online. As of 2019, there were around 370,000 Chinese students in the United States (Zwetsloot, *United States–China STEM Talent "Decoupling"*).

[44] Yoon-Hendricks, "Visa Restrictions for Chinese Students."

restrictions on the OPT program, which allows international students in STEM to work in the United States for up to three years after graduating.[45] Two-thirds of OPT participants come from India and China.[46]

Some of these policy proposals clearly violate the first principles delineated above and represent an overcorrection.

The Department of Education has recently launched ***investigations into foreign gifts*** made to universities. According to Section 117 of the Higher Education Act, colleges and universities are required to report gifts that exceed $250,000. Recent investigations, which have included investigations into Harvard, Yale, and other high-profile universities, have revealed $6.5 billion in undisclosed foreign gifts in the past year. Some universities reported previously undisclosed research ties to Chinese institutions.[47]

Finally, the DOJ's ***China Initiative*** has sought to increase prosecutions of fraud, espionage, and intellectual property theft committed by Chinese nationals.[48] Since November 2018, there have been over forty arrests made, and there are two thousand active investigations being conducted by the FBI.[49]

Some of these policy proposals clearly violate the first principles delineated above and represent an overcorrection. For example, visa restrictions that target Chinese students based solely on loose institutional ties, and not on evidence of actual misconduct, are racist in their approach and a blunt tool to deal with the problem. The recently announced (and overturned) US Immigration and Customs Enforcement measures, which would prohibit international students from staying in the United States, serve no practical policy purpose and appear to be another thinly veiled attempt to get even more Chinese citizens out of the United States. The fact that such measures target students who are mid-degree, therefore terminating their studies, is cruel. Similarly, policies that reduce opportunities of Chinese citizens to work in the United States or gain paths to citizenship are counterproductive—they will accelerate the return of human capital to China and create incentives for espionage and intellectual property theft.

The framing of the DOJ's China Initiative is similarly problematic. As Lewis[50] argues, "using 'China' as the glue connecting cases under the Initiative's umbrella creates an overinclusive conception of the threat and attaches a criminal taint to entities that have an even tangential nexus to China." Given the scope and stated aims of the initiative, it is hard to imagine a scenario where FBI field offices are not differentially investigating Chinese and Chinese Americans, assuming a higher degree of criminality among this population.[51] This assumption is discriminatory at its core.

Policy proposals that seek to enforce or enhance regulations around disclosure or reporting requirements for US universities are more sensible. Such policies target institutions, not individuals of a certain ethnicity, and can be implemented in a way that is not discriminatory in nature. The remainder of this discussion develops policy proposals using this general approach.

These ideas can be implemented through close coordination between universities and the relevant agencies in the US government. Formal legislation

[45] Redden, "Foreign Student Work Program."

[46] Bier, "Facts about Optional Practical Training."

[47] Redden, "Foreign Gift Investigations."

[48] Lewis, "Criminalizing China."

[49] Swan, "Inside DOJ's Nationwide Effort"; and Wray, "Chinese Economic Espionage Threat."

[50] Lewis, "Criminalizing China."

[51] Committee of 100, "Broad Brush Stereotyping and Targeting"; and Lewis, "Criminalizing China."

on the China issue tends to be written by people without much experience in university settings or knowledge of scientific research, and the blunt tools often proposed reflect that ignorance. This constitutes an infringement on academic self-governance, which is a core pillar of our university system. To improve research security, US universities do not need more rules handed down from above. They need mechanisms to collaborate with the US government and the resources to better manage their own faculty and research dollars.

Policy Proposals

Policy Proposal 1: A No Dual-Salary Rule

The few documented instances of espionage or malfeasance relating to China and US academic institutions involve two parties rather than one-sided theft by a Chinese agent. Researchers at US universities, especially faculty, should not be receiving substantial compensation from Chinese entities, as this creates conflicts of interest and can be a precursor to more problematic activities.

A No Dual-Salary Rule

No full-time employee of an American university should receive salary or substantial compensation from the government or military of, or a university or firm in, a country of high strategic concern.

This principle would be a significant departure from the status quo. Most universities permit faculty to draw salary from other institutions, and most do not restrict those institutions. At Princeton, for example, faculty are permitted to receive compensation for consulting and other endeavors, provided these obligations do not detract from teaching/research and do not occupy more than one day per week of the faculty member's time.

The phrase "high strategic concern" is meant to encompass countries that constitute security threats to the United States and have a demonstrated history of conducting espionage and coordinated intellectual property theft on US university campuses. This would include China, but other countries might also fit this description—namely Russia and Iran. The Department of Energy (DOE) has published a more extensive list of thirty-seven "sensitive countries."[52] Countries could be added or removed from such lists depending on sustained shifts in behavior.

A No Dual-Salary Rule would eliminate several currently undesirable situations with respect to threats from China. First, US faculty members would no longer be eligible to receive compensation from China's Thousand Talents Program or similar institutions, which may serve as vehicles for technology transfer or theft from US research institutions and firms.[53] Second, Chinese graduate students and postdoctoral researchers who are using academic credentials as cover for ties to the Chinese military/intelligence apparatus would formally be in violation of university regulations. This would give students with genuine academic aspirations pause before closely cooperating with the Chinese government. Third, it would encourage US faculty members to focus on their primary professional obligation—teaching and conducting research at their home institutions. This would reduce so-called "conflicts of commitment."

Some research institutions have already adopted policies in line with this proposal. For example, DOE-funded scientists are now prohibited from participating in foreign talent recruitment programs, namely China's Thousand Talents Program.[54] The proposal in this paper goes further and would mandate that no R1 researcher funded by

[52] Mervis and Cho, "New DOE Policies."

[53] Priestap, "China's Non-Traditional Espionage."

[54] Mervis and Cho, "New DOE Policies."

US university or government grant receive salary or substantial compensation from a Chinese entity.[55]

Exceptions to this rule would include US faculty visiting Chinese universities for teaching or other academic obligations. Faculty members should also be permitted to receive standard honoraria (less than $1,000) for attending conferences and giving lectures at Chinese institutions. Chinese faculty would also be permitted to visit the United States while drawing salary from their home institutions.

This rule would not preclude individual donors of Chinese citizenship or descent contributing to universities or research centers, provided that such donations are made without requirements of sharing classified or sensitive information with Chinese entities. US researchers should also be permitted to participate in research partnerships with Chinese counterparts and entities.

Policy Proposal 2: Centralized Disclosure

Most universities require faculty members to submit annual disclosure or conflict of interest forms that describe their professional activities outside their normal teaching and research. These forms vary across universities and are meant to be analyzed by administrators in coordination with department chairs. Scientists who receive large grants through the National Science Foundation, NIH, and other agencies often have to complete separate but similar forms. Many researchers view these requirements as cumbersome and complete them as an afterthought. Some US universities do not have the capacity to conduct large-scale internal audits of funding and grants, so it is unclear whether and how disclosure forms are used.

Centralized Disclosure

The US government should work with universities to create a standardized, centralized disclosure system for faculty professional activities and conflicts of interest. The system can include an audit component conducted by the National Science Foundation.

This paper shares the opinion of JASON that an expanded understanding of research integrity is central to addressing the challenges in conducting science posed by the Chinese government.[56] Disclosure is the best available tool, and it remains underutilized. The White House Office of Science and Technology Policy is currently working on processes to strengthen and coordinate disclosure requirements across agencies, but this appears to be limited to federally funded research.[57]

A centralized system would allow universities and the broader scientific community to identify problematic professional and financial relationships among US faculty members. The system should be constructed such that audits by the National Science Foundation are not targeted at faculty members of a certain citizenship or ethnicity.

This system would require significant financial and technical investment as well as buy-in from leading universities. It could build on existing disclosure policies in place at the National Science Foundation and be extended to cover all US faculty members at R1 institutions, not just those that receive NSF funding. If properly designed, the system could actually reduce reporting requirements for many scientists. Researchers would only have to populate a standard form once per year, and that form could be used for all grant applications and for conflict of interest/commitment reporting at their home institutions. Many universities do not have the capacity to adequately monitor the

[55] This proposal is distinct from the Secure Campus Act, which states that no participant in a Chinese talent recruitment program can receive federal research funding and that US universities would be required to attest that they do not knowingly employ members of such programs.

[56] JASON, *Fundamental Research Security.*

[57] Droegemeier, "Letter to the United States Research Community."

outside professional activities of faculty, and the capacity that does exist varies across institutions. A centralized system could actually save resources and standardize practices across universities.

Malfeasance or poor reporting practices among faculty members should be considered a form of research misconduct and should carry professional sanctions on par with those for plagiarism, data fabrication, or other research integrity violations. Researchers must be trained on how to properly fill in the forms and report foreign funding and conflicts of interest.[58]

If the NSF audit system revealed misconduct, penalties and discipline would be levied by the faculty member's university. This is important to preserve academic self-governance. But universities should be encouraged to be more vigilant, enforce the rules that are already on their books, be clear in telling faculty what they can and cannot do, and punish violators. This would be a significant cultural shift in most universities, where faculty professional activities are only loosely monitored if at all, and tenured faculty, in particular, operate with a degree of impunity.

Policy Proposal 3: Pretravel Counterintelligence Training

It is commonplace for Americans studying and conducting research in China to be approached by members of the Chinese intelligence apparatus. Sometimes these intermediaries pose as members of the government, think tanks, or university administrations, and they seek to cultivate ties with US citizens with the ultimate goal of getting access to classified information or trade secrets. More informal elicitation is also quite common.[59] The relationships might be benign at first, but they can involve financial transactions and requests for "reports" or other output from the American targets. These relationships can be developed over several years.

Many students and faculty are unaware of this possibility and can unknowingly find themselves in awkward or compromising situations. This problem is exacerbated by the fact that American researchers and journalists in China are already vulnerable to repression and intimidation from the Chinese security apparatus.[60]

Pretravel Counterintelligence Training

US citizens traveling to China as part of an academic exchange should receive pretravel training from the FBI and State Department on issues relating to Chinese espionage and elicitation practices.

American students and faculty members need more training on how to assess these risks and how to handle delicate situations once they arise. The FBI and State Department can develop a short, ten- to twenty-minute training module that could be distributed to American researchers and students prior to travel in China. US universities can partner with the government to encourage completion of this training module in advance of exchange programs, study abroad, and faculty visits. The module should be developed with language consistent with academic values and should avoid militaristic depictions of Chinese citizens (e.g., "foreign adversary"). Ideally, the module could be developed with significant input from professors and university administrators, serving as a trust-building exercise between the academic, intelligence, and diplomatic communities.

The module should also include clear descriptions of how and where to report a possible intelligence situation. Most students and academics are unaware of where to do so and are perhaps reluctant to

[58] Mitchell, "Letter to ACE Member Presidents and Chancellors."

[59] FBI, "Elicitation."

[60] Greitens and Truex, "Repressive Experiences."

report anything for fear of being targeted for an espionage investigation. The FBI needs to foster an environment of trust where Americans living or traveling in China feel comfortable reporting suspicious incidents without feeling suspected of wrongdoing themselves.

Science today is global and borderless—it cannot be nationalized.

Finally, the module should include training for US citizens on how best to protect their personal information and data while traveling to China. Many Americans traveling to China are not aware of the cybersecurity risks, and in accessing their accounts and personal computers, they may be putting university networks and sensitive information in jeopardy. Basic education on the importance of VPNs, encryption, loaner computers, and so forth can reduce security risks.[61]

Policy Proposal 4: Reduce Expectations of Universities to Engage in Surveillance

Recent discourse on countering espionage calls for increased vigilance on the part of American universities, particularly administrators and faculty members. In its report, the FBI identifies foreign visitors as a potential security threat, telling universities to "keep visitor groups together and monitor them at all times."[62] It also recommends that universities "provide nonthreatening, convenient methods for employees to report suspicious behavior, and encourage such reporting." This language effectively tasks universities and their employees to engage in an "if you see something, say something" form of intelligence collection on behalf of the US government.

This expectation is inappropriate and unrealistic. University employees are not well trained to spot suspicious behavior. Worse, if faculty and staff are socialized into thinking that individuals of Chinese ethnicity are possible "foreign adversaries," this will create an environment of discrimination and distrust. Any gains from the few credible intelligence leads generated by university employees would be outweighed by false leads and legal issues arising from racial profiling. At this point, there is not sufficient evidence of espionage on university campuses to merit a substantial shift in the culture of monitoring and surveillance.

The No Surveillance Rule

US universities and their employees should not be expected to engage in monitoring or surveillance on behalf of the law enforcement community.

Creating a hostile environment for Chinese graduate students in the United States will erode the competitiveness of American universities, as elite Chinese scientists and engineers will choose to return home after graduation or even do their primary training in China or elsewhere. It is strategically important that China's best and brightest students feel welcome in the United States.

Conclusion

The current security focus on the problems of espionage, human capital outflow, and compromising relationships frames science as another forum of geopolitical competition. These are real problems, to be sure, and we must adopt policies that reduce the vulnerability of researchers in the United States to theft and coercion emanating from the Chinese government. The proposals raised in this paper seek to address these issues in a way that will not

[61] Mitchell, "Letter to ACE Member Presidents and Chancellors."

[62] FBI, *China: The Risk to Academia*.

increase discrimination against people who are ethnically Chinese.[63]

Science today is global and borderless—it cannot be nationalized. The Open Science Model has been the primary force behind the dominance of American universities and technology firms, and it is a model where people cannot be excluded on the basis of their citizenship or nation of origin. Any efforts to tinker with that model may very well bring costs orders of magnitude greater than those incurred from espionage or human capital transfer to China. The widespread visa restrictions, heightened surveillance, and targeted investigations proposed and implemented by the Trump administration amount to an attack on business as usual at US universities. At this point, there is not sufficient evidence of Chinese theft on US campuses to merit such a fundamental shift in our model of science. We must be careful not to propose solutions that are worse than the problem.

[63] Committee of 100, "Broad Brush Stereotyping and Targeting."

Bibliography

Bier, David J. "The Facts about Optional Practical Training (OPT) for Foreign Students." Cato Institute, May 20, 2020. https://www.cato.org/blog/facts-about-optional-practical-training-opt-foreign-students.

Chen, Stephen. "China's Brain Drain to the US Is Ending, Thanks to Higher Salaries and Donald Trump." *South China Morning Post*, September 6, 2018. https://www.scmp.com/news/china/science/article/2163001/chinas-brain-drain-us-ending-thanks-higher-salaries-and-donald.

Clarke, Donald. "Hong Kong's National Security Law: An Assessment." *China Leadership Monitor*, July 13, 2020. https://www.prcleader.org/clarke?utm_campaign=09f81b7c-375a-48a8-8d4a-a7f-5afd319a5&utm_source=so&utm_medium=mail&cid=181f57b0-7589-4ba6-b97c-2032dc9bab59.

Committee of 100. "Committee of 100 Denounces Broad Brush Stereotyping and Targeting of Chinese Students and Academics." Press release, February 16, 2018. https://www.committee100.org/press_release/committee-of-100-denounces-broad-brush-stereotyping-and-targeting-of-chinese-students-and-academics/.

———. "Legal Defense and Education Fund." https://www.committee100.org/projects/legal-defense-education-fund/.

Cotton, Tom. "Cotton, Blackburn, Kustoff Unveil Bill to Restrict Chinese STEM Graduate Student Visas & Thousand Talents Participants." Press release. May 27, 2020. https://www.cotton.senate.gov/?p=press_release&id=1371.

Department of Justice. *Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity*. Department of Justice, 2014. https://www.justice.gov/sites/default/files/ag/pages/attachments/2014/12/08/use-of-race-policy.pdf.

———. "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases." Department of Justice, Office of Public Affairs, January 28, 2020. https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.

———. "Information about the Department of Justice's China Initiative and Compilation of China-Related Prosecutions Since 2018." Last updated July 10, 2020. https://www.justice.gov/opa/page/file/1223496/download.

Department of Justice, US Attorney's Office, Southern District of Ohio. "Researcher Charged with Illegally Using U.S. Grant Funds to Develop Scientific Expertise for China." News release. Department of Justice, US Attorney's Office, Southern District of Ohio, July 9, 2020. https://www.justice.gov/usao-sdoh/pr/researcher-charged-illegally-using-us-grant-funds-develop-scientific-expertise-china.

Droegemeier, Kelvin. "Letter to the United States Research Community." Washington, DC: Executive Office of the President, Office of Science and Technology Policy, September 16, 2019. https://www.whitehouse.gov/wp-content/uploads/2019/09/OSTP-letter-to-the-US-research-community-september-2019.pdf.

FBI (Federal Bureau of Investigation). *China: The Risk to Academia.* Federal Bureau of Investigation, 2019. https://www.fbi.gov/file-repository/china-risk-to-academia-2019.pdf/view.

———. "Elicitation." https://ucr.fbi.gov/investigate/counterintelligence/elicitation-brochure.

———. "Higher Education and National Security: The Targeting of Sensitive, Proprietary and Classified Information on Campuses of Higher Education." White paper prepared by the Counterintelligence Strategic Partnership Unit, 2011. https://www.fbi.gov/file-repository/higher-education-national-security.pdf/view.

Greitens, Sheena Chestnut, and Rory Truex. "Repressive Experiences among China Scholars: New Evidence from Survey Data." *The China Quarterly* 242 (2020): 349–375.

Hainmueller, Jens, and Michael J. Hiscox. "Attitudes toward Highly Skilled and Low-Skilled Immigration: Evidence from a Survey Experiment." *American Political Science Review* 104, no. 1 (2010): 61–84.

Hoover Institution. *Chinese Influence and American Interests: Promoting Constructive Vigilance*. Stanford, CA: Hoover Institution Press, Stanford University, 2018. https://www.hoover.org/sites/default/files/research/docs/chineseinfluence_americaninterests_fullreport_web.pdf.

JASON. *Fundamental Research Security*. JSR-19-21. McLean, VA: MITRE Corporation. December 2019. https://www.nsf.gov/news/special_reports/jasonsecurity/JSR-19-2IFundamentalResearchSecurity_12062019FINAL.pdf.

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

Laskai, Lorand, and Samm Sacks. "The Right Way to Protect America's Innovation Advantage." *Foreign Affairs*, October 23, 2018. https://www.foreignaffairs.com/articles/2018-10-23/right-way-protect-americas-innovation-advantage.

Lewis, Margaret K. "Criminalizing China." *Journal of Criminal Law and Criminology* 111 (forthcoming). Preprint available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3600580.

McFadden, Cynthia, Aliza Nadi, and Courtney McGee. "Education or Espionage? A Chinese Student Takes His Homework Home to China." *NBC News*, July 24, 2018. https://www.nbcnews.com/news/china/education-or-espionage-chinese-student-takes-his-homework-home-china-n893881.

McKiernan, Erin C., Philip E. Bourne, C. Titus Brown, Stuart Buck, Amye Kenall, Jennifer Lin, Damon McDougall, et al. "Point of View: How Open Science Helps Researchers Succeed." *elife* 5 (2016): e16800.

Mervis, Jeffrey, and Adrian Cho. "New DOE Policies Would Block Many Foreign Research Collaborations." *Science*, February 8, 2019. https://www.sciencemag.org/news/2019/02/new-doe-policies-would-block-many-foreign-research-collaborations.

Mitchell, Ted. "Letter to ACE Member Presidents and Chancellors." Washington, DC: American Council on Education, May 10, 2019. https://www.acenet.edu/Documents/Memo-ACE-membership-foreign-espionage.pdf.

National Science Board. *Science and Engineering Indicators 2018*. Alexandria, VA: National Science Foundation, 2018. https://www.nsf.gov/statistics/2018/nsb20181/assets/nsb20181.pdf.

Office of the US Trade Representative. "2017 Special 301 Report." Office of the US Trade Representative, 2017. https://ustr.gov/sites/default/files/301/2017%20Special%20301%20Report%20FINAL.PDF.

Perano, Ursula. "Wray: FBI Has over 2,000 Investigations that Trace Back to China." Axios, June 24, 2020. https://www.axios.com/fbi-wray-china-counterintelligence-invetsigations-f809b7df-865a-482b-9af4-b1410c0d3b49.html?utm_campaign=organic&utm_medium=socialshare&utm_source=twitter.

Priestap, Bill. "China's Non-Traditional Espionage against the United States: The Threat and Potential Policy Responses." Statement before the Senate Judiciary Committee, December 12, 2018. https://www.fbi.gov/news/testimony/chinas-non-traditional-espionage-against-the-united-states.

Redden, Elizabeth. "Bills Target Academic Espionage." *Inside Higher Ed*, June 19, 2019. https://www.insidehighered.com/news/2019/06/19/two-new-bills-take-different-approach-protecting-us-research-foreign-threats.

———. "Foreign Gift Investigations Expand and Intensify." *Inside Higher Ed*, February 20, 2020. https://www.insidehighered.com/news/2020/02/20/education-department-escalates-inquiry-reporting-foreign-gifts-and-contracts.

———. "Will Trump Opt to Restrict Foreign Student Work Program?" *Inside Higher Ed*, May 29, 2020. https://www.insidehighered.com/news/2020/05/29/trump-administration-reportedly-considers-restrictions-foreign-student-work-program.

Sargent, John F., Jr. *U.S. Research and Development Funding and Performance: Fact Sheet*. Congressional Research Service, 2020. https://fas.org/sgp/crs/misc/R44307.pdf.

Swan, Betsy Woodruff. "Inside DOJ's Nationwide Effort to Take on China." *Politico*, April 7, 2020. https://www.politico.com/news/2020/04/07/justice-department-china-espionage-169653.

Tabak, Lawrence A., and M. Roy Wilson. "Foreign Influences on Research Integrity." Presentation to the 117th Meeting of the Advisory Committee to the Director, National Institutes of Health, December 2018. https://acd.od.nih.gov/documents/presentations/12132018ForeignInfluences.pdf.

Tollefson, Jeff. "Keep US Research Open Amid Threat from China, Says Elite JASON Group." *Nature*, December 11, 2019. https://www.nature.com/articles/d41586-019-03818-4.

Truex, Rory. "Colleges Should All Stand up to China." *The Atlantic*, December 28, 2019. https://www.theatlantic.com/ideas/archive/2019/12/how-defend-campus-free-speech-china/604045/.

"US Intelligence Warns China Is Using Student Spies to Steal Secrets." CNN, February 1, 2019. http://lite.cnn.com/en/article/h_0ea71e9963f942c7443747637c1ef945.

White House. *National Security Decision Directive 189: National Policy on the Transfer of Scientific, Technical and Engineering Information*. NSDD-189. Washington, DC: White House, September 21, 1985. Available via Federation of American Scientists: https://fas.org/irp/offdocs/nsdd/nsdd-189.htm.

Witze, Alexandra. "Trump's Top Scientist Outlines Plan to Reduce Foreign Influence on US Research." *Nature*, September 17, 2019. https://www.nature.com/articles/d41586-019-02787-y.

Woelfle, Michael, Piero Olliaro, and Matthew H. Todd. "Open Science Is a Research Accelerator." *Nature Chemistry* 3, no. 10 (2011): 745–748.

Wolfe, Audra J. "Spying in Plain Sight: Scientific Diplomacy during the Cold War." Science History Institute, January 28, 2020. https://www.sciencehistory.org/distillations/spying-in-plain-sight-scientific-diplomacy-during-the-cold-war.

Wong, Edward, and Julian E. Barnes. "U.S. to Expel Chinese Graduate Students with Ties to China's Military Schools." *New York Times*, May 28, 2020. https://www.nytimes.com/2020/05/28/us/politics/china-hong-kong-trump-student-visas.html.

Wray, Christopher. "Responding Effectively to the Chinese Economic Espionage Threat." Remarks prepared for the Department of Justice China Initiative Conference, Center for Strategic and International Studies, February 6, 2020. https://www.fbi.gov/news/speeches/responding-effectively-to-the-chinese-economic-espionage-threat.

Yoon-Hendricks, Alexandra. "Visa Restrictions for Chinese Students Alarm Academia." *New York Times*, July 25, 2018. https://www.nytimes.com/2018/07/25/us/politics/visa-restrictions-chinese-students.html.

Zwetsloot, Remco. *United States–China STEM Talent "Decoupling": Background and Policy Considerations.* National Security Report NSAD-R-20-057. Laurel, MD: Johns Hopkins University Applied Physics Laboratory, 2020.

Zwetsloot, Remco, James Dunham, Zachary Arnold, and Tina Huang. *Keeping Top AI Talent in the United States.* Washington, DC: Center for Security and Emerging Technology, December 2019. https://cset.georgetown.edu/wp-content/uploads/Keeping-Top-AI-Talent-in-the-United-States.pdf.

Acknowledgments

My gratitude goes to Avril Haines and Richard Danzig for their guidance and for including me in the "Measure Twice, Cut Once" project at the Johns Hopkins University Applied Physics Laboratory. I also thank Jacques DeLisle, Avery Goldstein, Neysun Mahboubi, and the Penn Project on United States–China relations, which co-sponsored the project. In addition to the above, I have received helpful feedback from Tarun Chhabra, Robert Daly, Mary Gallagher, Mike Green, Scott Kennedy, Kaiser Kuo, Lorand Laskai, Evan Medeiros, Shailagh Murray, Yeling Tan, Susan Thornton, Graham Webster, Jack Zhang, and Remco Zwetsloot. The views expressed in this paper are my own and do not reflect the opinions of the above individuals or their institutions.

About the Author

Rory Truex is currently an assistant professor of politics and international affairs at Princeton University. His research and teaching focuses on Chinese politics. He received his PhD in political science from Yale in 2014 and previously worked as an associate consultant at Bain & Company, Inc. He can be reached at rtruex@princeton.edu.

JOHNS HOPKINS
APPLIED PHYSICS LABORATORY