Global Engagement

RETHINKING RISK IN THE RESEARCH ENTERPRISE

A PUBLICATION OF THE HOOVER INSTITUTION

Global Engagement

Global Engagement

RETHINKING RISK IN THE RESEARCH ENTERPRISE

Edited by

GLENN TIFFERT

HOOVER INSTITUTION PRESS
STANFORD UNIVERSITY STANFORD, CALIFORNIA

With its eminent scholars and world-renowned library and archives, the Hoover Institution seeks to improve the human condition by advancing ideas that promote economic opportunity and prosperity, while securing and safeguarding peace for America and all mankind. The views expressed in its publications are entirely those of the authors and do not necessarily reflect the views of the staff, officers, or Board of Overseers of the Hoover Institution.

hoover.org

Hoover Institution Press Publication
Hoover Institution at Leland Stanford Junior University,
Stanford, California 94305-6003

First printing 2020
26 25 24 23 22 21 20 7 6 5 4 3 2 1

Manufactured in the United States of America
Printed on acid-free, archival-quality paper

CONTENTS

FOREWORD

Under Chairman Xi Jinping, the Chinese Communist Party (CCP) has resolved to strengthen its grip on power, take center stage in the world, and make good on Xi's pledge to lead the development of new rules and a new international order sympathetic to China's interests. The CCP is strengthening an internal system that stifles human freedom and extends its authoritarian control while exporting that model and undermining the rules-based international order. That is why it is vital for Americans and citizens of other democracies to read and discuss this important study. *Global Engagement: Rethinking Risk in the Research Enterprise* reveals how the CCP has orchestrated a sophisticated campaign of espionage and subterfuge to gain a differential military advantage, dominate the emerging global economy, and perfect its surveillance police state. But authors Jeffrey Stoff and Glenn Tiffert make clear in Chapter 1 that China's theft and application of cutting-edge technologies in pursuit of its ambitions is a problem that demands more than discussion. Americans and citizens of other free societies must put an end to what, at this point, has become willful ignorance concerning the scope of the threat. It is past time to undertake due diligence and risk assessments, end partnerships with institutions that act as fronts for the People's Liberation Army (PLA) or the Ministry of State Security (MSS), and prevent research institutions from aiding the CCP's aggression and repression of the Chinese people.

This study has arrived just in time. The CCP's campaign is intensifying as international awareness of the dangers that Xi Jinping's China

poses to freedom and prosperity is increasing. The party's aggressive actions during the COVID-19 pandemic, a crisis foisted on the world in part due to a deliberate cover-up of the initial outbreak in Wuhan, have forced a reassessment among even the most hopeful proponents of China's transformation into a "responsible stakeholder" in the international order. China's heavy-handed "Wolf Warrior diplomacy," which uses disinformation to obscure its responsibility for the pandemic and portrays European and American responses to the crisis as indicative of the West's ineptitude, corruption, and incompetence, has generated a long overdue awakening to dangers associated with China's promotion of its authoritarian model as superior to democracy.[1]

China's effort to undermine democratic nations, however, is more than a war of words. In the spring and summer of 2020, the People's Liberation Army (PLA) used the COVID-19 pandemic as cover for aggression, from the South China Sea (where its navy and maritime militias stepped up attacks to advance specious territorial claims) to the East China Sea (where the PLA Navy increased incursions into Japanese territorial waters near the Senkaku Islands) and to China's Himalayan border with India (where the PLA violated the Line of Actual Control multiple times and in June 2020 bludgeoned twenty Indian soldiers to death).[2] Taiwan received special attention as the PLA conducted nighttime drills in the Taiwan Strait and its fighter and bomber aircraft conducted threatening overflights as the chief of the Joint Staff Department, Li Zuocheng, vowed to "resolutely smash any separatist plots or actions."[3] In July 2020, in a particularly callous rejection of international agree-

1. See, for example, Thomas Wright, "Europe Changes Its Mind on China," *Brookings*, July 2020, https://www.brookings.edu/research/europe-changes-its-mind-on-china.
2. Lindsey W. Ford and Julian Gewirtz, "China's Post-Coronavirus Aggression Is Reshaping Asia," *Foreign Policy*, June 18, 2020, https://foreignpolicy.com/2020/06/18/china-india-aggression-asia-alliance; Steven Lee Meyers, "China's Military Provokes Its Neighbors, but the Message Is for the United States," *New York Times*, June 29, 2020, https://www.nytimes.com/2020/06/26/international-home/china-military-india-taiwan.html.
3. Anna Fifield, "China Vows to 'Smash' Any Taiwan Independence Move As Trump Weighs Sanctions," *Washington Post*, May 29, 2020, https://www.washingtonpost

ments and rule of law, the CCP implemented a national security law in Hong Kong to end the "one country, two systems" agreement and extinguish freedom and rule of law there.[4]

During the COVID-19 pandemic Chinese aggression in cyberspace was as brazen as its actions in the physical world. In the midst of the crisis, the PLA and the Ministry of State Security attacked hospitals, pharmaceutical companies, and medical research facilities developing COVID-19 therapies and vaccines.[5] Winning the race for a vaccine would reinforce the Wolf Warrior narrative that China's authoritarian system is superior to Western democratic systems. Australia was targeted with massive cyberattacks after calling for a World Health Organization investigation into the origins of the pandemic. The attacks demonstrated that the CCP was willing to perpetuate suffering abroad to ensure that China emerged from the crisis in a position of relative advantage economically and psychologically.[6]

CCP leaders took aggressive action on the Chinese mainland as well as abroad.[7] The COVID-19 pandemic served as a catalyst for expanding their surveillance regime. A "health code" assigned to individuals through the use of surveillance and artificial intelligence technologies augmented

---

.com/world/asia_pacific/china-vows-to-resolutely-smash-any-taiwan-independence-moves/2020/05/29/ae9c1af0-a158-11ea-be06-af5514ee0385_story.html.

4. Alice Su and Rachel Cheung, "The New Hong Kong: Disappearing Books, Illegal Words and Arrests over Blank White Paper," *Los Angeles Times*, July 10, 2020, https://www.latimes.com/world-nation/story/2020-07-10/this-is-a-cultural-purge-with-new-security-law-even-blank-paper-is-subversive-in-hong-kong.
5. David E. Sanger and Nicole Perlroth, "U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks," *New York Times*, May 13, 2020, https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html.
6. Alex Marquardt, Kylie Atwood and Zachary Cohen, "U.S. Officially Warns China Is Launching Cyberattacks to Steal Coronavirus Research," *CNN*, May 13, 2020, https://www.cnn.com/2020/05/13/politics/us-china-hacking-coronavirus-warning/index.html.
7. Lily Kuo, "'The New Normal': China's Excessive Coronavirus Public Monitoring Could Be Here to Stay," *Guardian*, March 8, 2020, https://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay.

other forms of social control such as the social credit score. The social credit score is designed to co-opt the population into conformity and coerce recalcitrant individuals who believe that they should have a say in how they are governed. The brilliance of the social credit score is that it mobilizes a person's social networks against her or him. If, for example, a Chinese citizen protests against the government in a way deemed threatening, the protestor's score will fall, and purchases of train tickets, apartment rentals, loans, and other services will be denied. The Party will also drop the scores of family and friends to mobilize social networks against protestors. The social credit score uses cutting-edge technology to co-opt and coerce people into reinforcing the state's draconian system of population control.[8]

China's minorities bear the brunt of this technology-enabled repression as the CCP continues a campaign of cultural genocide against its mostly-Muslim ethnic Uyghur population.[9] Artificial-intelligence technologies access an "Integrated Joint Operations Platform" that contains biomedical data gathered during mandatory physicals and other data to generate lists of "suspicious people," who are then rounded up and sent to concentration camps. More than a million people have been interned. Prisoners are subjected to systematic brainwashing and forced labor. Many males are sterilized, and many females are forced to have abortions or have contraceptive devices implanted into their bodies. In certain regions, the combination of these actions resulted in a reduction of the Uyghur birth rate by sixty percent.[10]

---

8. H. R. McMaster, *Battlegrounds: The Fight to Defend the Free World* (New York: HarperCollins, 2020), 119.
9. Bernhard Zand, "The Equivalent of Cultural Genocide," *Der Spiegel*, November 11, 2019, https://www.spiegel.de/international/world/chinese-oppression-of-the-uighurs-like-cultural-genocide-a-1298171.html.
10. Lindsay Maizland, "China's Repression of Uighurs in Xinjiang," Council on Foreign Relations (backgrounder), June 30, 2020, https://www.cfr.org/backgrounder/chinas-repression-uighurs-xinjiang; Amie Ferris-Rotman, "Abortions, IUDs, and Sexual Humiliation: Muslim Women Who Fled China for Kazakhstan Recount Ordeals," *Washington Post*, October 5, 2019, https://www.washingtonpost.com/world/asia_pacific/abortions-iuds-and-sexual-humiliation-muslim-women

* * *

The CCP's exploitation of American research institutions is foundational to its repression of its people, promotion of its authoritarian model, and coercion of its neighbors. The CCP uses censorship, espionage, theft of intellectual property, and surveillance of and intimidation on US academic campuses to advance sophisticated strategies such as Made in China 2025 and military-civil fusion. The former is designed to fuel China's economic growth with a vast amount of transferred technology and eventual domination of key sectors of the emerging global economy. The latter pursues dual-use technologies that would give China military as well as economic advantage. These strategies are successful in part because the CCP co-opts individuals, companies, research institutions, and academic institutions to act as witting or unwitting agents or to turn a blind eye to their activities. Co-option takes the form of foreign investment, donations, thinly veiled bribes, and other benefits, such as access to China's heavily monitored academic facilities. What is expected in return is for individuals and organizations to ignore egregious behavior such as the coercion of Chinese students and for the Chinese diaspora community to extract technology and conform to Chinese Communist orthodoxy.[11] Much of the espionage occurs under the veneer of academic research and partnerships with institutions such as China's "Seven Sons of National Defense" universities, which act as fronts for and extensions of the People's Liberation Army and the Ministry of State Security.

The egregious nature of the CCP's actions and the negligence of the US government, research institutions, and academia are likely to leave readers outraged. But it is most important that the combination of surprise, disgust, and anger that this study elicits be put to good purpose. The revelations in this study should inspire an end to the complacency,

---

-who-fled-china-for-kazakhstan-recount-ordeals/2019/10/04/551c2658-cfd2-11e9-a620-0a91656d7db6_story.html; *Associated Press*, "China Cuts Uighur Births with IUDs, Abortion, Sterilization," Associated Press, June 28, 2020, https://apnews.com/269b3de1af34e17c1941a514f78d764c.

11. McMaster, *Battlegrounds*, 110–11, 115–21.

avarice, and short-sightedness that have allowed the CCP to pursue its programs with near impunity. They should also lead to actions designed to curtail those programs and restore the integrity of sensitive research. Fortunately, in Chapter 2 authors Kevin Gamache and Glenn Tiffert have provided a framework for those actions in what they have labeled a global engagement risk assessment and management program. The basic steps proposed for addressing the problem set—know your partners, know your funders, take contracts seriously, train, iterate, and adapt—have relevance beyond research institutions. For example, international companies susceptible to CCP industrial espionage and vulnerable to the coercive power of the party might implement an analogous program.

Readers might also keep in mind a warning and a qualification. Growing appreciation for the CCP's systematic campaign of espionage coincides with an economic recession and growing populist sentiment that threaten to amplify anti-immigrant and protectionist impulses. Simultaneously, racial divisions laid bare by the murder of George Floyd at the hands of a Minneapolis police officer in May 2020 have combined with other sources of popular discontent to sap confidence in America's democratic institutions as well as its free-market economic system. Those conditions have generated twin dangers that Americans will either overreact to the threat described in these pages by treating Chinese people prejudicially or underreact by indulging in the conceit that deliberate actions of China's authoritarian regime are equivalent to the shortcomings of US institutions. Thankfully, the recommendations in this study are designed to reduce the risk associated with the CCP's exploitation of research activities while also avoiding excesses motivated by either jingoistic verve based in bigotry or careless passivity based in moral equivalency. The authors of this study are advocates of academic freedom and international cooperation. If leaders of research institutions adopt the proposed program, it will be a first step in restricting behavior that threatens to cheapen and debilitate both.

A Chinese proverb tells the story of chancellor Li Yifu, a great flatterer of the early Tang dynasty whose smile concealed his duplicitous intentions. Eventually Emperor Gaozong discovered his duplicity and banished him. Li's smile seems analogous to the veneer of academic col-

laboration that masks the CCP's sustained campaign of espionage. The CCP's "flattery" is delivered in the forms of sponsored research, philanthropic gifts, stipends, and joint appointments to Chinese universities. It is past time to expand collaboration with genuine partners while banishing agents who are advancing the interests of the CCP at the expense of not only Americans and citizens of other democracies, but also the Chinese people.

H. R. MCMASTER
Fouad and Michelle Ajami Senior Fellow
Hoover Institution, Stanford University

ACKNOWLEDGMENTS

The authors wish to thank Debra L. for brokering introductions among them, Teresa Domzal for her review of early drafts and invaluable guidance, Cyrus M. for his advice and support, Lauren Schroeder for her flexibility and diligence in creating the graphics, and Neelay Trivedi for his assistance with citations. Special thanks go to Larry Diamond for his tireless support, and to the editorial staff at the Hoover Institution Press.

Introduction

Across partisan and other familiar dividing lines on foreign policy in the United States, there is growing recognition that rapid accumulation and projection of power on the world stage by the People's Republic of China (PRC) constitutes the most serious of all current challenges to US national security. Beyond the breathtaking pace of modernization and enlargement of all branches of the People's Liberation Army, and China's increasingly aggressive and expansionist deployment of military power in the South China Sea and throughout the Indo-Pacific region (and beyond), there is the more subtle—but by no means benign—expansion of China's "sharp power." This is not the "hard" military power or economic coercion that leads to war and conquest. Neither is it the soft power that wins friends and influences societies transparently, through the diffusion of ideas, symbols, values, and cultural achievements. Rather, sharp power burrows deeply and deceptively into the soft tissues of democracies, seeking to subvert and sway them through methods that are, in the now paradigmatic words of the former Australian prime minister Malcolm Turnbull, "covert, coercive, or corrupting."

In the 2018 Report of the Hoover Institution–Asia Society Working Group on Chinese Influence Activities in the United States, *China's Influence and American Interests: Promoting Constructive Vigilance*, Orville Schell and I—along with a stellar team of China and foreign policy specialists that included an author of this current report, Glenn Tiffert—documented a number of ways that China's Communist party-state has

been working to penetrate, pressure, and compromise the integrity of American institutions. These include universities, think tanks, mass media, corporations, state and local governments, and the Chinese American community. A chapter of that report also sketched the myriad ways that the PRC has been trying to penetrate sensitive dimensions of the research enterprise in the United States—in part to misappropriate for economic benefit many of our most precious breakthroughs in science, medicine, computer science, and engineering, but in large measure to plow the fruits of this espionage and intellectual property theft into the modernization of its military. No dimension of our report was more troubling, and more directly threatening to US national security, than this relentless, audaciously conceived, decades-long, and multilayered campaign of technology theft, a subject that had earlier been systematically exposed in a groundbreaking 2018 study by Michael Brown and Pavneet Singh for the Defense Innovation Unit Experimental (DIUx), *China's Technology Transfer Strategy*.

Neither of the above reports, however, was able to delve sufficiently deeply into a particular vulnerability of our scientific research enterprise: the engagement of our universities and research laboratories with foreign scholars from countries that are (or could well be) adversaries of the United States—and worse, foreign scholars from military-linked universities and research centers, or to be specific, the "Seven Sons of National Defense" in China. And still worse for national security are PRC scholars who in at least some instances (documented here) have deliberately tried to obfuscate their connections to military projects and affiliated institutions. This raises the absurd possibility that some United States–based scientists and engineers are collaborating with counterparts from the PRC on scientific papers whose findings are then being exploited to modernize a military that the United States may someday have to face in armed conflict—or at least deter from conflict. And even more incredibly, some of these research collaborations appear to benefit, directly or indirectly, from US federal government funding.

To say that American institutions have been naïve about, and ill-prepared to confront and contain the risk from, the PRC's wide-ranging efforts at technology misappropriation is—I believe the reader of this

report will conclude—an understatement. But these aims remain only one dimension of the PRC's larger effort to project its sharp power around the world, and to control the global narrative specifically about China and generally about freedom, so that the Chinese Communist Party (CCP) might make the world safe for autocracy. This is more than a national security threat: It is an existential challenge to the entire global liberal order that has enabled political freedom and human rights to expand and thrive to an unprecedented extent in recent decades. If freedom is to be defended globally and the current deepening democratic recession is to be reversed, government leaders, politicians, journalists, and civil society activists must understand how China's Communist party-state operates in the shadows to shape and control information flows, bully governments and corporations, infiltrate and corrupt political systems, and disrupt and debase civic institutions.

Going forward, this larger mission of research and public education will be the work of our new Hoover Institution Project on China's Global Sharp Power. Over the coming year, we will build a clearinghouse of news, policy briefs, reports, and analysis on the PRC's disinformation and sharp power activities around the world, what we term a "China Influence Tracker." We will take a focused look at the history and practice of the United Front, the vast web of front organizations and proxies that are tasked with cultivating human relationships, dangling material inducements, and preying on emotional, financial, or ideological vulnerabilities in order to cajole and co-opt non-CCP partners into serving the CCP's interests, often unwittingly. We will advance policy options for exposing and countering these surreptitious influence activities. In that vein, we will endeavor to train journalists and civil society leaders around the world in how the PRC works to establish and disguise its inappropriate influence. We will seek to illuminate its efforts to reshape global institutions and norms, examining the PRC's participation in international organizations and multilateral forums, its influence efforts in regional organizations, its quest for dominance over the rules and tools of artificial intelligence, and its diffusion of digital technologies of surveillance and control. We will research more deeply into PRC sharp power projection in specific sectors of American society.

In doing all of this, we do not seek to foment hostility toward China—and we reject the language and imagery of an impending "new cold war" between the United States and China, or an inevitable military showdown between the two superpowers. We continue to warn explicitly at every opportunity of the dangers of ethnic profiling in the United States. We favor engagement with China—including in education and research—and we encourage diverse partnerships and exchanges. But as we urged in our 2018 report, engagement with China can only serve our national interest if it is based on three principles: transparency in all of these relationships, which in the context of this report must include full and truthful disclosure of researchers' ties to China's military-industrial complex and its state; reciprocity in access—for researchers, journalists, and partners of all kinds; and robust efforts to defend the integrity of our democratic institutions. The first line of defense is always knowledge. We hope this report will contribute to the foundation of knowledge necessary to structure international research engagements that will both advance the horizons of scientific discovery and protect the national interest.

LARRY DIAMOND
Senior Fellow
Hoover Institution, Stanford University

Executive Summary

I. Introduction

Neither the US government nor the universities and national laboratories in the US research enterprise are adequately managing the risks posed by research engagements with foreign entities. The task is quite simply falling through the cracks. Data with which to assess the performance of current frameworks for managing foreign engagement risk, to identify their defects, and to devise proportionate fixes is consequently in short supply. Dueling narratives have filled this evidentiary vacuum, pitting some who propose incremental adjustments against others who call for far-reaching change. Without a common set of facts to anchor the debate, consensus has proven elusive.

This report offers a way forward. Chapter 1 identifies more than 250 published research collaborations between scholars based in the United States and counterparts from seven universities in the People's Republic of China (PRC) that are integral to that nation's defense research and industrial base. This report maintains that it is not in the US national interest to collaborate and assist with the military development efforts of the PRC, a nation that the US government increasingly views as a strategic competitor and military rival, even if the relevant research is unclassified, considered basic or fundamental, and is ultimately published

in open sources.[1] Such collaborations are emblematic of systemic flaws in the ways that the US research community approaches foreign engagement risk. To remedy those flaws, the research community should embrace a new, proactive risk assessment and management paradigm informed by the principles of Operational Security (OPSEC) and implemented through capability maturity modeling. Chapter 2 delivers that paradigm.

II. Background

Bound by constitutional principles, the US government has generally accorded US scholars and the institutions that employ them wide discretion to manage their own research affairs. The research community has in turn nurtured a climate that favors openness, autonomy, and collaboration. It follows a decentralized approach to governance that aspires to promote free inquiry in the pursuit of knowledge by insulating scholars not just from external political authority and economic power, but also from undue interference from their own administrators. The result is a deliberately permissive model that has performed extraordinarily well and that exemplifies and renews the values at the heart of a liberal democratic society.

At the same time, the permissiveness of this model leaves it open to exploitation by those who do not share its values, including illiberal regimes that have proven adept at taking advantage of its lightly policed spaces. For much of the last thirty years, American hegemony has permitted US research institutions the luxury of overlooking this vulnerability, freeing them to pursue globalization unencumbered by the complications of geo-strategic competition. But the shifting balance of power is now impinging on that latitude and forcing an uncomfortable reckoning.

The direct and largely unrestricted access that the PRC in particular has enjoyed to US research creates challenges for the United States

1. National Security Council, *United States Strategic Approach to the People's Republic of China*, May 26, 2020, https://www.whitehouse.gov/articles/united-states-strategic-approach-to-the-peoples-republic-of-china.

and for the research institutions that rely on US government funding to support their work. Although these challenges do not always rise to the level of explicit illegality, in the realm of science and technology (S&T) research they can nonetheless adversely impact national and economic security and violate norms of academic integrity, ethics, or administrative rules. The challenges include (but are not limited to) the following:

- Conversion of US government-funded research into intellectual property that is then commercialized in the PRC in violation of research grant or university terms and conditions.
- Direction or redirection of US research to the PRC government by selectees of the PRC's state-run talent recruitment programs.
- Improper PRC influence over, or manipulation of, US research grant evaluations and award decisions.
- Diversions of US research to PRC defense programs and weapons system development, which can undermine or eliminate US military superiority.
- Diversions of US research to applications that violate ethical standards or democratic norms and values, such as those that enable or enhance the PRC's domestic surveillance apparatus and human rights abuses.
- Failing to report or misreporting foreign affiliations, research projects, and additional sources of funding in violation of federal research grant disclosure rules.[2]

It would be a grave error to mistake the comparatively low number of publicized cases that dramatize these challenges as evidence that existing safeguards are sufficient or as grounds for complacency. Owing to gaps in oversight and reporting, cases have escaped detection, several of which this report brings to light. These cases establish that US scholars

2. White House Office of Science and Technology Policy, *Enhancing the Security and Integrity of America's Research Enterprise*, June 2020, https://www.whitehouse.gov/wp-content/uploads/2017/12/Enhancing-the-Security-and-Integrity-of-Americas-Research-Enterprise-June-2020.pdf.

and research institutions have been contributing directly to the PRC's military modernization.

III. Overview of the PRC's Seven Sons of National Defense (Universities)

The seven universities profiled in Chapter 1 of this report have a long history of supporting the PRC's military programs. The PRC's Ministry of Industry and Information Technology (MIIT) has administered the universities since 2008 and refers to them as the "Seven Sons of National Defense" (国防七子).[3] The group includes the following:

1. Beijing Institute of Technology (北京理工大学)
2. Beihang University (a.k.a. Beijing University of Aeronautics & Astronautics, 北京航空航天大学)
3. Harbin Institute of Technology (哈尔滨工业大学)
4. Harbin Engineering University (哈尔滨工程大学)
5. Northwestern Polytechnical University (西北工业大学)
6. Nanjing University of Aeronautics & Astronautics (南京航空航天大学)
7. Nanjing University of Science and Technology (南京理工大学)

All seven universities were originally founded either as institutes of the People's Liberation Army (PLA) or from mergers of military engineering academies.[4] They eventually became civilian universities (typically in the late 1970s and 1980s) and hence incorporate nonmilitary

3. 吴志华 [Wu Zhihua], "国防七子"招生就业办领导首秀江西国科 ["National Defense Sevens Sons" Admissions and Job Placement Office Leaders Visit Jiangxi National Defense Technology Military Industry Group for the First Time]," 国家军民融合公共服务平台 [National Military-Civil Fusion Public Service Platform], June 21, 2017, http://jmjh.miit.gov.cn/web/newsInfoWebMessage.action?newsId=493942&moduleId=1062.
4. The exception is Harbin Institute of Technology, which was founded in 1920 (seven years before the PLA) but has focused on supporting defense research for most of its history.

disciplines such as social sciences. Nevertheless, all seven stipulate that their core mission is to support the PRC's defense research and industrial base and promote or execute military-civil fusion policies, which channel civilian research into military applications. Despite this shared mission, only four of the seven are on the US Department of Commerce's Entity List for export control purposes.[5]

IV. Methodology

The findings in Chapter 1 of this report rest primarily on bibliographic data extracted from a corpus of 254 English- and Chinese-language articles published in the scientific and engineering literature between January 1, 2013 and March 31, 2019. The articles were identified by searching the China National Knowledge Infrastructure (CNKI) platform for publications with coauthors from one or more of the Seven Sons universities and at least one US institution. CNKI is one of the most comprehensive online aggregators of peer-reviewed academic journals, conference proceedings, theses, and dissertations in the PRC. Supplementary research, mostly in Chinese-language sources, was also conducted on the PRC-based coauthors and institutional affiliations appearing in the collected corpus.[6]

This report makes no claims regarding the comprehensiveness or representativeness of that corpus. The report's scope is limited, and the cases it features were selected for the clarity of the risks that they expose. Because no technical assessments of the research implicated in these cases were sought, additional research would be necessary to characterize the concrete risks that they pose to US national and economic security. A deeper methodological discussion appears in the Appendix to

5. Beihang University, Northwestern Polytechnical University, Harbin Engineering University, and Harbin Institute of Technology are on the Department of Commerce's Entity List. The latter two were added on June 5, 2020, after the data for this report was collected.
6. For the purposes of this study, bibliographic data includes article title, authors, affiliated institutions, publication source, date, funding details (if provided), etc.

facilitate such scholarship and to enhance due diligence efforts for risk assessment purposes.

V. Key Findings

With those understandings in mind, these are our key findings:

- The collected corpus of 254 articles names coauthors from 115 US research institutions. Most of these institutions are universities, but eleven are federal research facilities, including seven Department of Energy national laboratories and the US Naval Research Laboratory. US government funding sources were also credited in thirteen articles.
- PRC university departments employing coauthors who are named in the corpus have partnerships with the PLA's General Armament Department, the PLA Rocket Force (which manages the PRC's nuclear missile arsenal), and components of major state-owned defense conglomerates including: a) China Aerospace Science and Technology Corporation and divisions within its missile design and production subsidiary, the China Academy of Launch Vehicle Technology; b) China Aerospace Science and Industry Corporation; c) Aviation Industry Corporation of China and a subordinate research institute that supplies manufacturing technologies for defense industries; and d) China Shipbuilding Industry Corporation.[7]
- Several identified coauthors appear to have worked on classified defense projects, as indicated by "XXX" or "XXXXX" designators in their titles or funding codes; for example, a PLA General Armament Department "Panoramic View XXXXX System Preliminary Research Project."
- Some coauthors' biographies mention their work on projects for the PRC's Central Military Commission Science & Technology

7. The PLA's General Armament Department is now known as the Equipment Development Department of the Central Military Commission.

Committee, PLA General Staff Headquarters, PLA General Armament Department, and PLA Unit 65927. One coauthor claimed to concurrently serve as a PLA General Armament Department Stealth Technology Experts Group member and a General Armament Department Military Use Electronic Components Technologies expert evaluator.

- One article named researchers from Northwestern Polytechnical University, a US university, and the Xi'an Engineering College of the People's Armed Police (PAP), raising ethical concerns over applications of this research. The PAP performs domestic security and surveillance functions that help the Chinese Communist Party (CCP) maintain authoritarian control over the PRC's population. The PAP's Xi'an Engineering College subsequently merged with a PAP command unit in Xinjiang, which may implicate it in the mass detentions, internment, and repression of the region's large Muslim population. No biographical information was found on the PAP-affiliated coauthor, raising questions about the degree of due diligence the partnering US institution might have been able to perform on this individual.
- Dissertations filed at some of the Seven Sons universities claim support from the US National Science Foundation (NSF) and the National Institutes of Health (NIH). The identified PhD candidates studied in the United States prior to completing their doctoral degrees and credit the PRC central government-run China Scholarship Council for providing funding support for their study abroad. By naming NSF and NIH funding sources in their dissertations, these students are indicating that they used US government-funded research conducted in the United States to fulfill at least part of their PhD degree requirements. The students may have been working under recipients of NSF and NIH funding (i.e., principal investigators) while receiving PRC government scholarship support to do so.
- Coauthors affiliated with US Department of Energy national laboratories have published research with six of the Seven Sons

universities. Although some of this research is intended for civilian purposes (such as new energy development), some of the PRC-based coauthors have held positions at or worked on PLA programs.

- Some authors obfuscate their ties to defense programs by using incomplete or innocuous sounding English names to describe their affiliation with a subordinate division of a Seven Sons university. For example, the Chinese terms for "national defense key laboratory" were replaced with "state key laboratory" in English. English webpages of university departments associated with some coauthors also do not disclose numerous defense-related subdivisions listed on the universities' Chinese-language websites. This obfuscation likely inhibits the ability of US research institutions to perform adequate due diligence on research partnerships.
- Some coauthors list no biographical information or curricula vitae (CV) on their faculty pages or on the websites of their employing institution; in one case, a faculty profile on the Harbin Institute of Technology website is blocked from US internet points of presence. In another example, a CV was provided but does not mention any US affiliation despite naming one in an identified article.
- Several articles include coauthors from Huawei, a PRC telecommunications conglomerate that was added to the Entity List in 2019. The US government has identified national security concerns with Huawei, including suspected ties to PRC military and intelligence organs, alleged violations of economic sanctions, and intellectual property theft. Huawei's role in the surveyed literature is unclear; nonetheless, it documents the conglomerate's research relationships with key defense universities.

VI. Conclusions and Recommendations

Citing a threat to long-term economic vitality and the safety and security of the American people, Presidential Proclamation 10043 of May 29, 2020, directs the US secretary of state to deny visas to study or conduct research in the United States to any postgraduate student or researcher from the PRC "who either receives funding from or who currently is

employed by, studies at, or conducts research at or on behalf of, or has been employed by, studied at, or conducted research at or on behalf of, an entity in the PRC that implements or supports the PRC's 'military-civil fusion strategy.'"[8]

This report concludes that the proclamation's threat narrative is empirically well-founded. The PRC's "Seven Sons of National Defense" universities directly support military-civil fusion; the PLA; and the defense research and industrial base, weapons programs, and myriad other entities that are part of the PRC's military, public security, and surveillance apparatus. Scientific collaboration between US research institutions and these seven PRC universities has promoted the missions of those entities, compromised US national and economic security, and undermined the integrity of US research.

Proclamation 10043 is a forceful intervention in a long-neglected problem. Yet, if the past is any guide, then the PRC will adopt circumvention strategies in order to frustrate the proclamation's aims. This report documents cases of PRC entities, students, and researchers obfuscating or misrepresenting their identities. In addition, collaborations with US partners may shift online or outside of the United States. Research institutions must prepare for such contingencies on their own initiative and develop equally adaptive and robust internal processes in response or the US government may step in and impose blunt alternatives.

The binary test of (il)legality by which S&T collaborations with PRC entities are conventionally assessed sets too high of a bar and is plainly insufficient to satisfy that requirement. Most, if not all, of the collaborations featured in this report may have been legal at the time that they were undertaken. This report furthermore assumes that their research content qualified as basic or fundamental and was therefore not

8. US President, "Proclamation 10043 of May 29, 2020: Suspension of Entry as Nonimmigrants of Certain Students and Researchers From the People's Republic of China," document 85 FR 34353, *Federal Register* 85, no. 108 (June 4, 2020), https://www.federalregister.gov/documents/2020/06/04/2020-12217/suspension-of-entry-as-nonimmigrants-of-certain-students-and-researchers-from-the-peoples-republic.

subject to export or classification controls by the US government. In addition, failures to disclose foreign collaboration by federal research grant recipients may have reflected faulty compliance rather than intentionally unlawful activity. New approaches to identifying and managing risk are urgently required.

The authors of Chapter 1 therefore make the following four recommendations:

1. Expand the scope of this report.

- Other articles within the collected corpus merit scrutiny to identify potential risks to US entities. Further studies using the methodology detailed in the Appendix may identify US research collaborations with other PRC institutions that support the PRC's defense programs, especially those beyond the immediate compass of Presidential Proclamation 10043. This methodology could also be applied to collaborations with institutions and researchers from other nations.
- The economic implications of US-China research collaboration should be explored more fully. As PRC universities have partnerships with state-owned enterprises in both civilian and military sectors, further investigation is needed to determine if US taxpayers are funding technologies that are patented or commercialized by PRC universities or partner companies.

2. Expand vetting and due diligence of collaborations with PRC partners.

- US research institutions should determine if the US-based coauthors were recipients of or worked on federal grants that related to the research published in the scientific literature this report identifies.
- US research institutions should compile information on all PRC organizations that have demonstrable connections to the PRC's defense research and industrial base. They should obtain this information primarily through PRC-based vernacular information sources and create collective information sharing mechanisms that can be used to enhance vetting of visiting PRC students

and scholars, as well as ramp up due diligence on proposed or existing research partnerships with the PRC.
- US research institutions should partner / share information with foreign allies to enhance those nations' due diligence and risk assessments since the PRC's Seven Sons universities collaborate with many nations, not just the United States.

3. Enhance administrative oversight.

- Benign research cannot be separated a priori from potential dual-use applications pursued by foreign institutions that support defense research such as the Seven Sons universities. US research institutions should mandate disclosures and preapprovals for all forms of S&T collaboration with PRC institutions—even when the research is considered fundamental in nature or published openly—and undertake disciplinary measures when individuals fail to seek approvals. Effective oversight depends on comprehensive reporting and periodic review.

4. Create or revise common moral and ethical standards with respect to research collaboration in academia.

- US research institutions should create a common framework to determine when research collaborations, student and researcher exchanges, and other forms of partnership may contribute to the military or domestic repressive capabilities of authoritarian regimes, violate democratic values or human rights, or involve unethical research practices.
- US research institutions should develop, maintain, and share lists of foreign partners (distinct from governmental lists) that they consider off limits for collaboration based on agreed-upon standards and documented evidence of programs, activities, or associations that are inimical to US interests and values.

The authors of Chapter 2 of this report build on these foundations. Taking up the question of how to reconcile an open and globalized research enterprise with the imperative to safeguard US national security

and economic competitiveness, they propose a new paradigm for governing foreign engagement risk, regardless of its country of origin. Six additional recommendations flow from that.

5. Enhance due diligence and compliance for all foreign engagements.

- To ensure that US research institutions exercise their discretion to undertake foreign engagements wisely, they must redouble their efforts at basic due diligence and compliance. At a minimum, this includes better vetting of prospective partners and funders; careful scrutiny of the terms of proposed collaborations, especially when they involve formal contracts and agreements; constant iteration and adaptation of risk governance processes; and formal integration of diverse stakeholders, including area and subject matter specialists, into those processes.

6. Establish a strategic global engagement risk assessment and management program.

- Reclaiming control over foreign engagement risk begins by bringing all of an institution's international engagements under the governance of a unified strategic program. This program would impose coherence on policies and processes that rigorously assess the nature and degree of risk that foreign engagements pose and guide proportionate measures to mitigate those risks to acceptable levels.
- The program must incorporate the following: practical training in compliance mandates, and in risk awareness and mitigation for both formal and informal foreign engagements; transparent reporting and record keeping processes; and regular performance reviews.
- The program could support jointly administered regional vetting centers and secure computing enclaves, which would allow member institutions to spread costs, pool resources, and provide internal clients with security as a service at economies of scale. These regional facilities would establish cooperative points of contact with government partners to facilitate information sharing and compliance.

7. Establish a strategic global engagement review office.

- Each research institution should establish a stable, accountable authority with the institutional capital to drive its strategic global engagement risk assessment and management program to success across multiple constituencies.
- This Global Engagement Review Office would supervise program implementation and exercise unified leadership over foreign engagement risk policies and processes across the institution. In a typical university setting, it would report and make recommendations directly to the provost and advise other principals on foreign engagement risk. It would complement and coordinate with other units, such as export control and facilities security, that are commonly under the authority of the vice provost for research.

8. Change the paradigm.

- Research institutions should adopt Operational Security (OPSEC) as their governing paradigm for assessing and managing foreign engagement risk in order to cement a more proactive and adaptive posture than traditional compliance-driven approaches can deliver. OPSEC supplies a workflow for sustaining vigilance and innovation.

9. Embrace maturity modeling to consolidate and develop capabilities.

- Adoption of a global engagement maturity model establishes a methodology for formalizing and optimizing a global engagement risk assessment and management program from inception to full integration with an institution's operations. Such a model defines a ladder that institutions can climb to achieve and communicate preparedness for more demanding work requirements. Combined with OPSEC, this model promotes perfection and growth in an institution's capabilities.

10. Establish a government-sponsored entity to support better decision making.

- Research institutions have unequal resources and capabilities and cannot abate foreign engagement risk alone. Government support

is essential but currently fragmented and scoped too narrowly. A new interagency entity combining the equities of multiple government stakeholders and their open-source data streams could provide an urgently needed, unified point of contact for the research enterprise on compliance matters and foreign engagement risk; deepen relationships of trust; facilitate routine information sharing; and enhance research and analysis so that institutions can make better and more granular decisions for themselves.

CHAPTER ONE

Under the Radar: National Security Risk in US-China Scientific Collaboration

JEFFREY STOFF AND GLENN TIFFERT

I. Introduction

The rise of the People's Republic of China (PRC) as a major economic and military power has sparked serious national security concerns in the United States, particularly in response to the PRC's active development of force projection capabilities, its intensification of domestic surveillance, widespread human rights abuses, unfair trade practices, forced technology transfer, state-sponsored industrial espionage, and intellectual property (IP) theft.[1] Alarm also stems from the PRC's stated intention to dominate strategic technologies and industries and its poor transparency with respect to governance.[2]

All statements of fact, opinion, or analysis expressed are those of the authors and do not reflect the official positions or views of any US government agency. Nothing in the contents should be construed as asserting or implying US government authentication of information or endorsement of the authors' views. This material has been reviewed by responsible US government offices to prevent the disclosure of classified information.

1. Senator Mark Warner surveyed the range of threats China poses to US national and economic security in a speech at a Brookings Institution event, Global China: Assessing China's Growing Role in the World, May 19, 2019, http://www.brookings.edu/events/global-china-assessing-chinas-growing-role-in-the-world.
2. A suggested sampling of materials that examine these issues include: a) William C. Hannas, James C. Mulvenon, and Anna P. Puglisi, *Chinese Industrial Espionage* (London and New York: Routledge 2013); b) Michael Brown and Pavneet Singh,

Many of these concerns intersect with the PRC's access to and influence within the US research community, especially in universities and US national laboratories. These intersections include the following:

- The increasing number of unclassified research areas and technologies with potential military applications, which complicates US government oversight and regulation (e.g., through export controls).
- PRC state-run talent recruitment programs that harvest US research.
- Unreported or misreported research collaborations, which can distort resource allocation and raise research integrity concerns.
- Inadequate compliance, monitoring, and due diligence by US research institutions with respect to research collaborations and enforcement of ethics and conflict of interest and commitment rules.
- The absence of any comprehensive or empirical study of research collaborations in science and technology (S&T) between PRC and US institutions to identify and assess potential risks.

American universities are among the best in the world, and their S&T research programs attract a highly talented, global pool of applicants. There is no question that the openness of the US research system

---

"China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation," Defense Innovation Unit Experimental January 2018; c) Office of the US Trade Representative, Executive Office of the President, "Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974," March 22, 2018; d) National Bureau of Asian Research, "The Report of the Commission on the Theft of American Intellectual Property," May 2013; e) Committee on the Judiciary, US Senate, "China's Non-Traditional Espionage Against the United States: The Threat and Potential Policy Responses," December 12, 2018; f) Larry Diamond and Orville Schell, eds., "China's Influence and American Interests, Promoting Constructive Vigilance" (Stanford, CA: Hoover Institution Press, 2019); g) U.S.-China Economic and Security Review Commission, "China's Overseas United Front Work: Background and Implications for the United States," August 24, 2018; h) Levesque, Stokes, "Blurred Lines: Military-Civil Fusion and the 'Going Out' of China's Defense Industry," Pointe Bello report, December 2016.

has contributed to US economic, technological, and military superiority for decades. In fact, since the US government established official diplomatic relations with the PRC, it has facilitated and encouraged collaboration with PRC-based researchers and institutions as matters of policy and soft power diplomacy.[3]

Meanwhile, the PRC's S&T ambitions have mushroomed. Guided by the concept of military-civil fusion, the PRC is resolutely integrating private sector innovation into its defense industrial base, in part by tapping the capabilities of ostensibly civilian domestic institutions. Some of these institutions participate in a coordinated, state-directed technology transfer apparatus that is tasked with obtaining, commercializing, and weaponizing advanced foreign R&D. Only now is the US research community awakening to the intensity and scope of this enterprise and its military or dual-use dimensions. However, in the absence of external regulatory or policy mandates, US research institutions have been slow to adapt their due diligence and risk management frameworks. Weak institutional reporting mechanisms and compliance cultures have permitted some collaborations to go unknown, unreported, or underreported.[4] Even among vetted collaborations, conflicts of commitment, unreported or misreported elements, or other activities that undermine the integrity of US scientific research and exceed the scope of collaboration agreements occur. In short, prevailing due diligence and risk management practices for screening and tracking potential collaborations with PRC entities fall far short of what circumstances require.

The director of the National Institutes of Health (NIH) highlighted these gaps in a 2018 letter addressed to more than ten thousand institutions in which he expressed concern that some recipients of NIH

3. For an overview of the history of scientific collaboration with China and US policies that fostered much of this collaboration, see Richard P. Suttmeier, "Trends in U.S.-China Science & Technology Cooperation: Collaborative Knowledge Production for the Twenty-First Century?," Research Report Prepared on Behalf of the U.S.-China Economic and Security Review Commission, September 11, 2014.
4. Note that federal funding agencies have different requirements regarding disclosure of foreign collaborations and additional sources of funding; as such not all collaboration may have to be reported.

research funding had diverted IP in grant applications or from NIH-funded research to other countries; shared confidential grant application information with others, including foreign entities, or attempted to influence funding decisions; and failed to disclose substantial resources from foreign governments, thereby distorting decisions about the appropriate use of NIH funds.[5] The terminations of three ethnic Chinese scientists at the MD Anderson Cancer Center and two Emory University professors were related to these concerns.[6] The arrest of Professor Charles Lieber, chair of the Chemistry and Chemical Biology department at Harvard University, arose from them as well.[7]

Given the paucity of available data, we cannot determine if such cases are outliers. But we can say that the fragmentary way in which US policymakers and the research community generally assess the risks posed by PRC students, researchers, and collaborative exchanges is seriously flawed. Fundamentally, that assessment has hinged on the *legality* of an activity; i.e., if no US laws will be violated, then the hazards are assumed to be negligible, or perhaps manageable. This crude binary test and the law enforcement paradigm behind it are poorly suited to the spectrum of potential risks revealed by this chapter, to say nothing of the crimes of gravest concern—economic espionage and intellectual property theft

5. Francis S. Collins, "NIH Foreign Influence Letter to Grantees," official memorandum, Department of Health and Human Services, Bethesda, MD, August 20, 2018, https://doresearch.stanford.edu/sites/default/files/documents/nih_foreign_influence_letter_to_grantees_08-20-18.pdf.
6. Todd Ackerman, "MD Anderson Ousts 3 Scientists over Concerns about Chinese Conflicts of Interest," *Houston Chronicle*, April 19, 2019, https://www.houstonchronicle.com/news/houston-texas/houston/article/MD-Anderson-fires-3-scientists-over-concerns-13780570.php; Ariel Hart, "New Findings: 2 Emory Researchers Didn't Disclose Chinese Funding, Ties," *Atlanta Journal-Constitution*, May 23, 2019, https://www.ajc.com/news/state--regional-govt--politics/new-findings-emory-researchers-didn-disclose-chinese-funding-ties/QQ58XiznSllTLYv5rARfjL.
7. US Department of Justice, "Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases," Justice News, January 28, 2020, https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.

(18 U.S.C. § 1831,1832)—which can be exceptionally difficult to prove in academic research contexts. Perfecting or intensifying the implementation of this paradigm will therefore reap only limited gains.

Presidential Proclamation 10043 of May 29, 2020 does not substantially alter that. The proclamation directs the US secretary of state to deny F or J visas to study or conduct research in the United States to any postgraduate student or researcher from the PRC "who either receives funding from or who currently is employed by, studies at, or conducts research at or on behalf of, or has been employed by, studied at, or conducted research at or on behalf of, an entity in the PRC that implements or supports the PRC's 'military-civil fusion strategy.'"[8]

Effective implementation of the proclamation will narrow some of the channels through which the collaborations analyzed in this chapter have transpired, but it will not close them. For instance, collaborations with US partners may move online or to sites outside of the United States. The PRC government is highly disciplined and adaptive and will foreseeably seek ways to ensure that PRC students and researchers who pose security risks to the United States will continue to receive visas. It may, for example, work through entities that lie beyond the scope of the proclamation's application, always endeavoring, as it does now, to stay one step ahead.

This chapter documents cases of PRC entities, students, and researchers obfuscating or misrepresenting their identities. US consular officials may fail to discern such subterfuge in a visa applicant's background or connect the applicant's declared program of study to sensitive fields of knowledge or dual-use technologies, which means that the hardest cases to detect may still get through. It is incumbent on research institutions to develop the tools to distinguish these individuals and any activities that they may undertake that are prejudicial to the interests of the United States from the general population of PRC students and researchers who pose no security risks. If research institutions fail, then more prescriptive regulatory solutions will be waiting in the wings.

8. US President, "Proclamation 10043 of May 29, 2020."

A. Assessing the Risks of Research Collaboration

Academic institutions must adopt proactive risk management and due diligence frameworks in order to more fully meet the challenges that collaborations with the PRC pose to the US research and innovation ecosystem. These challenges implicate fundamental norms of research and academic integrity, ethics, and administrative rules (as opposed to criminal statutes), and they intersect with potential national and economic security threats. These threats include the following:

- Conversion of US government-funded research into intellectual property that is then commercialized in the PRC in violation of research grant or university terms and conditions.
- Direction or redirection of US research to the PRC government by selectees of the PRC's state-run talent recruitment programs.
- Improper PRC influence over, or manipulation of, US research grant evaluations and award decisions.
- Diversions of US research to PRC defense programs and weapons system development, which can undermine or eliminate US military superiority.
- Diversions of US research to applications that violate ethical standards or democratic norms and values, such as those that enable or enhance the PRC's domestic surveillance apparatus and human rights abuses.
- Failing to report or misreporting foreign affiliations, research projects, and additional sources of funding, in violation of federal research grant disclosure rules.

Moreover, these new frameworks must be evidence based and reflect the empirical state of R&D collaboration between the two nations. US collaboration with defense-affiliated institutions, scientists, and engineers in the PRC is a key vector through which the PRC obtains access to US R&D with national and economic security implications. Unfortunately, scholarship on this subject is sparse and grounded mostly in surveys of English-language publications aggregated by Elsevier, Web

of Science, Scopus, or other international publication databases. Even so, a seminal 2018 study by the Australian Strategic Policy Institute (ASPI) estimates that the People's Liberation Army (PLA) has sent more than 2,500 military scientists and engineers overseas to collaborate with researchers and institutions worldwide. The US is one of the top destinations for those personnel.[9] A subsequent ASPI study identified 115 PRC research institutions that pose "high" or "very high" risks to potential Western partners. The identified PRC institutions support the PLA, defense R&D, the major defense conglomerates, and/or the PRC's intelligence and security apparatus.[10]

These ASPI studies have shed critical light on the scale of the PRC military's exploitation of Western academic institutions and the national security interests at stake. Research into Chinese-language publications and the PRC's domestic scientific publication repositories could reveal higher numbers of PLA-affiliated researchers collaborating with overseas institutions and further substantiate the concrete risks of those engagements. However, peer-reviewed S&T publications from PRC sources (which include both Chinese- and English-language articles) remain virtually unexplored.

B. Research Design

This chapter targets that gap with a three-step methodology for reviewing and assessing US-PRC collaborations. (See Appendix.) First, it identifies seven key PRC universities ("Seven Sons") that directly support the country's defense research and industrial base and that operate as prime pathways for harvesting US research and diverting it to military applications. Second, using the search facilities of a major online publication repository (China National Knowledge Infrastructure, or CNKI), and

9. Alex Joske, *Picking Flowers, Making Honey; The Chinese Military's Collaboration with Foreign Universities*, Report No. 10 (Canberra: Australian Strategic Policy Institute, 2018), https://www.aspi.org.au/report/picking-flowers-making-honey.
10. Alex Joske, *The China Defence Universities Tracker*, Report No. 23 (Canberra: Australian Strategic Policy Institute, 2019), https://www.aspi.org.au/report/china-defence-universities-tracker.

supplementary data from Elsevier's ScienceDirect, it collects a corpus of English- and Chinese-language articles published in the S&T literature with coauthors from at least one of those universities *and* a US institution. The searches ranged from January 1, 2013 to March 31, 2019 in order to spotlight recent activity. Third, it unpacks illustrative cases from that corpus to expose their concrete links to PRC military programs. In order to keep the discussion focused on problematic practices and institutional relationships rather than on individuals and ethnicity, we choose not to identify specific coauthors by name. Given the PRC's global reach and access to scientific collaboration, publication records listing authors affiliated with institutions in other nations should also be analyzed for similar national security and research integrity concerns.

C. Research Limitations

Our research design has several limitations:[11]

- The survey of publications was limited to scientific journals and theses/dissertations. Conference proceedings, patents, and other types of information on scientific research exceed the scope of this chapter.
- CNKI offers a comprehensive repository of scientific publications, but it is not exhaustive. The collected corpus may not capture every publication in the scientific literature with authors from US institutions and Seven Sons universities.
- No technical assessments were made on the research in the collected corpus to determine potential military applications, assessments of PRC military capabilities, or comparisons to US military systems.
- An unscientific sample was selected from the collected corpus for scrutiny. Many other articles in the corpus merit close investigation.
- CNKI's web interface has reliability issues. Specifically, the CNKI website returned different results for the same searches performed

11. A detailed explanation of these limitations is provided in the Appendix to this chapter.

at different times. Performing identical searches repeatedly using different internet points of presence and collating the results mitigated this limitation.

- CNKI is operated by state-owned companies under the oversight of the Chinese Communist Party (CCP) and engages in documented censorship of search results.[12]

To be absolutely clear, we allege no specific transgressions, criminal or ethical, and acknowledge that the evidence presented here is circumstantial. In certain instances, the research underlying the cases featured in this chapter may have all been conducted in the PRC and later published at a moment when one or more of the coauthors had an affiliation with a US institution, which would admittedly render the US connection tenuous. It is also possible that some of the PRC-based coauthors who cite US affiliations or US government support for their research may have misrepresented or inflated those claims, but because we lack the investigatory authority to independently determine the relevant facts, we take them at their word.

We grant that the research featured in this chapter may be fundamental in nature and have no immediate, discernible military value, and that if it has civilian applications then it is legitimately subject to commercialization and fair competition in the marketplace. Furthermore, we welcome the PRC's growing role in global scientific and technological research and recognize that some of the information flows arising out of international collaborations with it may benefit all of the parties to them, and indeed humanity more generally.

D. Purpose of This Chapter

Our aim is not to audit these collaborations or to impugn the motivations or integrity of any particular participant, but rather to empirically document the alarming and inadequately screened institutional relationships

12. China's ability to censor academic journals was explored in Glenn D. Tiffert, "Peering Down the Memory Hole: Censorship, Digitization, and the Fragility of Our Knowledge Base," *American Historical Review* 124, no. 2 (April 2019): 550–68.

that lurk behind many of them, and the national and economic security interests at stake. Although our search criteria were narrow, they generated a rich body of evidence that reflects poorly on the state of research governance in the United States and portends ominously for the application of our methodology to other domains. The Seven Sons defense research universities share a clear mission to support the PRC's military-civil fusion efforts and defense industrial base, and the cases featured in this chapter substantiate specific, unambiguous links to the PRC's defense programs or classified weapons research. On these facts alone, pursuing S&T research collaborations with Seven Sons universities is unwise and contrary to US national interests.

II. Overview of the PRC's Seven Sons of National Defense (Universities)

The seven universities profiled in this chapter have a long history of supporting the PRC's military programs. From the early 1980s until 2008, they were directly managed by the Commission for Science, Technology and Industry for National Defense (COSTIND; 国防科学技术工业委员会). COSTIND was a PRC State Council (central government) organ responsible for formulating policies and regulations for defense industries. It oversaw the structure and subsequent reorganization of defense enterprises and institutes; drafted annual plans for R&D, production, investment, and "foreign fund utilization" of defense industries; coordinated military procurement; formulated industrial polices and development plans for nuclear, aerospace, aviation, shipbuilding, ordnance, and military electronics industries; and organized "international exchange and cooperation concerning defense industries."[13]

In 2008, the PRC restructured a number of State Council organs and created the Ministry of Industry and Information Technology (MIIT),

13. "2002 年中国的国防'白皮书 [2002 Chinese National Defense White Paper]," 中华人民共和国国防部 [Ministry of National Defense of the People's Republic of China], January 6, 2011, http://www.mod.gov.cn/affair/2011-01/06/content_4249946_4.htm.

which absorbed COSTIND. Since then, MIIT has directly administered the seven defense research universities, often referred to as the "Seven Sons of National Defense" (国防七子) or sometimes the "Seven Schools of National Defense" (国防七校).[14] MIIT's website itself uses this "Seven Sons of National Defense" term, which includes the following institutions:[15]

1. Beijing Institute of Technology (北京理工大学)
2. Beihang University (aka Beijing University of Aeronautics and Astronautics, 北京航空航天大学)
3. Harbin Institute of Technology (哈尔滨工业大学)
4. Harbin Engineering University (哈尔滨工程大学)
5. Northwestern Polytechnical University (西北工业大学)
6. Nanjing University of Aeronautics and Astronautics (南京航空航天大学)
7. Nanjing University of Science and Technology (南京理工大学)

The core missions of these universities include supporting the PRC's military and defense industrial base and its state-directed military-civil fusion efforts. Hence, even if some of the scientific and engineering research that they conduct is in civilian sectors, or is basic or fundamental in nature, it is safe to assume that they will consider military applications as a matter of policy. Consequently, international research collaboration via formal agreements or informal arrangements (known or unknown), student exchanges, or any other form of research facility or resource sharing between US institutions and the Seven Sons universities

14. "国防七校 [Seven Schools of National Defense]," 百度百科 [Baidu Baike], accessed June 13, 2020, https://baike.baidu.com/item/%E5%9B%BD%E9%98%B2%E4%B8%83%E6%A0%A1.
15. 吴志华 [Wu Zhihua], "国防七子"招生就业办领导首秀江西国科 ["National Defense Sevens Sons" Admissions and Job Placement Office Leaders Visit Jiangxi National Defense Technology Military Industry Group for the First Time]," 国家军民融合公共服务平台 [National Military-Civil Fusion Public Service Platform], June 21, 2017, http://jmjh.miit.gov.cn/web/newsInfoWebMessage.action?newsId=493942&moduleId=1062.

Table 1: Number of Articles Published in S&T Journals (January 2013–March 2019) with Seven Sons and US Institutional Coauthorship

PRC University	Articles with US Coauthorship	US Institutions Represented
Harbin Institute of Technology	106	63
Nanjing University of Science and Technology	36	32
Northwestern Polytechnical University	32	28
Beijing Institute of Technology	31	27
Beihang University	28	22
Harbin Engineering University	15	16
Nanjing University of Aeronautics and Astronautics	6	5

demands careful scrutiny. Table 1 summarizes the results yielded by our research methodology.

III. Harbin Institute of Technology: Collaboration with US Research Institutions

A. Summary of Findings

The Harbin Institute of Technology (哈尔滨工业大学, HIT) is a large university that describes itself as "serving national defense" and focuses on aerospace in particular.[16] In the 1960s and 1970s, HIT refocused its mission to "primarily serve national defense construction and military-civil integration." HIT's ties to the PRC's defense research and industrial base include the following:

- A partnership with PRC state-owned defense conglomerate China Aerospace Science and Technology Corporation (CASC). The partnership is known as the Collaborative Innovation Center of Astronautical Science and Technology. It was modeled in part on NASA's Jet Propulsion Laboratory and its members also include

16. "学校简介 [School Overview]," 哈尔滨工业大学 [Harbin Institute of Technology], May 7, 2020, Internet Archive, archived May 14, 2020, accessed June 15, 2020, https://web.archive.org/web/20200514004011/http://www.hit.edu.cn/236/list.htm.

Beihang University (another Seven Sons university), Peking University, and the University of Science and Technology of China.
- Relationships between HIT's School of Astronautics and research institutes of CASC and another state-owned defense firm, China Aerospace Science and Industry Corporation (CASIC), as well as "close collaboration" with the PLA General Armament Department (now known as the Equipment Development Department of the Central Military Commission) and the PLA Rocket Force (previously known as the Second Artillery Force, which manages the PRC's strategic / nuclear missile arsenal).
- Two engineering research centers supporting "national defense science and technology industry."

Research topics in the collected corpus of articles appear to involve a mix of plausibly benign disciplines such as zero energy buildings and environmental and life sciences and dual-use areas such as transportation automation, lithium ion battery development, photovoltaics, materials science, and chemistry. Although the majority of articles identified were in English and some of the published research appear innocuous, supplemental information compiled on select authors and institutional affiliations, primarily from Chinese-language sources, demonstrate that some of the PRC-based entities directly support the PLA, defense industrial organizations, and defense research programs, including what appear to be classified weapons projects. It is not known whether the US partner institutions were a) aware that this research collaboration was taking place; and/or b) had knowledge of the HIT researchers' involvement in PRC defense programs. Examples of this research include the following:

- An article coauthored by HIT and Lawrence Berkeley National Laboratory–affiliated researchers included an HIT faculty member who is involved in PLA General Armament Department research programs and a member of its Stealth Technology Experts Group, as well as two State Administration of Science and Technology Industry for National Defense (SASTIND) projects.

- An article naming Columbia University, University of Texas at San Antonio and HIT-affiliated coauthors included researchers working on projects for the PRC's Central Military Commission S&T Committee, PLA General Staff Headquarters, PLA General Armament Department, and PLA Unit 65927. Some of these projects used "XXXXX" in their title and/or funding codes that may indicate a PRC classified weapons program.
- One article involved Arizona State University collaboration with HIT, Beihang University, and a research institute under state-owned defense conglomerate Aviation Industry Corporation of China (AVIC), which supplies manufacturing technologies for national defense industries such as aerospace, electronics, weaponry, and naval vessels.
- An article coauthored by University of Michigan and HIT researchers on naval engineering included an individual who worked at naval defense conglomerate China Shipbuilding Industry Corporation. At HIT, that researcher has overseen defense projects on topics relating to ship vibration analysis, transmission, or prediction techniques—two of which may have been classified projects given the use of "XXX" in the research grant codes.

A secondary search of CNKI identified seven Chinese-language publications involving HIT that credit the US National Science Foundation (NSF) and the NIH, raising concerns that the PRC may be using US taxpayer-funded research to further the PRC's military modernization efforts. Six of these records are master's theses and doctoral dissertations. Four of the dissertations credit the PRC government-run China Scholarship Council (CSC) for funding their authors' study abroad at US institutions. This suggests that these students used US government-funded research conducted in the United States in partial fulfillment of their advanced degrees at HIT.

B. Overview of HIT and Support to the PRC's National Defense

HIT was founded in 1920 and came under CCP administration in 1950. It is a large university, with three campuses (Harbin, Shenzhen, and

Weihai) totaling more than 43,500 students (of which there are 16,384 graduate students) and more than 6,800 faculty and staff.[17] HIT is involved in a number of scientific and social science disciplines that may not involve defense research, such as architecture, environmental and life sciences, economics, law, humanities, etc., and it has one of the top-ranked engineering programs in the world.[18]

However, at its core, HIT is involved in national defense fields.[19] In the 1960s and 1970s, HIT changed its focus from a "multi-disciplinary technical university" to an institution that "primarily serves national defense construction and military-civil integration" in order to "strengthen the needs of national defense modernization."[20] In particular, HIT claims to have established the PRC's first aerospace academy. Its key contributions to aerospace and defense-related developments include the following:

- Testing of the PRC's first satellite-to-earth high-speed laser communication.
- The first "completely automated laser-target coupling process," used by the Shenguang 3 at the PRC's Laser Fusion Research Center (which conducts inertial confinement fusion research that may have nuclear weapons applications).
- Seven independently developed satellites in the PRC, including the first microsatellite developed and controlled by students.

17. "Harbin Institute of Technology 2017 Brief Introduction," Harbin Institute of Technology Office of Global Affairs, 2017, Internet Archive, archived November 15, 2019, accessed June 15, 2020, https://web.archive.org/web/20191115123613/http://en.hit.edu.cn/pdf/2017HIT%20Brief%20Introduction.pdf.
18. "Best Global Universities for Engineering," *U.S. News & World Report*, accessed June 13, 2020, https://www.usnews.com/education/best-global-universities/engineering.
19. "学校简介 [School Overview]," 哈尔滨工业大学 [Harbin Institute of Technology], 2020.
20. "哈工大精神 [The Spirit of HIT]," 哈尔滨工业大学 [Harbin Institute of Technology], May 16, 2017, Internet Archive, archived May 12, 2020, accessed June 15, 2020, https://web.archive.org/web/20200512095003/https://hit.edu.cn/240/list.htm.

- The first "new system radar."
- The world's first experimental use of a magnetic field Hall thruster for space.
- The world's first microsatellite that conducted a circumlunar flight.
- "Major contributions" to the successful inaugural launches of the Long March 5 and Long March 7 carrier rockets (manufactured by the China Academy of Launch Vehicle Technology (CALT), a unit of the China Aerospace Science and Technology Corporation). [21]

In 2008, HIT founded the Joint Technology Innovation Center in conjunction with CASC. This center became part of the Aerospace Science and Technology Innovation Institute founded two years later and became part of the Collaborative Innovation Center of Astronautical Science and Technology founded in 2012.[22]

An English-language brochure for a 2018 HIT PhD program claimed that HIT's School of Astronautics had established a "close relationship with research institutes in both CASC and CASIC," another major state-owned defense conglomerate. The brochure added that "our school's close collaboration with the PLA General Armament Department and the Second Artillery Force has greatly contributed to the construction of national defense."[23] The PLA's Second Artillery Force (now known as the PLA Rocket Force) is the PRC's strategic missile force, which includes its nuclear weapons arsenal.

HIT also has two engineering research centers directly tied to the PRC's defense industrial base, known in English as the Ultra-Precision Machining Research and Application Center for National Defense Science and Technology Industry, and the Welding Automation Research

21. "学校简介 [School Overview]," 哈尔滨工业大学 [Harbin Institute of Technology], 2020.
22. "Harbin Institute of Technology 2017 Brief Introduction," 2017.
23. "Harbin Institute of Technology-APSCO Full English PhD Program 2018," Harbin Institute of Technology, accessed June 13, 2020, https://uzay.tubitak.gov.tr/sites/images/uzay/1._hit-phd_program-2018_announcement_.pdf.

and Application Center for National Defense Science and Technology Industry.[24] HIT has a number of other research centers (twenty are listed only in Chinese on HIT's website), many of which may support HIT's defense R&D or industrial base. Below are names of some of these centers and approximate English translations, but this is not an exhaustive list of HIT subdivisions that may conduct defense research.[25]

- Research Institute for Gas Dynamics of Engine (发动机气体动力研究中心)
- Control and Simulation Center (控制与仿真中心)
- Analysis and Testing Center (分析测试中心)
- Ceramic Engineering Technology Center (陶瓷工程技术中心)
- Space Debris Hypervelocity Impact Research Center (空间碎片高速撞击研究中心)
- Microelectronics Research Center (微电子研究中心)
- Center for Precision Engineering (精密工程研究中心)
- Electroplating Research Center (电镀研究中心)
- Freespace Optical Communication Technology Research Center (空间光通信技术研究中心)
- Space Control and Inertial Technology Research Center (空间控制与惯性技术研究中心)
- Hydrodynamic Forming Engineering Research Center (液力成形工程研究中心)
- Special Processing Research Center (特种加工研究中心)
- Condensed Matter Physics Science and Technology Research Center (凝聚态科学与技术研究中心)[26]

---

24. Harbin Institute of Technology, "Harbin Institute of Technology 2017 Brief Introduction," 2017, available at: https://educationdocbox.com/Graduate_School/73727462-Harbin-institute-of-technology.html.
25. If HIT supplies an English name, then the authors have used it.
26. "研究所/中心 [Research Institutes and Research Centers]," 哈尔滨工业大学 [Harbin Institute of Technology], June 3, 2018, Internet Archive, archived May 12, 2020, accessed June 15, 2020, https://web.archive.org/web/20200512085553/https://hit.edu.cn/256/list.htm.

HIT aggressively recruits experts from around the world through the PRC's national state-sponsored talent programs. These recruits include 47 specially invited professors (selectees) of the Changjiang Scholars Award Program[27] (a national program to recruit experts from overseas run by the Ministry of Education) and 31 national level "Hundred, Thousand, Ten-Thousand Talents Project" selectees. The university's English-language website omits the latter figure.[28] It also notes that there are 86 "long-term contract overseas experts" and 124 "part-time overseas PhD Supervisors."[29] These last two statistics suggest there are 210 faculty members that retain positions overseas and simultaneously teach and conduct research at HIT, likely fostering some of the research collaboration with foreign institutions and HIT.

HIT also claims that it has signed academic cooperation agreements with 316 institutions of higher education in 35 countries. In 2016, 2,305 HIT students were sent to study overseas and HIT received 2,773 international students from 128 countries and regions.[30] In June 2020, HIT was added to the US Department of Commerce's Entity List for export control purposes, but this may not limit collaboration with US institutions if the research is categorized as fundamental in nature.[31]

C. Survey of Scientific Publications

Bibliographic data was compiled from CNKI using HIT and United States (美国) as search terms in the author affiliations fields. HIT's large size and the diversity of its programs means that some research disciplines may not have any obvious military applications. About half of the 106

27. HIT's English-language website, which is probably not updated as often, states that there are 43 Changjiang Scholars.
28. "学校简介 [School Overview]," 哈尔滨工业大学 [Harbin Institute of Technology], 2020.
29. Harbin Institute of Technology, "2017 Brief Introduction."
30. Harbin Institute of Technology, "2017 Brief Introduction."
31. Bureau of Industry and Security, Commerce, "Addition of Entities to the Entity List, Revision of Entries on the Entity List," *Federal Register* 85, no. 109 (June 5, 2020): 34495, https://www.govinfo.gov/content/pkg/FR-2020-06-05/pdf/2020-10869.pdf.

identified articles in the collected corpus are in fields such as architecture, environmental and civil engineering, new energy technologies, life sciences, and transportation, although some of this research may have dual-use potential. The remainder of the articles are in engineering, computer science, materials science, aeronautical, and aerospace fields that are more closely allied with the PRC's defense industrial and research base. Four examples are profiled below.

Given that the US government views the PRC as a strategic competitor and military rival, collaborations between US government-funded research facilities and programs (e.g. Department of Energy national laboratories) and HIT are presumptively problematic, irrespective of whether the research is intended for beneficial civilian use. It is simply inappropriate for US government facilities to support collaboration with a key PRC defense research institution, especially in the absence of robust vetting.

Within the corpus of 106 articles, thirteen had US government-affiliated coauthors. These articles cover a mix of seemingly innocuous research areas such as zero energy buildings and environmental and life sciences, and potential dual-use areas such as transportation automation, lithium ion battery development, photovoltaics, materials science, and chemistry. Just the same, supplemental research reveals that some of the PRC-based coauthors have directly supported PLA and defense programs, including what appears to be classified weapons projects.

Example 1: Lawrence Berkeley National Laboratory Collaboration with HIT

A superficial examination of an English-language article that names authors affiliated with HIT and the Department of Energy's (DoE) Lawrence Berkeley National Laboratory's (LBNL) Plasma Applications Group and Molecular Foundry may not identify national security concerns.[32] The article published in 2013 entitled "Transparent and conductive indium doped cadmium oxide thin films prepared by pulsed filtered cathodic arc deposition," credits DoE funding via the "LDRD Program

32. Also found in Elsevier's ScienceDirect.

of LBNL, in-part by the Assistant Secretary for Energy Efficiency and Renewable Energy under Contract No. DE-AC02-05CH11231" and a "user project at the LBNL Molecular Foundry supported by the Office of Science, Office of Basic Energy Sciences."[33] However, examination of the HIT-affiliated authors reveal direct ties to PRC defense programs.

No further information was found on one of the authors who claims dual LBNL and HIT affiliation. It is possible that this author was a visiting PhD student while conducting studies at HIT based on the fact that a) the article credits the "PhD Programs Foundation" of the PRC's Ministry of Education for funding support, and b) other coauthors appear to hold faculty positions.[34]

This publication's most concerning aspect relates to a second HIT-affiliated coauthor. A PRC website posted what appears to be this author's complete curriculum vitae (CV), indicating that he is a professor and doctoral advisor at HIT's School of Astronautics, where he conducts research on photonics and thin film-related materials science. He has worked with the (formerly named) PLA General Armament Department on multiple projects. Specifically, the CV lists "major positions" and research projects that should presumptively disqualify him from participation in US government-funded research:

- Served as a PLA General Armament Department Stealth Technology Experts Group Member
- Served as a PLA General Armament Department Military Use Electronic Components Technology Expert Evaluator
- Oversaw five PLA General Armament Department Preliminary Research Fund projects (总装预研基金 5 项) and two Preliminary Research Plan projects (总装预研计划 2 项)

33. Yuankun Zhu, Rueben J. Mendelsberg, Jiaqi Zhu, Jiecai Han, and André Anders, "Transparent and Conductive Indium Doped Cadmium Oxide Thin Films Prepared by Pulsed Filtered Cathodic Arc Deposition," *Applied Surface Science* 265 (January 2013): 738–44, https://doi.org/10.1016/j.apsusc.2012.11.096.

34. This is consistent with other articles surveyed in this study, in which individuals claiming dual US- and China-based affiliations were temporarily based in the United States as graduate students or postdoctoral researchers.

- Oversaw two SASTIND military products projects, multiple aerospace and aviation projects, and "[unnamed] Major National Science, Technology, and Engineering Fundamental Research Projects" (the lack of specificity on the latter may refer to classified research programs)[35]

A third HIT-affiliated researcher named in this article has coauthored many publications and filed patents with the second HIT author and may well be carrying out similar research supporting the PRC's military programs.

Example 2: Columbia University, University of Texas at San Antonio Collaboration with HIT and Harbin Engineering University

The second article, entitled "Weakly supervised codebook learning by iterative label propagation with graph quantization," was published in 2013 in the English-language journal *Signal Processing*. The article lists authors affiliated with HIT, Harbin Engineering University, Columbia University, and the University of Texas at San Antonio.[36]

The three PRC-affiliated coauthors appear to have professional connections to each other, and two have participated in numerous PRC defense research programs. At the time of the article's publication, the author affiliated with Harbin Engineering University (another Seven Sons university) was completing a PhD degree. This coauthor is now an associate professor at Xiamen University's Computer Science department and conducts research on spatial data science, remote sensing image interpretation, cloud data management, and multimedia content retrieval.[37]

---

35. "哈尔滨工业大学研究生导师简介-朱嘉琦 [Harbin Institute of Technology Graduate Student Supervisors-Zhu Jiaqi]," FREE 研究生招生 [FREE Graduate Student Recruitment], April 1, 2016, http://school.freekaoyan.com/heilongjiang/hit/daoshi/2016/04-01/1459455102545914.shtml.
36. Liujuan Cao, Rongrong Ji, Wei Liu, Hongxun Yao, and Qi Tian, "Weakly Supervised Codebook Learning by Iterative Label Propagation with Graph Quantization," *Signal Processing* 93, (August 2013): 2274–83, https://doi.org/10.1016/j.sigpro.2012.05.001.
37. "曹刘娟 副教授 [Associate Professor Cao Liujuan]," School of Informatics, Xiamen University, accessed June 13, 2020, https://information.xmu.edu.cn/info/1019/3182.htm.

The other PRC-based coauthors have more direct ties to defense programs. One of the authors claimed both a Columbia University and HIT affiliation for this article. According to biographical information posted on his current employer's website (Xiamen University), he received a PhD in 2011 from HIT, where he worked with his advisor (the third PRC-based coauthor of this article). From late 2010 through 2013, the former held a postdoctoral researcher position at Columbia University.[38] He is currently employed at Xiamen University's School of Information Science and Technology and is a 2017 "youth" selectee of the PRC government-run Ten-Thousand Talents Program.[39] Notably, he has worked on several defense projects, including the following:

- A "Central Military Commission S&T Committee High Technology Special Project."
- Preliminary research under the 13th Five-Year Plan for the PLA General Staff Headquarters
- Preliminary research under the 12th Five-Year Plan for the PLA General Armament Department
- Technology development projects in partnership with Tencent, Huawei, and DiDi[40]

Although it is not known if the research on behalf of Huawei, Tencent, and DiDi overlapped or was integrated with the defense special projects this coauthor conducted, its striking appearance among them underscores how research collaborations with US institutions may contribute to the development of dual-use technologies in the PRC and benefit PRC firms at the expense of US economic competitiveness.

Lastly, the third PRC-based coauthor is a professor at HIT's School of Computer Sciences Center for Intelligent and Human Machine Interface. This professor's CV lists work on multiple defense research projects,

38. "纪荣嵘 [Ji Rongrong]," Media Analytics and Computing Lab, Xiamen University, 2020, accessed June 13, 2020, http://mac.xmu.edu.cn/rrji-cn.html.
39. "纪荣嵘 [Ji Rongrong]."
40. "纪荣嵘 [Ji Rongrong]."

including those listed below. The use of "X" in project names or funding codes likely refers to classified programs.

- PLA General Armament Department "Panoramic View XXXXXX System Preliminary Research Project" (Mar. 2011-Dec. 2015)
- PLA Unit 65927 "Border Crossing Automated Warning System" project (Jan. 2007-Dec. 2009)
- MIIT "242 Project" (no title provided) with funding code "XXXXX (2005C41)"[41]

Given that both HIT-affiliated coauthors are actively involved in defense research programs, some of which are directly under the PLA, it would be prudent to assume that the research published in collaboration with US universities will also flow directly to the PRC military. Because the background information about these coauthors was derived exclusively from Chinese-language sources, it is not known if the US universities were aware of their associations with the PLA. Assuming that the collaboration complied with US export controls, this case demonstrates the inadequacy of that standard as a test for assessing risk.

Example 3: Arizona State University Collaboration with HIT, PRC Aerospace Defense Conglomerate

An English-language article published in 2017 entitled "Effect of gallium addition on the microstructure and micromechanical properties of constituents in Nb-Si based alloys" had eight contributing authors, some of whom are affiliated with HIT, Beihang University, and AVIC.[42] Supplemental research on the PRC-based authors and institutions demonstrates clear ties to the PRC's defense research and industrial base.

---

41. "姚鸿勋 [Yao Hongxun]," Harbin Institute of Technology, accessed June 13, 2020, http://homepage.hit.edu.cn/yaohongxun.
42. Enyu Guo et al., "Effect of Gallium Addition on the Microstructure and Micromechanical Properties of Constituents in Nb-Si Based Alloys," *Journal of Alloys and Compounds* 704, (May 2017): 89–100, https://doi.org/10.1016/j.jallcom.2017.02.054.

The article lists eight authors affiliated with one or more of the following institutions:

1. Materials Science and Engineering, Arizona State University (ASU)
2. School of Materials Science and Engineering, Harbin Institute of Technology
3. International Research Institute for Multidisciplinary Science, Beihang University
4. AVIC Beijing Aeronautical Manufacturing Technology Research Institute (BAMTRI)
5. Department of Materials Science and Engineering, Indian Institute of Technology, Kanpur, Uttar Pradesh

One of the two HIT-affiliated authors has been an associate researcher at HIT's School of Materials Science and Engineering since late 2013 and specializes in titanium and aluminum alloys. That author has worked with or at HIT's National Key Laboratory for Precision Hot Processing of Metals and, according to his faculty page, has worked on "national defense preliminary projects."[43]

Supplemental searches on CNKI's web interface indicate that the AVIC-affiliated researcher has coauthored a number of articles with the aforementioned HIT scientist and conducted similar research at BAMTRI. BAMTRI is the headquarters component of the Aviation Industry Corporation of China (AVIC) Manufacturing Technology Institute (MTI).[44]

MTI's English-language page states that this AVIC subsidiary focuses on "fundamental, application [*sic*], engineering, industrialization R&D of aeronautical materials, manufacturing technologies and special equipment" for new aircraft and aero-engines and provides support to "aerospace, electronics, ship, defense, and other industries." MTI houses key laboratories that involve "additive manufacturing, welding and joining,

43. "骆良顺 [Luo Liangshun]," Harbin Institute of Technology, accessed June 13, 2020, http://homepage.hit.edu.cn/luols.

44. BAMTRI is on the Department of Commerce's Entity List.

digital manufacturing, metal forming, precise manufacturing, and high performance electro-magnetic windows."[45]

MTI's Chinese-language page describes itself as a "comprehensive research organ specializing in aviation and national defense advanced manufacturing technologies and special use equipment development." BAMTRI is also known as the AVIC 625 Institute (625所) and develops "transformational research for the PRC's new and emerging airplanes, engines, cruise missiles, and related aviation equipment." BAMTRI supplies "advanced manufacturing technologies for national defense industries such as aerospace, electronics, weaponry, ships, etc." Lastly, the organization claims to have "long-standing technology exchanges and economic cooperative relations with 30+ countries," including the US, Russia, Germany, France, Italy, and Japan.[46]

Example 4: University of Michigan Collaboration with HIT on Naval Engineering

The last article examined—also an English-language publication available on Elsevier's website—was published in January of 2019 and named coauthors from HIT's College of Naval Architecture and Ocean Engineering (Weihai campus) and the University of Michigan's Department of Naval Architecture and Marine Engineering. Entitled "Numerical and experimental analysis of hydroelastic responses of a high-speed trimaran in oblique irregular waves,"[47] some of its authors have backgrounds in defense research projects.

One of the authors claimed a dual affiliation with the University of Michigan and HIT. The version of that author's CV that appears on

45. "MTI Profile," AVIC Manufacturing Technology Institute, accessed June 13, 2020, http://www.avicmti.avic.com/enweb/aboutus/mtip/index.shtml.
46. "制造院简介 [Introduction to the Manufacturing Technology Institute]," AVIC Manufacturing Technology Institute, accessed June 13, 2020, http://www.avicmti.avic.com/gxwm/zcyjg/index.shtml.
47. Zhanyang Chen, Hongbin Gui, Pingsha Dong, and Changli Yu, "Numerical and Experimental Analysis of Hydroelastic Responses of a High-Speed Trimaran in Oblique Irregular Waves," *International Journal of Naval Architecture and Ocean Engineering* 11 (January 2019): 409–21, https://doi.org/10.1016/j.ijnaoe.2018.07.006.

HIT's website, however, makes no mention of the University of Michigan affiliation. The CV states the author began his studies at HIT in 2004 and received BS and PhD degrees (completed December 2013) from the College of Naval Architecture and Ocean Engineering. Beginning April of 2014, he was employed by the same department at HIT.[48] This author has partnered with another of the article's HIT-affiliated coauthors on at least one other publication that involved naval research, which also included a Harbin Engineering University-affiliated professor.[49]

The other PRC-based author serves as vice dean of HIT's College of Naval Architecture and Ocean Engineering.[50] Interestingly, this author's faculty profile on HIT's website is not viewable from US-based internet points of presence. However, Chinese Baike—a PRC analog to Wikipedia hosted by search engine and internet firm Baidu—provides biographical information on the author and some of his research projects. According to this source, he served as a senior engineer at a major state-owned defense firm (China Shipbuilding Industry Corporation's 702nd Research Institute) from 2003 to 2008. He subsequently worked at HIT as a professor, department head, and since July 2014, as vice dean of its College of Naval Architecture and Ocean Engineering. He has overseen defense research projects on topics relating to ship vibration analysis, transmission, or prediction techniques.[51] A sampling of these research projects include the following:

---

48. "陈占阳 [Chen Zhanyang]," Department of Postgraduate, Harbin Institute of Technology at Weihai, accessed June 13, 2020, http://yjsc.hitwh.edu.cn/2017/0517/c1096a41314/page.htm.
49. 陈占阳 [Chen Zhanyang] et al., "舰船非线性设计值的水弹性直接计算方法 [Direct Calculation Method for Nonlinear Design Loads of Warship Based on Hydroelasticity Theory]," 哈尔滨工程大学学报 [*Journal of Harbin Engineering University*], 38, (January 2019): 37–42, https://doi.org/10.11990/jheu.201507066.
50. "海洋工程学院 [Marine Engineering School]," Harbin Institute of Technology at Weihai School of Marine Engineering, accessed June 13, 2020, http://snaoe.hitwh.edu.cn/41/list.htm.
51. "桂洪斌 [Gui Hongbin]," 百度百科 [Baidu Baike], accessed June 14, 2020, https://baike.baidu.com/item/%E6%A1%82%E6%B4%AA%E6%96%8C#reference-[1]-4416584-wrap.

- 863 Program (a national level R&D program that supports defense research) project on optimal design of subsurface systems and marine instrumentation
- Two research grants listed only as "XXX" (probably referring to classified research) associated with the PLA Navy Equipment Department
- China Shipbuilding Industry Corporation-sponsored project on "submarine vibration and acoustic radiation prediction techniques."[52]

D. Secondary Search: US Research Funding

A second set of searches of CNKI bibliographic records examined articles that named a US institution as providing funding support and at least one author affiliated with HIT. Seven Chinese-language publications were identified, including six theses and dissertations published at HIT and one article that appeared in a scientific journal shown in Table 2. The English translations of the titles were provided by the authors of the publications. Five of the records claim US NSF support; one claims involvement in a "China-US International Cooperation Project," and one claims US NIH funding. Unfortunately, it matters little if the authors reported their HIT affiliations to these funding institutions, because the institutions typically lack the mandate and toolset to properly assess the significance of those disclosures.

E. Observations on Identified Theses and Dissertations

Four of these titles, three of which are PhD dissertations, credit CSC funding for supporting their authors' study abroad. The NSF and NIH funding sources identified in the dissertations indicate that the authors used US government-funded research conducted in the United States towards partial fulfillment of their PhD degree requirements from HIT. Quite possibly, these students were working under recipients of NSF and NIH funding (i.e., principal investigators) and were compensated by the

52. "桂洪斌 [Gui Hongbin]."

Table 2: Research Naming US Funding Support and HIT Author Affiliation

Title	Organizations	Source	Funding*
数控无心磨床能量特性与等效碳排放量的建模与分析 (Modeling and Analysis of Energy Characteristics and Equivalent Carbon Emissions of CNC Centerless Grinding Machine)	HIT	HIT (June 2018 master's thesis)	China National Natural Science Foundation; China-US International Cooperation Project
基于角度坐标描述的三维柔性大变形梁动力学建模方法研究 (Research on Three-Dimensional Flexible-Large Deformation Beam Formulations Based on Rotational Coordinate [*sic*] Descriptions)	HIT	HIT (July 2017 PhD dissertation)	China National Natural Science Foundation; US NSF
双乳液滴内核可控包裹与融合机制及实验研究 (Mechanism and Experimental Research on Controllable Encapsulation and Coalescence of Inner Droplets in Double-Emulsion Drops)	HIT	HIT (June 2017 PhD dissertation)	CSC; China National Natural Science Foundation; US NSF
细菌运动中的物理生物学 (Physical Biology of Bacterial Motility)	HIT; China University of Science and Technology; Chinese University of Hong Kong and Chinese University of Hong Kong Shenzhen Research Institute; Brown University	(2016) Journal of Physics (aka Acta Physica Sinica) (物理学报)	US NSF (award CBET 1438033); Chinese Academy Sciences Institute of Theoretical Physics State Key Laboratory of Theoretical Physics Fund (Y4KF161CJ1); CSC; China National Natural Science Foundation (11374282, 21573214, 21473152); Research Grants Council of Hong Kong Special Administrative Region (CUHK409713)
集成微流控芯片及单细胞基因表达检测研究 (Integrated Microfluidic Chips for Single-Cell Gene Expression Profiling)	HIT	HIT (September 2015 PhD dissertation)	CSC; US NIH
基于交流电场的生物分子快速检测及其实验研究 (AC Electric Field Based Rapid Detection of Biomolecules and Experimental Studies)	HIT	HIT (2014 PhD dissertation)	CSC; China National Natural Science Foundation; US NSF; Zhejiang University State Key Laboratory of Fluid Power Transmission and Control Development Fund
聚苯胺及其纳米复合材料巨磁阻性能研究 (Giant Magnetoresistance in Polyaniline and Its Nanocomposites)	HIT	HIT (December 2013 PhD dissertation)	China National Natural Science Foundation; US NSF

* The authors of this study provided translations of the PRC funding grants when no English was provided.

PRC government to do so via the CSC. Details on four of the five dissertations follow; no additional information on the fifth was found.

- The July 2017 dissertation was submitted to HIT's School of Astronautics. Its author studied at the University of Maryland Baltimore Campus from December 2014 to December 2016.[53]
- The June 2017 dissertation was submitted to HIT's School of Mechatronics [*sic*] Engineering.[54] Its author was affiliated with HIT's Robotics and Systems National Key Laboratory and studied at the University of Pennsylvania from September 2013 to September 2015.
- The September 2015 dissertation was submitted in support of HIT's Aeronautics and Astronautics Manufacturing Engineering program. The author attended Columbia University from September 2012 to September 2014 as a visiting PhD student, and specifically named three NIH grants that supported the dissertation: 5U19AI067773, 8R21GM104204, 2P41EB002033-19A1.[55] The first

53. 樊伟 [Fan Wei], "[基于角度坐标描述的三维柔性大变形梁动力学建模方法研究] Research on Three-Dimensional Flexible Large-Deformation Beam Formulations Based on Rotational Coordinate Descriptions" (PhD diss., Harbin Institute of Technology, 2017), http://new.oversea.cnki.net/KCMS/detail/detail.aspx?dbcode=CDFD&dbname=CDFDLAST2019&filename=1018897420.nh&v=Mjg0MzgvQVZGMjZGcnV4R2RYT3I1RWJQSVI4ZVgxTHV4WVM3RGgxVDNxVHJXTTFGckNVUjdxZlllZHBGeTNrV3I=.
54. 侯立凯 [Hou Likai], "双乳液滴内核可控包裹与融合机制及实验研究 [Mechanism and Experimental Research on Controllable Encapsulation and Coalescence of Inner Droplets in Double-Emulsion Drops]" (PhD diss., Harbin Institute of Technology, 2017), http://new.oversea.cnki.net/KCMS/detail/detail.aspx?dbcode=CDFD&dbname=CDFDLAST2018&filename=1017862365.nh&v=Mjk1NjNVUjdxZlllZHBGeTNrV3IvSVZGMjZHYnUrSE5MS3FwRWJQSVI4ZVgxTHV4WVM3RGgxVDNxVHJXTTFGckM=.
55. 孙浩 [Sun Hao], "集成微流控芯片及单细胞基因表达检测研究 [Integrated Microfluidic Chips for Single-Cell Gene Expression Profiling]" (PhD diss., Harbin Institute of Technology, 2017), http://new.oversea.cnki.net/KCMS/detail/detail.aspx?dbcode=CDFD&dbname=CDFDLAST2017&filename=1016739476.nh&v=MDUyOTFMcVpFYlBJUjhlWDFMdXhZUzdEaDFUM3FUcldNMUZyQ1VSN3FmWWVkcEZ5M2tXNy9MVkYyNkdMUzdGOVg=.

grant deals with developing rapid methods to identify individuals who have significant exposure to radiation, especially from an improvised nuclear device or dirty bomb.[56]

- The December 2013 dissertation was submitted to HIT's School of Chemical Engineering and Technology. Another 2013 article coauthored by this PhD student shows him affiliated with HIT and Lamar University (perhaps as a visiting PhD student).

Again, only a small subset of the corpus of 106 articles was examined here. Research on the affiliations and authors of the other articles may identify additional instances in which US government funding agencies are supporting researchers at universities integral to the PRC defense establishment.

IV. Nanjing University of Science and Technology: Collaboration with US Research Institutions

A. Summary of Findings

The Nanjing University of Science and Technology (南京理工大学, NJUST) was originally founded in 1953 as the PLA Engineering Institute. After relocating to Nanjing in 1962, NJUST has been focused on developing weapons technologies and related systems.

- NJUST has a nationally designated discipline in "weapons science and technology construction," and has created ten "special national defense disciplines" and nine "national defense science and technology innovation teams."
- NJUST's School of Energy and Power Engineering integrates numerous defense disciplines, including ordnance firing theory and technology, weapons systems and applications engineering, fluid dynamics, and engineering thermophysics.

56. David J. Brenner, "Center for High-Throughput Minimally-Invasive Radiation Biodosimetry," National Institutes of Health, accessed June 14, 2020, http://grantome.com/grant/NIH/U19-AI067773-12.

- Seven out of thirty-five articles that have authors affiliated with NJUST and US institutions name NJUST's School of Energy and Power Engineering. Supplemental research on an NJUST-affiliated coauthor listed in six articles reveals that he conducts ordnance firing, ballistics, and weapons systems research.
- A NJUST doctoral dissertation credits the US NSF but does not identify which US university hosted that NSF-funded research.

B. Overview of NJUST and Support to the PRC's National Defense

NJUST was originally founded as the PLA Engineering Institute (中国人民解放军军事工程学院, or Institute of Military Engineering) in 1953. In 1962, the university relocated to Nanjing, and after some restructuring and name changes, became known as the Nanjing University of Science and Technology.[57] The Chinese-language website offers more details on NJUST's defense-related missions. For example, it states that the university has a long history of developing weapons and equipment, electronics, information technology, and chemical and materials science disciplines for national defense purposes. In 2017, NJUST was selected as a "Double First-Class discipline" university in "weapons science and technology construction."[58] This refers to the Double First Class University Plan that the PRC government initiated in 2015 in order to foster a group of elite PRC universities and individual university departments into world class universities and disciplines by the end of 2050.[59] NJUST

57. "Overview," Nanjing University of Science and Technology, accessed June 14, 2020, http://english.njust.edu.cn/582/list.htm.
58. "学校简介 [School Overview]," 南京理工大学 [Nanjing University of Science and Technology], April 2020, http://www.njust.edu.cn/3627/list.htm.
59. 国务院 [State Council], "统筹推进世界一流大学和一流学科建设总体方案 [Overall Plan to Promote the Construction of World-Class Universities and First-Class Disciplines]" Document 64, October 24, 2015, http://www.gov.cn/zhengce/content/2015-11/05/content_10269.htm.; "China sets direction for world class universities," Commonwealth of Australia, Department of Education, Skills and Employment, accessed June 14, 2020, https://internationaleducation.gov.au/News/Latest-News/Pages/China-sets-direction-for-world-class-universities.aspx.

has designated ten "special national defense disciplines" and nine "national defense science and technology innovation teams." The university also has four award recipients of the "outstanding youth talent fund for national defense science and technology" (国防科技卓越青年人才基金获得者 4 人).[60]

NJUST's School of Energy and Power Engineering is focused on weapons and defense research. Its predecessor was the Ballistics Research Institute (弹道研究所), established in 1981 by the then Ministry of Ordnance Industry. In 2010, the school was restructured into the current School of Energy and Power Engineering. The school integrates numerous defense disciplines such as ordnance firing theory and technology, which was designated as a national "Double First Class" discipline in 2017. Its weapons systems and firing engineering major is designated as a "national special major" (国家特色专业). The school runs two postdoctoral programs on weapons science and technology and mechanics and four doctoral degree programs in weapons science and technology, mechanics, control science and engineering, and engineering thermophysics. Master's degree programs involving defense areas include the following: ordnance firing theory and technology, weapons systems and applications engineering, engineering thermophysics, fluid dynamics, engineering mechanics, refrigeration and cryogenic engineering, electronics systems and automation, and ordnance engineering. Lastly, the school claims to have a long history of conducting civilian- and military-use technologies and is "anchored" to the China Ordnance Society's Specialty Committee on Ballistics.[61]

Like the other MIIT universities, NJUST recruits experts globally. NJUST claims to have three "foreign academicians" on its faculty, eighteen selectees of the Changjiang Scholars Award Program, and

60. "学校简介 [School Overview]," 南京理工大学 [Nanjing University of Science and Technology], 2020.

61. "学院简介 [School Overview]," 南京理工大学动力工程学院 [Nanjing University of Science and Technology School of Energy and Power Engineering], September 2019, http://nd.njust.edu.cn/1845/list.htm.

fourteen selectees of the Hundred, Thousand, and Ten-Thousand Talents Program.[62]

C. Survey of Scientific Publication Records

A total of thirty-five articles were identified that contained coauthors from US institutions and NJUST. As NJUST's School of Energy and Power Engineering is engaged in weapons development, articles that listed authors affiliated with that division merit closer scrutiny. One of the authors appeared in six articles from this corpus. In addition, a secondary search of US funding sources named on NJUST-authored publications revealed one doctoral dissertation. No biographical information was found on its author, but the dissertation published at NJUST credits the US NSF for research support.

Example: NJUST School of Energy and Power Engineering

Publications with authors from NJUST's School of Energy and Power Engineering appeared in seven articles in the collected corpus along with US-based coauthors from the University of Minnesota, Twin Cities, the University of Michigan, and the University of Texas at Austin. Six of the seven publications had the same PRC coauthor.

One of them, published in 2016, includes a UT Austin faculty author, a NJUST faculty author, and a PhD student with both affiliations.[63] Although the article specifies that the student's NJUST affiliation was with the School of Energy and Power Engineering, that appears to have been a ruse. Two years earlier, the student published an article in the journal of another Seven Sons university entitled "An intelligent anti-removal system for blockade mines." The affiliation given in that article was the Ministerial Key Laboratory of Intelligent Ammunition under

62. "学校简介 [School Overview]," 南京理工大学 [Nanjing University of Science and Technology], 2020.

63. Yujia Sun et al., "Evaluation of Three Different Radiative Transfer Equation Solvers for Combined Conduction and Radiation Heat Transfer," *Journal of Quantitative Spectroscopy & Radiative Transfer* 184 (2016): 262–73, http://dx.doi.org/10.1016/j.jqsrt.2016.07.024.

NJUST's School of Mechanical Engineering, and in 2019 the student in fact graduated from that school.[64]

The NJUST faculty author received a PhD in ballistics from NJUST in 1995. In 2002–03, he was a visiting scholar at Carnegie Mellon University pursuant to a PRC national study abroad program, which very likely refers to the CSC. In 2008, the researcher began serving as vice dean of the School of Energy and Power Engineering. He specializes in research related to interior ballistics theory and applications, multiphase flow theory and applications, and new types of point fire technologies.[65] He works on "preliminary national defense research" and was a recipient of the Eighth China Ordnance Society Youth Science and Technology Award.[66] Among his other distinctions, he is director-general of the China Ordnance Society's Specialty Committee on Ballistics, a standing member of the Jiangsu Academy of Military Industry, and a correspondent for the PRC *Journal of Artillery Launch and Control*.

In addition to the six articles in this corpus, this NJUST vice dean has coauthored other publications with purely PRC-based collaborators. Two of these articles directly relate to weapon designs (ballistics) and both name NJUST's National Key Laboratory of Transient Physics (瞬态物理国家重点实验室) as their funding source.[67]

---

64. 孙宇嘉 [Sun Yujia], "封锁雷智能防排系统 [An Intelligent Anti-removal System for Blockade Mines], 哈尔滨工程大学学报 [Journal of Harbin Engineering University], 35, no. 5 (2014): 580–84, http://doi.org/10.3969/j.issn.1006-7043.201303071.
65. In 2008, the division was referred to as the School of Power Engineering.
66. The official award in Chinese is 第八届中国兵工学会青年科技奖. "能动学院教师简介—张小兵 [School of Energy and Power Engineering Professor-Zhang Xiaobing]," 南京理工大学动力工程学院 [Nanjing University of Science and Technology School of Energy and Power Engineering], March 11, 2015, http://nd.njust.edu.cn/25/9c/c1905a9628/page.htm.
67. 程诚 [Cheng Cheng] and 张小兵 [Zhang Xiaobing], "某制导炮弹二维两相流内弹道性能分析与数值模拟研究 [Two-Dimensional Numerical Simulation on Two-Phase Flow Interior Ballistic Performance of a Guided Projectile]," 兵工学报 [*Acta Armamentarii*] 36, no. 1 (2015): 58–63, http://doi.org/10.3969/j.issn.1000-1093.2015.01.009; 罗乔 [Luo Qiao] and 张小兵 [Zhang Xiaobing], "基于 FLU-

The National Key Laboratory of Transient Physics (NKLTP) began its operations in 1995 under COSTIND authorities and serves as NJUST's "research platform" for the "national key discipline of ordnance firing theory and techniques." Its website claims NKLTP has created an "interdisciplinary research system" of theoretical, fundamental, and applied research and information technologies related to ultra-high firing mechanics, flight dynamics, chemical kinetics, fluid dynamics, explosive mechanics, modern damage mechanics, guidance and control, plasma physics, engineering thermophysics, high simulation technology, and transient testing technologies. The laboratory claims that it has undertaken two hundred national scientific research projects and more than one hundred "other" projects, published more than seven hundred articles, and filed more than twenty patents. NKLTP has won a National Defense Science and Technology Prize, a National Defense Technology Invention prize, and an Army Science and Technology Progress award.[68]

V. Northwestern Polytechnical University: Collaboration with US Research Institutions

A. Summary of Findings

Northwestern Polytechnical University (西北工业大学, NWPU) runs education and research programs in aeronautics, astronautics, and marine technology engineering "dedicated to national defense," and it promotes military-civil fusion policies. NWPU's School of Aeronautics was formed from the former Harbin Military Engineering Institute and

ENT 软件和内弹道模型双向耦合的超高射频火炮发射过程模拟 [Simulation for Launch Process of Ultrahigh Firing Rate Guns Based on Two-Way Coupling of FLUENT and Interior Ballistic Model]," 兵工学报 [*Acta Armamentarii*] 37, no. 10 (2016): 1949–55, http://doi.org/10.3969/j.issn.1000-1093.2016.10.023.

68. "瞬态物理国家重点实验室 [National Key Laboratory of Transient Physics]," 南京理工大学瞬态物理国家重点实验室 [Nanjing University of Science and Technology National Key Laboratory of Transient Physics], December 12, 2019, http://zdsys.njust.edu.cn/38/bb/c2552a14523/page.htm.

is involved in "almost all major aircraft and spacecraft development of China," including fighter jets, large transport aircraft, near space flight vehicles, and new-concept aircraft and drone projects.[69]

Supplemental information compiled on select authors and institutional affiliations, primarily from Chinese-language sources, demonstrates that some of the NWPU-based entities collaborating with US institutions oversee numerous defense research and engineering programs and develop potential surveillance capabilities for the People's Armed Police (PAP). The PAP is a paramilitary police force under the direct authority of the CCP Central Committee and its Military Affairs Commission. The PAP performs domestic security and surveillance functions to support the CCP's authoritarian control over the PRC population. NWPU is on the US Department of Commerce's Entity List for export control purposes, but this may not limit collaboration with US institutions if the research is categorized as fundamental in nature.

- Several NWPU-affiliated coauthors have overseen PLA research projects, won National Defense Science and Technology Awards, and have been involved in projects that are likely classified weapons programs given the "XXX" designators in their project titles. Projects include research into computational software systems integration, high-speed wind tunnels, fluid dynamics, and aerodynamics.
- One article named a coauthor affiliated with a missile design and production subsidiary, CALT, which is subordinate to a major defense conglomerate, the China Aerospace Science and Technology Corporation (CASC).
- Another article named researchers from NWPU, a US university, and the Xi'an Engineering College of the People's Armed Police, raising ethical concerns over the potential applications of this

69. "Overview," Northwestern Polytechnical University School of Aeronautics, Internet Archive, archived September 13, 2019, accessed June 15, 2020, https://web.archive.org/web/20190913235933/http://hangkong.nwpu.edu.cn/home/overview/view.htm.

research. No biographical data was found on the PAP-affiliated coauthor, raising questions about the background information the partnering US institution could have gathered about this individual.

- Several identified articles use incomplete or innocuous sounding English-language names for a defense laboratory in NWPU's School of Aeronautics in an apparent attempt to obfuscate its ties to defense programs.
- Four identified English-language articles list coauthors affiliated with US government institutions, including the NIH, the DoE, and the US Naval Research Laboratory (NRL). Although the research associated with these articles may be benign in nature, the NWPU coauthors are affiliated with departments that conduct defense research projects. Two other articles were found that credited NIH and NSF funding, yet these articles only appear in Chinese-language sources. Consequently, federal agencies may be unaware that research results were being published in the PRC.

B. Overview of NWPU and Support to the PRC's National Defense

NWPU claims to be the only research institution in the PRC that simultaneously runs education and research programs in aeronautics, astronautics, and marine technology engineering. As an MIIT-designated Seven Sons university, NWPU's website states that it is "dedicated to national defense." NWPU is the result of several mergers of older schools and departments, in this case dating back to 1938. NWPU's current name was designated in 1957, having previously been named the Northwestern Institute of Engineering.[70] In addition, the PLA's Air Force Engineering Department of the former Harbin Military Engineering Institute was merged into NWPU in 1970 and is now part of NWPU's School of Aeronautics.[71]

---

70. "History of NPU," 西北工业大学 [Northwestern Polytechnical University], accessed June 14, 2020, http://en.nwpu.edu.cn/EnglishNew/AboutNPU/History.htm.
71. "Overview," Northwestern Polytechnical University School of Aeronautics.

NWPU states that it was one of the first universities to establish a graduate school and a national university science park; it now hosts the Northwestern Institute of Industrial Technology and the PRC's top UAV (uncrewed aerial vehicle) Research and Development Base.[72] NWPU also houses eight state key laboratories, two national engineering research centers, four national and international S&T cooperation bases, one National Defense S&T Innovation Center, and eight "national defense innovation teams." These entities are involved in large aircraft, manned spaceflight, aerospace manufacturing engineering, flight mechanics, aero-engines, naval and submarine weapons, and rocket engines. NWPU also claims to hold an "important position in shipbuilding and naval weapons industries."[73]

The School of Aeronautics clearly plays a key role in NWPU's defense programs and touts well-known graduates of the school, such as: Yang Wei, chief designer of the PRC's "new-generation fighter aircraft;" Tang Changhong, chief designer of large aircraft; and Chen Yong, chief designer of the PRC's next-generation regional transport aircraft (the ARJ21). The school also claims that faculty and students have participated in "almost all major aircraft and spacecraft development of China," including the J7E (fighter jet), large transport aircraft, near space flight vehicles, and new-concept aircraft and UAV projects.[74]

NWPU also boasts that it houses the PRC's only national key laboratory for special drone technology and a national engineering center for drone systems. The university built Asia's largest satellite ground control station, the PRC's first small drone, and the first 50kg underwater autonomous vehicle.[75]

---

72. "History of NPU," 西北工业大学 [Northwestern Polytechnical University], 2020.
73. "学校简介 [School Overview]," 西北工业大学 [Northwestern Polytechnical University], December 2019, http://www.nwpu.edu.cn/xxgk/xxjj.htm.
74. "学校简介 [School Overview]," 西北工业大学 [Northwestern Polytechnical University].
75. "学校简介 [School Overview]," 西北工业大学 [Northwestern Polytechnical University].

NWPU seeks to accelerate technology transfer and promotes military-civil integration policies. For example, NWPU has built platforms for collaboration with the PRC's major defense conglomerates, and in partnership with the Ministry of Science and Technology established an S&T Military-Civil Fusion Evaluation Research Center. Below the national level, NWPU also houses the Shaanxi (Provincial) Military-Civil Fusion Training Base and the Shaanxi Military-Civil Fusion Evaluation Center.[76]

NWPU is involved in considerable international collaboration efforts, claiming to have agreements with 280 schools overseas and ten national-level international cooperation platforms. These platforms include four national-level international S&T cooperation bases and six innovative talent introduction bases.[77]

NWPU is one of four Seven Sons universities on the US Department of Commerce's Entity List for export control regulation.

C. Survey of Scientific Publications

Searches conducted on CNKI's website resulted in thirty-two publications having both NWPU and US-based coauthors. The majority of identified articles were in English, but the corpus includes several Chinese-language publications that merit further scrutiny.

Supplemental research on publications selected from the collected corpus of thirty-two articles reveals collaboration between US institutions and entities supporting PRC weapons development programs and the PAP.

Example 1: University of California–Irvine Collaboration with Researchers Associated with the PRC's Missile Programs, Presumably Classified Defense Projects

A 2013 Chinese-language article entitled "Numerical Computation and Analysis of Flow Over a Conical Forebody at High Angle-of-Attack,"

76. "学校简介 [School Overview]," 西北工业大学 [Northwestern Polytechnical University].
77. "学校简介 [School Overview]," 西北工业大学 [Northwestern Polytechnical University].

published in the PRC *Journal of Projectiles, Rockets, Missiles and Guidance*, names seven coauthors affiliated with the following institutions:[78]

1. National Defense Science and Technology Key Laboratory of Airfoil and Cascade Aerodynamics, NWPU
2. Beijing Research Institute of Near Space Aircraft Systems Engineering (北京临近空间飞行器系统工程研究所)
3. University of California–Irvine

Several coauthors and the two PRC institutions named in this article warrant closer scrutiny. The first institution listed, NWPU's National Defense Science and Technology Key Laboratory of Airfoil and Cascade Aerodynamics (西北工业大学翼型/叶栅空气动力学国防科技重点实验室), was established in 1992 by COSTIND and NWPU.[79] This laboratory is part of NWPU's School of Aeronautics and has two name variants. Some sources (on NWPU websites and scientific publications) remove the Chinese terms for "national defense science and technology" (国防科技) and replace it with "national" or "state" (国家), thereby referring to it in English as a "state key laboratory" instead.[80] In the collected corpus, there were two articles that used this variant, which *suggests a deliberate effort to obfuscate the laboratory's ties to the PRC's defense programs*.

78. 王中一 [Wang Zhongyi] et al., "圆锥前体大攻角绕流的数值计算与分析 [Numerical Computation and Analysis of Flow Over a Conical Forebody at High Angle-of-Attack]," 弹箭与制导学报 [*Journal of Projectiles, Rockets, Missiles and Guidance*] 33, no. 3 (2013): 123–125, http://doi.org/10.15892/j.cnki.djzdxb.2013.03.044.
79. "西北工业大学航空学院流体力学系（三系）简介 [Northwestern Polytechnical University School of Aeronautics Department of Fluid Mechanics (Three Departments) Overview]," 西北工业大学航空学院 [Northwestern Polytechnical University School of Aeronautics], January 6, 2017, https://hangkong.nwpu.edu.cn/info/1368/8220.htm.
80. For example, this NWPU page removes the words "national defense": https://hangkong.nwpu.edu.cn/info/1053/1309.htm.

One of the coauthors of this article is a professor at NWPU's School of Aeronautics, who has served since 2015 as the deputy director of the Academic Committee of the National Defense Science and Technology Key Laboratory of Airfoil and Cascade Aerodynamics. This NWPU scientist specializes in aerodynamics and fluid mechanics research and has worked extensively on defense projects, including what appear to be classified weapons programs.[81] His NWPU faculty webpage highlights a number of defense projects, including these:

- 863 Programs (national high-tech research programs supporting defense research)
- National defense major fundamental research (国防重大基础研究)
- PLA General Armaments Department Key Fund (总装重点基金) projects
- Five "major projects" with "XXX" designators in their titles (likely referring to classified programs) involving computational software systems integration, high speed wind tunnels, fluid dynamics, aerodynamics
- Winner of a 2014 National Defense Science and Technology Award related to a high speed airfoil and wind tunnel project (also with an "XXX" designator)[82]

Another PRC-based collaborator is affiliated with the Beijing Research Institute of Near Space Aircraft Systems Engineering. This institute falls under CALT, indicated in the illustration (Fig. 1) of the Academy's organizational structure.

CALT is a missile design and production academy under the state-owned defense conglomerate CASC.[83] According to the Nuclear Threat

81. "高超 [Gao Chao]," 西北工业大学 [Northwestern Polytechnical University], accessed June 14, 2020, http://teacher.nwpu.edu.cn/gaochao.html.
82. "高超 [Gao Chao]."
83. "China Academy of Launch Vehicle Technology (CALT)," Nuclear Threat Initiative, February 1, 1994, www.nti.org/learn/facilities/59/.

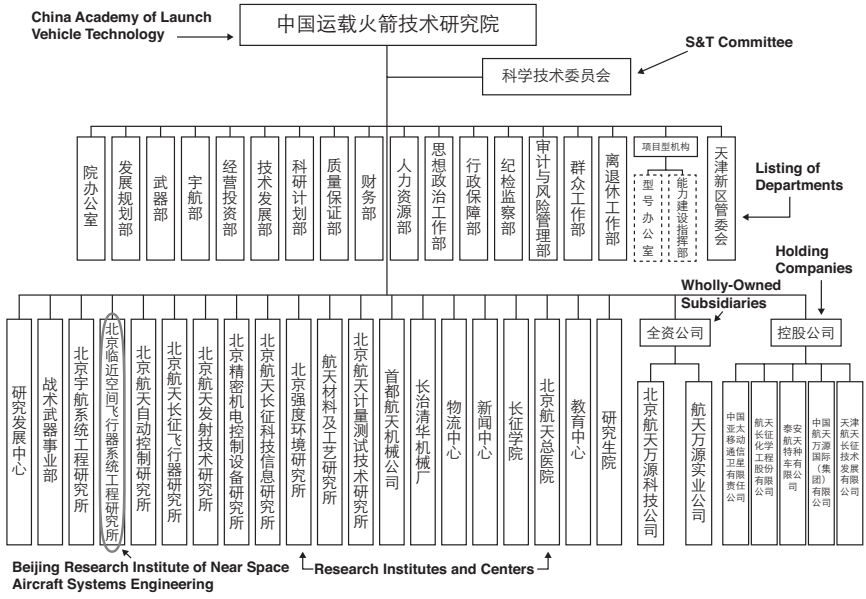


Figure 1. China Academy of Launch Vehicle Technology organizational structure (with added English annotations). *Source:* "组织机构, [Organizational Structure]" 中国运载火箭技术研究院 [China Academy of Launch Vehicle Technology], accessed June 14, 2020, http://www.calt.com/n481/n490/index.html.

Initiative, CALT is the PRC's "largest, most important organization for the research, development and production of space launch vehicles (SLVs), liquid-fueled surface-to-surface missiles, and solid-fueled surface-to-surface and submarine-launched ballistic missiles." The academy produces short-and medium-range ballistic missiles and intercontinental ballistic missiles.[84]

The participation of researchers from an NWPU defense laboratory and a component of the PRC's missile design academy raises serious questions about the potential weaponization of this research and concerns about the nature of the collaboration between these researchers and their coauthors at the University of California, Irvine.

84. "China Academy of Launch Vehicle Technology (CALT)."

Example 2: University of California–Merced Collaboration with NWPU and the PRC's People's Armed Police

Another Chinese-language article raises potential national security and ethical concerns.[85] This article, published in 2013, lists four authors affiliated with NWPU, Xi'an Engineering College of the People's Armed Police, Tianjin University, and the University of California–Merced.[86]

The primary author of this article serves as dean of NWPU's School of Applied Mathematics. After receiving undergraduate, master's and doctoral degrees from NWPU, this author served as a visiting researcher at Florida Atlantic University's Applied Research Center, paid for by the PRC government-run CSC. He/she also spent time as a postdoctoral researcher at the University of Colorado Boulder. Some of the author's research focuses on nonlinear random dynamics, broad cell mapping, path integral formulation, and finite difference and stochastic dynamics. Some of the author's professional associations include serving on an advisory committee of the Ministry of Education's Aerospace Professional Educators Association and the Chinese Society of Vibration Engineering.[87]

No biographical information was found on the other PRC-based coauthor affiliated with the Technical College of the Xi'an People's Armed Police (西安武警技术学院).[88] According to the school's website, its name was changed to the People's Armed Police Engineering University (武警工程大学) in 2011. In June 2017 (after the identified article was published), the university was reorganized and merged with the

85. 徐伟 [Xu Wei] et al., "胞映射方法的研究和进展 [Development and Study on Cell Mapping Methods]", 力学进展 [*Advances in Mechanics*] 1, (2013): 91–100, https://caod.oriprobe.com/articles/32319667/DEVELOPMENT_AND_STUDY_ON_CELL_MAPPING_METHODS.htm.

86. 徐伟 [Xu Wei] et al., "胞映射方法的研究和进展 [Development and Study on Cell Mapping Methods]."

87. "徐伟 [Xu Wei]," 西北工业大学 [Northwestern Polytechnical University], accessed June 14, 2020, http://jszy.nwpu.edu.cn/1978000010.html.

88. The English name is how it was rendered in the referenced article, but the Chinese name more closely resembles "Xi'an People's Armed Police Technology Institute."

former People's Armed Police Ürümqi Command College (武警乌鲁木齐指挥学院).[89]

The implications of this collaboration between UC Merced, NWPU and a PAP institution are serious. The PAP school merged with an Ürümqi-based PAP training unit, which is located in the capital of the PRC's Xinjiang region. The PAP in Xinjiang is deeply involved in what many in the international community consider to be the most oppressive surveillance regime in the world, including widespread extrajudicial detentions and forced mass internments of ethnic Uyghurs in reeducation camps.[90] Similar to Example 1, given that this publication appeared in a PRC source and only in Chinese, it is unknown whether UC Merced was aware of this research collaboration. Regardless, this article substantiates the need for heightened due diligence over academic collaboration with the PRC.

Example 3: Articles Involving Researchers at US Government Facilities

The collected corpus includes four English-language articles that name coauthors affiliated with US government institutions: the NIH, the DoE, and the NRL. Table 3 lists the publication source, title, authors, and affiliated institutions.

It is beyond the scope of this chapter to determine if the research in these articles has military applications or has violated US export controls. A more fundamental question is at stake: should the US government collaborate on S&T research of any kind with scholars from an

89. "武警工程大学简介 [Overview of the Engineering University of the People's Armed Police]," 武警工程大学 [Engineering University of the People's Armed Police], Internet Archive, archived November 5, 2019, accessed June 15, 2020, https://web.archive.org/web/20191105035753/http://www.wjgcdx.com/zhongxuejianjie/daxuejianjie/2018-06-07/47.html.

90. Maya Wan., "*Eradicating Ideological Viruses*": *China's Campaign of Repression Against Xinjiang's Muslims*, (New York: Human Rights Watch, 2018), https://www.hrw.org/report/2018/09/09/eradicating-ideological-viruses/chinas-campaign-repression-against-xinjiangs.

Table 3: NWPU Research Collaboration with US Government Institutions

Title	Source / Year	PRC Organization	US Organizations	Other Organizations
Knowledge-Guided Robust MRI Brain Extraction for Diverse Large-Scale Neuroimaging Studies on Humans and Nonhuman Primates	PLOS ONE (2014)	School of Automation, NWPU	Neuroimaging Research Branch, National Institute on Drug Abuse, NIH; Department of Radiology and Biomedical Research Imaging Center, University of North Carolina at Chapel Hill	Department of Brain and Cognitive Engineering, Korea University
Supported Tetrahedral Oxo-Sn Catalyst: Single Site, Two Modes of Catalysis	Journal of American Chemical Society (2016)	NWPU	Chemical Sciences Division, Argonne National Laboratory; Chemical Engineering Department, Purdue University	
A New High-Order Spectral Difference Method for Simulating Viscous Flows on Unstructured Grids with Mixed-Element Meshes	Computers and Fluids (2019)	School of Astronautics, NWPU	National Wind Technology Center, National Renewable Energy Laboratory; Department of Mechanical and Aerospace Engineering, George Washington University	
Main α Relaxation and Slow β Relaxation Processes in a La30 Ce30 Al15 Co25 Metallic Glass	Journal of Materials Science and Technology (2019)	School of Mechanics, Civil Engineering and Architecture, NWPU	Chemistry Division, NRL, Code 6120	Université de Lyon, France

institution that is on the Entity List, and more specifically who are from units of that institution known to participate in the defense programs of a strategic competitor? Perhaps NIH, DoE, and the Department of Defense did not know that these collaborations were taking place and would not have approved of them. Given that all four articles were published in English-language sources accessible online from US entities such as Elsevier and the NIH's website, the pertinent affiliation data was readily discoverable.

Table 4: Research Naming US Funding Support and NWPU Author Affiliation

Title	Organizations	Source	Funding
基于超像素的多模态 MRI 脑胶质瘤分割 (Segmentation of Glioblastoma Multiforme from Multimodal MR Images Based on Superpixel)	Houston Methodist Research Institute; School of Automation, NWPU	Journal of Northwestern Polytechnical University, 2014	NIH Grant 5G08LM893
无线视频通信跨层资源分配及性能优化 (Cross-Layer Resource Allocation and Performance Optimization for Wireless Video Communication)	Software Engineering Depart, Shenzhen Institute of Information Technology); Graduate School at Shenzhen, Tsinghua University; School of Computer Science and Engineering, University of Electronic Science and Technology of China; School of Electronics and Information, NWPU; Department of Electrical and Computer Engineering, University of Missouri	Journal of University of Electronic Science and Technology of China, 2013	NSF Grant DBI-0529082, DBI-0529012; 51st Round of Postdoctoral Fund of China 2012M510453

D. Secondary Search: US Research Funding

The second set of searches of CNKI bibliographic records examined articles that named a US institution as providing funding support and at least one author affiliated with NWPU. Only two records were found published in 2013 and 2014, both of which were in Chinese. Table 4 provides the bibliographic information on these articles.

Example 1: NWPU's Apparent Collaboration on NIH-Funded Projects

The first article in Table 4 credits the NIH as the sole funding source. It was published in Chinese in NWPU's own scholarly journal in 2014.[91] One of the NWPU-affiliated authors is a professor at NWPU's School

91. 苏坡 [Su Po] et al., "基于超像素的多模态 MRI 脑胶质瘤分割 [Segmentation of Glioblastoma Multiforme from Multimodal MR Images Based on Superpixels]," 西北工业大学学报 [*Journal of Northwestern Polytechnical University*] 32, no. 3 (2014): 417–22, http://doi.org/10.3969/j.issn.1000-2758.2014.03.017.

of Automation and has taught at NWPU since 1992. This professor's research areas include gas sensors and applications, integration testing techniques, noise and vibration measurement, and medical / biological imaging management. The scientist is also a member of the Chinese Society of Aeronautics and on the experimentation and testing expert committee of the Shaanxi Provincial Society of Aeronautics. He has received funding from the National Natural Science Foundation of China, aerospace science and technology funds, NWPU basic research funds, and other provincial and municipal sources.[92] No biographical information was found on the other NWPU-affiliated coauthor.

Here too, the NIH may not have been aware of all of the relevant facts. On its face, the research would appear benign, but in the absence of a robust vetting framework that is able to reliably detect and block funding of PRC-based projects with military or dual-use applications, prudence dictates barring collaborations with a PRC researcher who has defense-related expertise and furthermore works at a School of Automation that focuses on defense and aeronautical disciplines in a university that is on the Entity List.

Example 2: NSF Funding to NWPU Defense Researchers

The second article in Table 4 underscores how entangled many NWPU researchers are with defense research and funding streams tied to the PRC military. This article was published in the Chinese-language *Journal of the University of Electronic Science and Technology of China* in 2013 and credits two awards from the US NSF Division of Biological Infrastructure, as well as PRC postdoctoral research funds. One coauthor hailed from the University of Missouri.

Another coauthor is an associate professor at NWPU's School of Computer Science. At the time of this article's publication, this coauthor was completing his PhD studies at NWPU. NWPU's website states that he conducts research in areas such as vehicle networking

92. "西北工业大学自动化学院 [Northwestern Polytechnical University School of Automation]," 西北工业大学自动化学院 [Northwestern Polytechnical University School of Automation], accessed June 14, 2020, https://zdhxy.nwpu.edu.cn/info/1167/2565.htm.

design and optimization, driver behavioral analysis and safety support systems, and autonomous systems integration. Notably, of the eleven major research projects listed on his faculty webpage, four of them involved national defense and probably classified projects. Examples include the following:

- A National Defense Science and Technology Innovation Special Zone Plan project relating to uncrewed group systems
- A National Defense Basic Scientific Research project described as "XXX software integration support techniques"
- A 12th Five-Year Plan Preliminary Research Project entitled "XXX polymorhpic real-time computing platform"
- An 11th Five-Year Plan Preliminary Research Project described as "XXX distributed real-time calculation techniques"[93]

VI. Beijing Institute of Technology: Collaboration with US Research Institutions

A. Summary of Findings

The Beijing Institute of Technology (BIT, 北京理工大学) claims to have been the first institution of higher education in the PRC to specialize in defense industries and to have filed the most defense-related patents of any PRC higher education institution. Like its Seven Sons peers, BIT promotes military-civil fusion efforts.

- BIT's School of Mechatronical [*sic*] Engineering (机电学院) pursues weapons development such as warhead design, uncrewed aerial and underwater vehicles, and corresponding systems. Two identified articles named researchers from a laboratory on explosion and shock physics that is subordinate to this BIT school and the Georgia Institute of Technology (Georgia Tech).

93. "姚远 [Yao Yuan]," 西北工业大学 [Northwestern Polytechnical University], accessed June 14, 2020, http://teacher.nwpu.edu.cn/2017010188.html.

- Two BIT doctoral dissertations and one thesis credited US NSF as providing funding support. All three students also reported receiving PRC government funding via the CSC to study in the United States.

B. Overview of BIT and Support to the PRC's National Defense

BIT's origins trace to around 1940 in Yan'an as a research academy. In 1949, the school relocated to Beijing, and after experiencing a few name changes, it assumed its current name in 1988. BIT's official (Chinese-language) website boasts that it is the first PRC institution of higher education to specialize in national defense industries. BIT also claims that more than 120 of its graduates have served as provincial-level or higher government / Communist Party officials or PLA generals and that another was the chief designer of the PRC's first nuclear submarine.[94]

BIT claims to have developed hardware such as high-altitude solid rockets, low-altitude radars, the first light tank, advanced military use information systems, and other national defense technologies. BIT also claims to have filed the most national defense-related patents of any higher education institution in the PRC. Furthermore, BIT is involved in "military-civil fusion and innovation development" (军民融合与创新发展) efforts that are key to the PRC's current military modernization policies. In short, BIT has a stated mission to transfer civilian research areas to defense applications. It claims cooperative agreements with seventy-one countries or regions and student exchange agreements with more than fifty universities.[95]

C. Survey of Scientific Publications

Searches on CNKI's portal identified thirty-one articles that name at least one US institution and BIT. Supplemental research identified one additional article that likely supports PRC weapons development

94. "学校简介 [School Overview]," 北京理工大学 [Beijing Institute of Technology], June 2019, http://www.bit.edu.cn/gbxxgk/gbxqzl/xxjj/index.htm.

95. "学校简介 [School Overview]," 北京理工大学 [Beijing Institute of Technology].

programs. Examples of articles and their associated entities are profiled below.

Example 1: Georgia Tech Collaboration with BIT Weapons Laboratory

The most glaring example of research collaboration in support of PRC weapons programs are two articles by researchers affiliated with Georgia Tech's School of Materials Science and Engineering, and BIT's State Key Laboratory of Explosion Science and Technology (SKLEST). One article was published in May 2018, and the other (not found in CNKI) was published in July 2018, both by the same pair of PRC-based coauthors.[96]

One of the coauthors claimed affiliations with both BIT and Georgia Tech. This individual was a postdoctoral researcher at BIT around the time of the articles' publication.[97] He completed at least part of his graduate studies at Georgia Tech, which may explain the dual affiliation.[98]

The other PRC-based coauthor is the dean of BIT's School of Mechatronical Engineering and a professor at SKLEST. This author conducts research on material dynamics behavior, explosives working and composite materials, numerical simulation of explosions and shocks, energetic materials damage theory, and explosion safety technologies. He is also vice chair of the China Ordnance Society Explosion and Safety Technology Expert Committee and a member of the society's Youth Work Com-

---

96. Jianrui Feng et al., "Absence of 2.5 Power Law For Fractal Packing In Metallic Glasses," *Journal of Physics: Condensed Matter* 30, no. 25 (June 2018), https://doi.org/10.1088/1361-648X/aac45f; Jianrui Feng et al., "Existence of Fractal Packing in Metallic Glasses: Molecular Dynamics Simulations of $Cu_{46}Zr_{54}$," *Physical Review B* 98, no. 2 (July 2018): 024201, http://doi.org/10.1103/PhysRevB.98.024201.

97. "我校 18 名博士后研究人员获第 65 批中国博士后科学基金面上资助 [Eighteen of Our School's Postdoctoral Researchers Were Funded by the 65th Batch of China Postdoctoral Science Fellowships]," 北京理工大学 [Beijing Institute of Technology], May 8, 2019, http://renshichu.bit.edu.cn/xwtz/xw/147273.htm.

98. "毕业生 [Graduates]," 北京理工大学冲击波物理与化学实验室 [Shock Physics and Chemistry Lab at Beijing Institute of Technology], September 13, 2018, http://shock.bit.edu.cn/zncy/byxs/129358.htm.

mittee. The professor oversees a number of PRC government-funded research programs under the National Natural Science Foundation as well as ten National Defense Scientific Research Projects.[99]

The School of Mechatronical Engineering is extensively involved in weapons and defense research programs at BIT. For example, some of the subordinate divisions within the school include the Agile Weapons Research Institute (灵巧武器研究所), the Underwater Uncrewed Vehicles Systems Research Institute (水下无人系统研究所), the Intelligent Robotics Institute (智能机器人研究所), and the UAV Flight Engineering Department (无人飞航工程系). Additionally, the school houses three national defense science and technology innovation teams involving "target detection and damage control," "new concept warhead technologies," and "micro UAV systems."[100]

SKLEST is subordinate to BIT's School of Mechatronical Engineering.[101] According to its website, SKLEST "involves the disciplines of weapons science and technology, mechanics, safety science and engineering, materials science and engineering, chemical engineering and technology, and chemistry. . . . Research areas include theory and application of energetic materials, explosion mechanics, damage theory and application, protective theory and technology, and explosion safety theory and assessment methods."[102]

---

99. "陈鹏万 教授 [Professor Chen Pengwan]," 北京理工大学冲击波物理与化学实验室 [Shock Physics and Chemistry Lab at Beijing Institute of Technology], June 21, 2011, http://shock.bit.edu.cn/zncy/js/5731.htm.
100. "2017 年多物理场国际会议在北京理工大学成功举行 [The 2017 International Conference of Multiphysics Was Held at the Beijing Institute of Technology]," 北京理工大学冲击波物理与化学实验室 [Shock Physics and Chemistry Lab at Beijing Institute of Technology], December 21, 2017, http://shock.bit.edu.cn/xwdt/75518.htm.
101. "科研机构 [Institutional Structure]," 北京理工大学 [Beijing Institute of Technology], accessed June 14, 2020, http://smen.bit.edu.cn/kxyj/kygk/index.htm.
102. "Introduction," 爆炸科学与技术国家重点实验室 [State Key Laboratory of Explosion Science and Technology, Beijing Institute of Technology], January 4, 2017, http://est.bit.edu.cn/english/about/introduction/index.htm.

SKLEST claims to have hired five researchers through the Changjiang Scholars Program, two Thousand Talents Program "specially-appointed" professors, and three Thousand Talents Youth professors.[103] This means that at least ten SKLEST employees were recruited from overseas. It is not known if any came from the United States or if any of the coauthors identified here are PRC talent program selectees.

D. Secondary Search: US Research Funding of BIT Students

The second set of CNKI bibliographic searches examined articles that named a US institution as a funding source and at least one author affiliated with BIT. Three Chinese-language publications were identified, all of which were theses and dissertations published at BIT. These records appear in Table 5. Additional information on the authors appears below the table. All spent part of their graduate studies in the United States with funding from the PRC CSC and subsequently returned to BIT to complete their degrees. They also all cite support from the NSF in their theses.

The first author credits the PLA General Armament Department and the NSF for funding support in his master's thesis. He received bachelor's and PhD degrees in electronics engineering from BIT's School of Information and Electronics. According to the student's CV, he spent a year (2015–16) as a visiting researcher at the Department of Electrical and Computer Engineering at Temple University, funded by the CSC. His work on NSF-funded research may date to this time, and he may have ultimately applied that research towards fulfillment of his doctoral degree requirements. He also spent a year at the University of Edinburgh (UK), from 2017 to 2018. He is now an associate professor at the PRC's Southeast University School of Information Science and Engineering and conducts research in areas such as artificial intelligence, radar signal processing, and image reconstruction in electrical tomography.[104]

103. "实验室简介 [Overview of Laboratory]," 爆炸科学与技术国家重点实验室 (北京理工大学) [State Key Laboratory of Explosion Science and Technology (Beijing Institute of Technology)], May 6, 2016, http://est.bit.edu.cn/sysgk/sysjj/index.htm.

104. "Shengheng Liu [刘升恒]," accessed June 14, 2020, https://sites.google.com/site/shenghengliu/.

Table 5: Research Naming US Funding Support and BIT Author Affiliation

Title	Organization	Funding
稀疏分数傅里叶变换理论及其在探测中的应用 (Sparse Fractional Fourier Transformation and Its Applications in Exploration)	Beijing Institute of Technology (December 2016 master's thesis)*	National Natural Science Foundation of China; US NSF; PLA General Armament Dept. Preliminary Research Fund (国家自然科学; 美国国家自然科学基金; 总装预研基金)
新兴技术竞争情报挖掘方法研究 (The Competitive Technical Intelligence Methodology for Emerging Technology)	Beijing Institute of Technology (November 2015 PhD dissertation)†	National Software Science Fund; National Natural Science Foundation of China; US NSF (国家软科学; 国家自然基金; 美国国家自然科学基金)
新兴技术热点领域识别及技术路线图研究—以纳米导药系统为例 (Research on Hot Topic Identification and Technology—Roadmapping: A Case Study of Nano-Enabled Drug Delivery)	Beijing Institute of Technology (June 2015 PhD dissertation)‡	US NSF (美国自然科学基金)

* 刘升恒 [Liu Shengheng], "稀疏分数傅里叶变换理论及其在探测中的应用 [Sparse Fractional Fourier Transform and Its Applications in Exploration]" (PhD diss., Beijing Institute of Technology, 2016), http://new.oversea.cnki.net/KCMS/detail/detail.aspx?dbcode=CDFD&dbname=CDFDLAST2018&filename=1018811862.nh&v=Mjk4MThySVZGMjZGcnU1SDluS3JaRWJQSVI4ZVgxTHV4WVM3RGgxVDNxVHJXTTFGckNVUjdxZlllZHBGeTNrVkw=.

† 张嶷 [Zhang Yi], "新兴技术竞争情报挖掘方法研究 [The Competitive Technical Intelligence Methodology for Emerging Technology]" (PhD diss., Beijing Institute of Technology, 2016), http://new.oversea.cnki.net/KCMS/detail/detail.aspx?dbcode=CDFD&dbname=CDFDLAST2016&filename=1016710629.nh&v=MDg0MDI0Zk9wcEViUElSOGVYMUx1eFlTN0RoMVQzcVRyV00xRnJDVVI3cWZZZWRwRnlyaFViL0FWRjI2R0xTNUg=.

‡ 周潇 [Zhou Xiao], "新兴技术热点领域识别及技术路线图研究—以纳米导药系统为例 [Research on Hot Topic Identification and Technology Roadmapping: A Case Study of Nano-Enabled Drug Delivery]" (PhD diss., Beijing Institute of Technology, 2015), http://new.oversea.cnki.net/KCMS/detail/detail.aspx?dbcode=CDFD&dbname=CDFDLAST2016&filename=1016706825.nh&v=MDM2MTBuT3FwRWJQSVI4ZVgxTHV4WVM3RGgxVDNxVHJXTTFGckNVUjdxZlllZHBGeTNrVUx6TFZGMjZHTFM0R04=.

One of the 2015 doctoral dissertations was filed by a student at BIT's School of Management and Economics who spent a year (2011–12) at Georgia Tech through a "joint PhD training" program.[105] A brief biography in the dissertation states that the student's visit to Georgia Tech was funded by the CSC. The student participated in an NSF-funded

105. "张嶷 [Zhang Yi]," 北京理工大学管理与经济学院知识管理与数据分析实验室 [Knowledge Management and Data Analysis Laboratory, Beijing Institute of Technology School of Management and Economics], accessed June 14, 2020, http://www.aaaa.org.cn/team_desc.asp?id=24.

symposium entitled "Revealing Innovation Pathways: Hybrid Science Maps for Technology Assessment and Foresight" with Georgia Tech, which may be related to the NSF funding credited in the dissertation.[106]

The second dissertation was written by a PhD candidate who received a bachelor's and master's degree at BIT. In 2007, she spent a year at the Illinois Institute of Technology. In 2012–13, she spent a year at Georgia Tech, funded by the CSC.[107]

VII. Beihang University: Collaboration with US Research Institutions

A. Summary of Findings

Beihang University (北京航空航天大学, previously known as Beijing University of Aeronautics and Astronautics) has been involved in defense aerospace-related research since shortly after the university's founding in 1952. A significant subset of this research appears to focus on rocket engine design, missile design, and missile control systems. Beihang University appears to be heavily involved in defense research, as it claims to oversee 448 national defense research projects and 241 National 863 Program projects (which often involve military applications). This may be a key reason behind Beihang University's placement on the Department of Commerce's Entity List. The collected corpus reveals the following findings:

- One article with a coauthor from Beihang University also included a coauthor from the PLA's National University of Defense Technology (NUDT).
- Researchers affiliated with DoE laboratories—Argonne National Laboratory and Oak Ridge National Laboratory—coauthored

106. 张嶷 [Zhang Yi]."

107. 周潇 [Zhou Xiao], 北京理工大学管理与经济学院知识管理与数据分析实验室 [Knowledge Management and Data Analysis Laboratory, Beijing Institute of Technology School of Management and Economics], accessed June 14, 2020, http://www.aaaa.org.cn/team_desc.asp?id=146.

publications with Beihang University, raising concerns over the potential use of US federal government resources for this research.

- A researcher at Old Dominion University has collaborated on multiple research projects with Beihang University spanning at least six years, and one article was also coauthored by a researcher affiliated with an institute under the missile design and production facility CALT.
- One article involving researchers from US, Canadian, and PRC universities names coauthors from Beihang University and PRC telecommunications giant Huawei. The US government has placed Huawei on the Department of Commerce's Entity List. Huawei's participation in research collaborations that may have military significance between Beihang University and US institutions is therefore noteworthy.

B. Overview of Beihang University and Support to the PRC's National Defense

Beihang University was founded on October 25, 1952 as the Beijing Institute of Aeronautics, which originated from the merger of the aeronautical departments of a number of other universities, including Tsinghua University, Beiyang University, Xiamen University, and Sichuan University. In 1956, it instituted the PRC's first degree programs for guided missiles, missile design, liquid rocket engines, and aerodynamics. The university subsequently developed programs for radio equipment, aeronautical engineering, and instrument technology. By 1959, it created programs for aeronautical nonmetallic materials, corrosion and surface protection, radio navigation, radar, telemetry, and two laboratories on rocket engines and missile control systems.[108]

Additional research programs followed, including airplane design, winged missile design, aircraft high-altitude equipment design, aircraft engine design, solid rocket engine design, aviation gyro instruments,

108. "History," Beihang University, accessed June 14, 2020, https://ev.buaa.edu.cn/About/History.htm.

and inertial navigation.[109] Beihang University has also been involved in civilian aerospace fields (with dual-use potential); the main designers and chief engineers of the PRC's first manned space flight, the Shenzhou-5 Spacecraft, are Beihang alumni.

Beihang University highlights its successful recruitment of experts who have received training and/or work experience overseas. It hired twenty-seven selectees of the Recruitment Program of Global Experts "Innovative Talents" (a subcomponent of the PRC's flagship Thousand Talents Program), as well as fifty-eight selectees of the Thousand Talents youth component (also known as the Recruitment Program for Young Professionals). The university claims that it has recruited sixty-seven selectees of the Changjiang Scholars Award Program.[110] It has also joined with the elite Écoles Centrales network of graduate engineering schools in France to operate the Sino-French École Centrale de Pékin, which confers on its graduates both PRC and French degrees and integrates industrial training into the curriculum via Western corporate partners.

The website of the PRC's Ministry of National Defense (MND) offers other significant details on Beihang University's mission. MND confirms that the university was under the supervision of COSTIND, and the university was jointly sponsored by COSTIND, the Ministry of Education, the Beijing municipal government, and the Chinese Academy of Engineering. Additionally, Beihang University has two "national defense S&T innovation groups" and oversees 241 projects under the PRC's National High Technology 863 Program and 448 "national defense preliminary research projects" (国防预研项目).[111] Finally, it is a partner in the Collaborative Innovation Center of Astronautical Science and Technology, which also includes the China Aerospace Science

109. "History," Beihang University.

110. "Beihang at a Glance," Beihang University, October 2017, https://ev.buaa.edu.cn/About/Beihang_at_a_Glance.htm.

111. "国防生招生院校介绍: 北京航空航天大学 [Introduction to National Defense College Admissions: Beihang University]," Ministry of National Defense of the People's Republic of China, June 3, 2008, www.mod.gov.cn/service/2008-06/03/content_4085764.htm.

and Technology Corporation (CASC), Peking University, and the University of Science and Technology of China.

C. Survey of Scientific Publications

Searches on CNKI's portal identified twenty-eight articles that named coauthors from at least one US institution and Beihang University. Three of the articles merit closer scrutiny based on the affiliations of these coauthors.

- Two articles name coauthors from DoE: one article lists Argonne National Laboratory and the other names Oak Ridge National Laboratory.[112] The potential use of federal government resources or facilities to facilitate research collaborations with Beihang University is concerning in light of the university's presence on the Entity List. Further investigation is recommended to determine if: a) DoE facilities or resources were used to contribute to the published research results; b) whether leadership at the DoE laboratories were informed or consented to such collaboration; or c) whether Beihang University or a PRC government-funded program provided funding or compensation to the DoE-affiliated collaborators.
- Another article listed coauthors affiliated with the University of Illinois at Chicago, the University of Michigan, and the PRC's NUDT, in addition to Beihang University.[113] One of the coauthors claims a dual affiliation with Beihang and the University of Illinois, and another coauthor claims a dual affiliation with NUDT and the University of Michigan. NUDT is a university directly managed

112. Yang Li et al., "Theoretical Kinetics Analysis for Ḣ Atom Addition to 1,3-Butadiene and Related Reactions on the $\dot{C}_4H_7$ Potential Energy Surface," *Journal of Physical Chemistry A* 121, no. 40 (September 2017): 7433–7445, https://doi.org/10.1021/acs.jpca.7b05996; Xiaojun Yan et al., "The Effects Of DS Blade's Geometry Features on Material's Creep Strength," *Propulsion and Power Research* 3, no. 3 (September 2014): 143–150, https://doi.org/10.1016/j.jppr.2014.07.004.

113. Yang Yang et al., "A Robust Method for Inferring Network Structures," *Scientific Reports* 7 (2017), https://doi.org/10.1038/s41598-017-04725-2.

by the PLA. These dual affiliations invite scrutiny of the US institutions' involvement.

Supplemental research was conducted on individuals and institutions associated with two other articles in the collected corpus and are profiled below.

Example 1: Old Dominion University Collaboration with the PRC's Missile Programs

The article of greatest concern was published in 2014 in the journal *Computers and Fluids* and has demonstrable connections to the PRC's missile programs.[114] Coauthors listed affiliations with the following institutions:

1. School of Energy and Power Engineering, Beihang University
2. Department of Mathematics and Statistics, Old Dominion University (Virginia)
3. Beijing Institute of Space Launch Technology

While Beihang's participation is sufficient to warrant concern, the addition of the Beijing Institute of Space Launch Technology (北京航天发射技术研究所) raises the risk profile of this collaboration substantially. The Beijing Institute of Space Launch Technology is a division of CALT (a missile design and production group profiled in Section IV on NWPU). Figure 2 depicts this organizational relationship, with the Beijing Institute of Space Launch Technology circled.

Supplemental research found two other articles coauthored by two of the same scientists listed in this article who are affiliated with Old Dominion University and Beihang University.[115] One article was published in 2010 and the other published in 2016, suggesting a long-standing research partnership.[116]

---

114. Li Liu et al., "Nonuniform-Time-Step Explicit Runge–Kutta Scheme for High-Order Finite Difference Method," *Computers and Fluids* 105, (December 2014): 16678, https://doi.org/10.1016/j.compfluid.2014.09.008.
115. Note the additional articles did not appear in searches of CNKI's web portal.
116. 林大楷 [Lin Dakai] et al., "完全耦合层边界条件在圆柱绕流 DNS 中的应用 [Perfectly Matched Layer Boundary Conditions Using in DNS of Flow Around

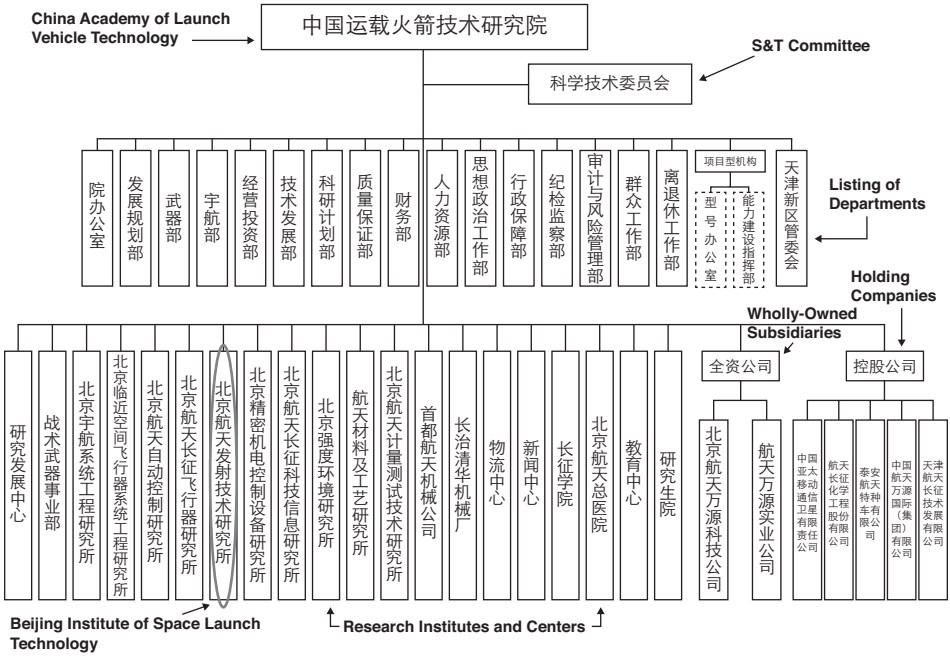


Figure 2. China Academy of Launch Vehicle Technology organizational structure (with added English annotations). *Source:* "组织机构, [Organizational Structure]" 中国运载火箭技术研究院 [China Academy of Launch Vehicle Technology].

Example 2: MIT Collaboration with Huawei Technologies

A 2016 article in the collected corpus named coauthors affiliated with the Massachusetts Institute of Technology (MIT), Beihang University, PRC telecommunications giant Huawei, and several other PRC and Canadian universities.[117] Huawei's involvement is noteworthy as the US government has since raised national security concerns over Huawei's

---

Cylinder]," 工程热物理学报 [*Journal of Engineering Thermophysics*], (May 2010): 757–760; 徐希海 [Xu Xihai] et al., "复杂几何条件下伴随格林函数的数值求解 [Numerical Solutions of Adjoint Green's Function for Complex Geometries]," 航空动力学报 [*Journal of Aerospace Power*], (April 2016): 927–933, http://doi.org/10.13224/j.cnki.jasp.2016.04.020.

117. Changqing Zou et al., "An Example-Based Approach to 3D Man-Made Object Reconstruction from Line Drawings," *Pattern Recognition* 60, (December 2016): 543–553, https://doi.org/10.1016/j.patcog.2016.05.031.

potential global dominance in 5G technologies and suspected ties to the PRC government and PLA. The US Department of Justice has also issued multiple indictments alleging intellectual property theft, obstruction of justice, and fraud related to evasion of US sanctions against Iran.[118] In May 2019, the US Department of Commerce placed Huawei and its affiliates on the Entity List.[119]

The coauthors of this article published in the journal *Pattern Recognition* are affiliated with the following institutions:

1. Hengyang Normal University (PRC)
2. Simon Fraser University (Canada)
3. Massachusetts Institute of Technology
4. Shandong University (PRC)
5. School of Automation Science and Electrical Engineering, Beihang University (PRC)
6. Huawei Technology Co. Ltd. (PRC)

Elsevier's ScienceDirect also posted information on this article and included biographies of the coauthors.[120]

- Two of the coauthors studied at HIT and worked in remote sensing, image processing, and other computer science fields. One of

118. US Department of Justice, Office of Public Affairs, "Chinese Telecommunications Device Manufacturer and its U.S. Affiliate Indicted for Theft of Trade Secrets, Wire Fraud, and Obstruction Of Justice," January 28, 2019, https://www.justice.gov/opa/pr/chinese-telecommunications-device-manufacturer-and-its-us-affiliate-indicted-theft-trade; Sean Keane, "Huawei Ban Timeline: NATO Head Supports UK Review of Chinese Firm's Role in 5G Rollout," CNET, June 10, 2020, https://www.cnet.com/news/huawei-ban-full-timeline-on-how-and-why-its-phones-are-under-fire/.
119. Bureau of Industry and Security, Commerce, "Addition of Entities to the Entity List," *Federal Register* 84, no. 98 (May 21, 2019): 22961, https://www.federalregister.gov/documents/2019/05/21/2019-10616/addition-of-entities-to-the-entity-list.
120. Zou et al., "An Example-Based Approach to 3D Man-Made Object Reconstruction from Line Drawings."

the HIT graduates held a research position at Griffith University in Australia and was subsequently recruited through a PRC Ministry of Education-sponsored recruitment program known as the New Century Excellent Talents to work at Beihang University.
- The Huawei-affiliated author claims to be a chief scientist specializing in computer vision, machine learning, image processing, and related artificial intelligence (AI) disciplines and previously worked at the Chinese Academy of Sciences Shenzhen Institutes of Advanced Technology.[121]

The apparent research collaboration with Huawei and Beihang University raises questions as to whether Huawei was developing military applications for this research or commercializing it for civilian purposes.[122]

VIII. Harbin Engineering University: Collaboration with US Research Institutions

A. Summary of Findings

The Harbin Engineering University (哈尔滨工程大学, HEU) has been an integral part of the PLA since its origins and has a strong focus on the development of PLA Navy technologies and equipment manufacturing such as naval nuclear power, underwater robotics, noise reduction, ship stabilization, marine propulsion, integrated navigation, hydrolocation, subsurface detection, (ocean) surface drones, and nuclear power simulation.

- HEU's College of Nuclear Science and Technology conducts defense research and, according to the collected corpus of articles,

121. Zou et al., "An Example-Based Approach to 3D Man-Made Object Reconstruction from Line Drawings."
122. In April 2019, MIT announced that it will no longer accept new or renew existing partnerships with Huawei and that collaborative projects will be subject to additional review (http://orgchart.mit.edu/node/27/letters_to_community/new-review-process-elevated-risk-international-proposals).

partners with US institutions, including DoE laboratories and the University of Michigan. The English-language articles in the collected corpus obfuscate the associations of their coauthors with defense programs by referring to their institutional affiliations with innocuous sounding translations.

- One of the HEU-affiliated coauthors is involved in national organizations that promote military-civil fusion efforts on behalf of the PRC government and CCP.

B. Overview of HEU and Support to the PRC's National Defense

The Harbin Engineering University's roots began with the founding of the PLA Military Engineering Institute (中国人民解放军军事工程学院) in 1953. In 1960–62, several departments were relocated to form the basis of other defense-related universities such as the (now named) Nanjing University of Science and Technology (another Seven Sons university) and the PLA's Institute of Chemical Defense. In 1966, the university changed its name to the Harbin Engineering Institute. In 1970, a Naval Engineering department was created and the university became known as the Harbin Shipbuilding Engineering Institute. Administration of the university then came under several machinery ministries and subsequently the China State Shipbuilding Corporation.[123] Other departments, such as Electronic Engineering, Missile Engineering, and Computer Engineering were transferred to what is now NUDT.[124]

In 1994, the university was renamed the Harbin Engineering University and administered by COSTIND. In 2007, the university was jointly (re)established by COSTIND, the Ministry of Education, the Heilongjiang provincial government, and the PLA Navy. HEU has played a key role in the PRC's military modernization, with a focus on naval technologies. HEU has seven MIIT-run national laboratories, two national defense key laboratories, ten "national defense special disciplines," and

123. "学校简介 [School Overview]," 哈尔滨工程大学 [Harbin Engineering University], September 2019, http://www.heu.cn/xygk/xxjj.aspx.

124. "Our History," Harbin Engineering University, accessed June 14, 2020, https://english.hrbeu.edu.cn/5666/list.htm.

seven "national defense urgently needed and key majors," and serves as a military reserve officer training school.[125]

- HEU claims to have developed the PRC's first experimental submarine, the first hydrofoil, the first ship-based computer, the first depth finder instrument, and other military equipment technologies.
- HEU serves as an "important talent cultivation and research base" for "3 marine and 1 nuclear fields" (三海一核)—referring to ship engineering, naval equipment, ocean exploration, and nuclear power applications.
- HEU conducts research on naval nuclear power, underwater robotics, noise reduction, ship stabilization, marine propulsion, integrated navigation, hydro-location, subsurface detection, (ocean) surface drones, and nuclear power simulation fields.
- HEU boasts that it is a "key organization for advanced technologies in PLA Navy equipment development and manufacturing" (海军先进技术装备研制的重点单位) and that it has received national recognition for high-technology weapons equipment development and engineering and aircraft carrier construction.[126]

HEU is also involved in international collaboration and talent recruitment. It boasts thirteen Thousand Talents Program selectees, four Changjiang Scholars Award Program professors, seven National Hundred, Thousand, Ten-Thousand Talent Project selectees (国家百千万人才工程), and six "national defense science and technology innovation teams." These programs typically hire experts from abroad to lead or guide research programs. Lastly, HEU claims to have established "stable, cooperative relationships" with more than twenty-two countries and one hundred organizations including the University of California–Berkeley, the University of Michigan, the University of Southampton (UK), the

125. "学校简介 [School Overview]," 哈尔滨工程大学 [Harbin Engineering University].

126. "学校简介 [School Overview]," 哈尔滨工程大学 [Harbin Engineering University].

University of Sydney (Australia), and the Bauman Moscow State Technical University.[127] In June 2020, HEU was added to the US Department of Commerce's Entity List for export control purposes, but this may not limit collaboration with US institutions if the research is categorized as fundamental in nature.[128]

C. Survey of Scientific Publications

Searches in CNKI's web portal produced no Chinese-language publications affiliated with HEU and a US institution. The fifteen English articles identified originate from Elsevier, according to the CNKI records.

There are two articles with HEU-affiliated authors that also name researchers from the US DoE as well as the University of Michigan. One of these articles appears to involve US research on ocean-related energy development.[129] Assuming there are no intended military applications behind this research, the article nonetheless raises the recurring question of whether the DoE should fund research with potential commercial applications at institutions that are closely integrated into the defense establishment of a strategic competitor.

Example 1: Argonne National Laboratory, University of Michigan Collaboration with HEU

Supplemental research was conducted on an article that named DoE's Argonne National Laboratory as one of the partnering institutions.

---

127. "学校简介 [School Overview]," 哈尔滨工程大学 [Harbin Engineering University].
128. Bureau of Industry and Security, Commerce, "Addition of Entities to the Entity List, Revision of Entries on the Entity List," *Federal Register* 85, no. 109 (June 5, 2020): 34495, https://www.govinfo.gov/content/pkg/FR-2020-06-05/pdf/2020-10869.pdf.
129. Hai Sun et al., "Flow-Induced Vibration of Tandem Circular Cylinders with Selective Roughness: Effect of Spacing, Damping and Stiffness," *European Journal of Mechanics / B Fluids* 74, (March-April 2019): 219–241, https://doi.org/10.1016/j.euromechflu.2018.10.024.

That article was published in the June 2018 issue of *Annals of Nuclear Energy*,[130] and despite the apparent civilian orientation of the research, the collaboration with an HEU-affiliated researcher merits scrutiny. Specifically, that researcher claimed to be affiliated with both the Department of Nuclear Engineering and Radiological Sciences at the University of Michigan and the "Fundamental Science on Nuclear Safety and Simulation Technology Laboratory" at HEU.[131] He served as a visiting professor at the University of Michigan[132] and is currently an assistant professor and master's student advisor in HEU's College of Nuclear Science and Technology (CNST). Notably, the HEU faculty webpage shows his position title but leaves blank all other sections on work and education experience.[133]

Background on HEU College of Nuclear Science and Technology

The researcher's affiliation with CNST raises questions. According to its English-language webpage, CNST was founded in 2005 and has been involved in "comprehensive research and development of nuclear power plants." CNST developed "new research directions - reprocessing of nuclear fuel, radiation damage and materials, and decommissioning of nuclear facilities" and signed "comprehensive cooperation agreements" with more than twenty institutions, including the University Michigan, Texas A&M University, Kyoto University, Lancaster University (UK), the International Atomic Energy Agency, and domestically with China Institute of Atomic Energy, China National Nuclear Corporation, and

130. Chen Hao et al., "Multi-Level Coarse Mesh Finite Difference Acceleration with Local Two-Node Nodal Expansion Method," *Annals of Nuclear Energy* 116, (June 2018): 105–113, https://doi.org/10.1016/j.anucene.2018.02.002.

131. Hao et al., "Multi-Level Coarse Mesh Finite Difference Acceleration with Local Two-Node Nodal Expansion Method."

132. Nuclear Engineering and Radiological Sciences, *Annual Report: September 1, 2016–August 31, 2017*, (Ann Arbor, MI: University of Michigan, 2017), https://ners.engin.umich.edu/wp-content/uploads/sites/7/2018/07/ners-ar2017.pdf.

133. "郝琛 [Hao Chen]," 哈尔滨工程大学 [Harbin Engineering University], accessed June 14, 2020, http://homepage.hrbeu.edu.cn/web/haochen.

China General Nuclear Power Group.[134] The HEU-affiliated researcher's visiting professorship at the University of Michigan and the dual affiliation claimed in the article may have been connected to one of these "cooperation agreements."

However, CNST's Chinese-language website lists five subdivisions that do not appear on the English-language website, including a national defense key laboratory and a SASTIND-sponsored innovation center. (Table 6)

The researcher in question lists his HEU affiliation as the "Fundamental Science on Nuclear Safety and Simulation Technology Laboratory." This is almost certainly a minor variant of the "Nuclear Safety and Simulation Key Discipline Laboratory" named on HEU's English-language webpage. However, the official (Chinese) name only lists one "key laboratory" associated with nuclear safety and simulation: the SASTIND Nuclear Safety and Simulation Technology National Defense Key Laboratory. The article is presumably referring to this defense laboratory and reproduces HEU's obfuscation of its connections to PRC national defense-associated entities in English-language sources.

The same HEU researcher is also involved in advancing the PRC government's military-civil fusion policies. In 2018, he was named a designee of a newly formed presidium of the Youth Alliance of the China Association of Science and Technology's Military-Civil Fusion Alliance.[135] The announcement of his selection appeared in a news story entitled "China Association of Science and Technology Military-Civil

134. "Nuclear Science and Technology College Introduction," Harbin Engineering University, accessed June 14, 2020, https://english.hrbeu.edu.cn/2017/1102/c5855a169731/page.htm.

135. "中国科协军民融合学会联合体青年人才托举论坛在江门召开 [China Association of Science and Technology Military-Civil Fusion Alliance Young Talents Forum Convenes in Jiangmen]," 中国航空学会 [China Society of Aeronautics and Astronautics], November 23, 2018, http://www.csaa.org.cn/a/tmp/zuzhigongzuo/2018/1123/2371.html.

Table 6: HEU College of Nuclear Science and Technology Subdivisions

Subdivisions Listed on English Webpage*	Subdivisions Listed on Chinese Webpage† (English translation added)
National Scientific Innovation Team	核动力安全与仿真创新引智基地 (Nuclear Power Safety and Simulation Innovative Talents Introduction Base)
Ministry of Education-State Administration of Foreign Expert Affairs (SAFEA) Nuclear Power Safety and Simulation Innovation Base	教育部核科学与技术虚拟仿真实验教学中心 (Ministry of Education Nuclear Science and Technology Virtual Simulation Experimental Teaching Center)
Nuclear Safety and Simulation Key Discipline Laboratory	科技部核安全与仿真技术国际联合研究中心 (Ministry of Science and Technology Nuclear Safety and Simulation Technology International Joint Research Center)
Heilongjiang Provincial Key Laboratory of Radiation Technology	工信部核动力安全与仿真技术协同创新中心 (MIIT Nuclear Power Safety and Simulation Technology Collaboration Innovation Center)
	国防科工局核安全与仿真技术国防重点学科实验室 (SASTIND Nuclear Safety and Simulation Technology National Defense Key Laboratory)
	国防科工局"核动力技术国防科技工业创新中心 (SASTIND Nuclear Power Technology National Defense Science and Technology Industry Innovation Center)
	黑龙江省核科学与技术实验教学示范中心 (Heilongjiang Provincial Nuclear Science and Technology Experimental Teaching Demonstration Center)
	黑龙江省辐射技术高校实验室 (Heilongjiang Provincial Radiation Technology Higher Education Laboratory)
	黑龙江省核动力装置性能与设备重点实验室 (Heilongjiang Provincial Nuclear Power Equipment and Facilities Key Laboratory)

* "Nuclear Science and Technology College Introduction," Harbin Engineering University, accessed June 14, 2020, https://english.hrbeu.edu.cn/2017/1102/c5855a169731/page.htm.

† "学院简介 [School Overview]," 哈尔滨工程大学核科学与技术学院 [Harbin Engineering University College of Nuclear Science and Technology], accessed June 14, 2020, http://cnst.hrbeu.edu.cn/1928/list.htm.

Fusion Alliance Young Talents Forum Convenes in Jiangmen."[136] The news article described the new members of this body as contributors to "promoting military-civil fusion S&T development and lifting up the future of [the PRC's] national defense."[137]

136. The original Chinese title is "中国科协军民融合学会联合体青年人才托举论坛在江门召开."

137. See note 136.

The China Association of Science and Technology (CAST) claims to be the largest "nongovernmental organization" of S&T professionals in the PRC. Despite this claim, CAST also states that it serves as a "bridge that links the Communist Party of China and the PRC government to the country's S&T community." CAST is a subordinate organ of the Chinese People's Political Consultative Conference, an apex organ of the United Front that institutionalizes the CCP's cooptation of nonparty elites from all walks of life.[138]

The CAST Military-Civil Fusion Alliance consists of eleven PRC professional societies (which are all also under CAST). They are listed below.

- China Ordnance Society (中国兵工学会)
- Chinese Society of Aeronautics and Astronautics (中国航空学会)
- Chinese Society of Naval Architects and Marine Engineers (中国造船工程学会)
- Chinese Nuclear Society (中国核学会)
- Chinese Society of Astronautics (中国宇航学会)
- Chinese Institute of Electronics (中国电子学会)
- China Instrument and Control Society (中国仪器仪表学会)
- Chinese Society for Composite Materials (中国复合材料学会)
- China Institute of Navigation (中国航海学会)
- China Textile Engineering Society (中国纺织工程学会)
- Chinese Society for Optical Engineering (中国光学工程学会)[139]

138. "Profile," China Association for Science and Technology, accessed June 14, 2020, http://english.cast.org.cn/col/col471/index.html.

139. "中国科协军民融合学会联合体 [China Association of Science and Technology Military-Civil Fusion Alliance]," 中国科协军民融合学会 [China Association for Science and Technology], May 6, 2019, http://www.cast.org.cn/art/2019/5/6/art_558_39761.html.

IX. Nanjing University of Aeronautics and Astronautics: Collaboration with US Research Institutions

A. Summary of Findings

The Nanjing University of Aeronautics and Astronautics (南京航空航天大学, NUAA) was founded in 1952 and focuses primarily on aerospace engineering disciplines. NUAA was placed under the authority of COSTIND in 2004 and is heavily involved in defense aerospace programs and in the development of UAVs. The university oversees ten "national defense special disciplines" and numerous national defense fundamental research projects and has won multiple national defense invention and progress awards.

- Two subdivisions named in the collected corpus of articles directly support defense research and weapons programs. The College of Aerospace Engineering houses a national defense key laboratory and oversees projects under the (formerly named) PLA General Armament Department. The College of Automation Engineering manages "weapons science and technology" research disciplines and claims to have graduated more than 1,100 students that are part of the "national defense system."
- One of the publications involving hypersonic flight vehicle engineering research named a grant that describes an apparent collaborative relationship between NUAA and the PRC's missile design and production entity CALT. A listed coauthor of the article oversees this joint hypersonics project.
- A doctoral dissertation published at NUAA credited the US NSF for research support, which may have been conducted during the author's study abroad at Stanford University's Department of Aeronautics and Astronautics.

B. Overview of NUAA and Support to the PRC's National Defense

NUAA was founded in 1952 and has focused on aerospace engineering throughout its history. In 2004, COSTIND took over oversight of the

university. NUAA's English-language webpage notes that the university "will deeply implement the national innovation-driven development strategy and the military-civilian integration development strategy . . . in aeronautics, astronautics and aviation."[140]

Chinese-language descriptions on NUAA's website note that the university has a National Defense Science and Technology Industry Technology Research Applications Center (国防科技工业技术研究应用中心) and manages ten "national defense special disciplines." NUAA claims that "in national defense fields, NUAA has participated in advanced research, addressed key technology problems, and conducted experimental research on nearly every major aerospace model." Some of NUAA's noted achievements are production of the PRC's first large uncrewed target drone, the first uncrewed nuclear materials testing drone, the first uncrewed helicopter, the first uncrewed micro aircraft, and the successful launch of an independently developed microsatellite. NUAA also claims to have provided input into many of the technologies behind the PRC's Chang'e 3 robotic lunar surface exploration mission and related aerospace engineering projects.[141]

The Chinese-language website of NUAA's College of Aerospace Engineering states that the college is involved in military-related aircraft research and has a Study Discipline and Scientific Research Secrecy Protection Office, suggesting that some of the research may involve classified programs. Additionally, the college houses the National Defense Key Laboratory of Precision Drive Technology (精密驱动技术国防重点学科实验室), which is subordinate to NUAA's Ultrasonic Motor Research Center. This defense key laboratory was established in 2007 under COSTIND authorities. Interestingly, the Ultrasonic Motor Research Center was endorsed and established as a Ministry of Education and State Administration of Foreign Expert Affairs (SAFEA) Higher

140. "NUAA's History," Nanjing University of Aeronautics and Astronautics, accessed June 14, 2020, http://iao.nuaa.edu.cn/nuaas-history/.

141. "南航简介 [Overview of NUAA]," 南京航空航天大学 [Nanjing University of Aeronautics and Astronautics], accessed June 14, 2020, http://www.nuaa.edu.cn/479/list.htm.

Education Innovative Talent Introduction Base (高等院校学科创新引智基地). SAFEA is a PRC central government organ in charge of recruiting experts worldwide to facilitate transfers of technology and intellectual capital.[142] The center is involved in seventeen national defense fundamental research projects and "[the former] PLA General Armament Department key projects."[143]

NUAA's College of Automation Engineering is also involved in defense research and engineering programs, despite no indication of this on its English-language webpage. The Chinese-language website notes that the college has two "national defense special majors" and that it has been recognized for outstanding contributions to national defense projects, including: one project winning second prize and another winning third prize in the "National Defense Technology Invention Award"; three projects winning second prize and one project winning third prize in the "National Defense Science and Technology Progress Award"; one individual recognized among the "national defense science and technology industry 100 outstanding doctorates"; and three individuals recognized as a "COSTIND outstanding PhD graduate." Additionally, the College of Automation Engineering claims to have graduated more than 1,100 students who are part of the "national defense system." The college is engaged in weapons science and technology research, and its website provides documents on "required materials for NUAA classified scientific research project management work processes" (南京航空航天大学涉密科研项目管理各业务流程所需材料).[144]

142. SAFEA (国家外专局) was an organ directly under the PRC State Council but was later absorbed as a subordinate division of the Ministry of Science & Technology.

143. "精密驱动技术国防重点学科实验室," Nanjing University of Aeronautics and Astronautics College of Aerospace Engineering, accessed June 14, 2020, http://aero.nuaa.edu.cn/2017/0224/c9603a78292/page.htm.

144. "南京航空航天大学涉密科研项目管理各业务流程所需材料," 南京航空航天大学自动化学院 [Nanjing University of Aeronautics and Astronautics School of Automation], accessed June 15, 2020, http://cae.nuaa.edu.cn/5410/list.htm.

C. Survey of Scientific Publication Records

Searches in CNKI resulted in only five identified science and engineering articles that had coauthors from US institutions and NUAA, the smallest set of results among the Seven Sons universities. A secondary search of US funding sources named on NUAA-authored publications resulted in one doctoral dissertation that credits the US NSF for support. All six publications were in the Chinese language, a unique finding among the universities profiled in this chapter. The reasons for such a low number of articles and the absence of any English-language publications among them are unknown. Two of the articles that named authors affiliated with NUAA's colleges of Aerospace Engineering and Automation Engineering are profiled below and document the coauthors' connections to PRC defense programs.

Example 1: NUAA College of Aerospace Engineering Collaboration with University of Texas at Arlington

A 2016 publication entitled "Motion Around Vortices and Λ Vortex Rings in Boundary Layer Transition" named two authors affiliated with NUAA's College of Aerospace Engineering and one from the University of Texas at Arlington.[145] No biographical information was found on the primary coauthor affiliated with NUAA.[146] The second NUAA-affiliated coauthor is a professor and doctoral advisor who conducts research in computational fluid dynamics. His CV on NUAA's website mentions his past and current affiliations but lacks details on current research areas. The CV states that he was a second prize winner of the 2006 National Defense Science and Technology Award and currently

145. 王义乾 [Wang Yiqian] et al., "平板湍流转捩过程中Λ涡和环状涡的周围流场研究 [Motion Around Vortices and Λ Vortex Rings in Boundary Layer Transition]," 航空计算技术 [*Aeronautical Computing Technology*] 46, no. 2 (2016): 15–18, https://kns.cnki.net/kcms/detail/detail.aspx?filename=HKJJ201602004&dbcode=CJFQ&dbname=CJFD2016&v=.

146. It is possible this individual was a graduate student at the time of publication, which may explain the lack of additional biographical information.

oversees "national defense fundamental research projects."[147] Baidu Baike hosts a more complete biography of the professor and lists "national defense preliminary research projects" he has worked on at NUAA. Examples include numerical simulation methods involving fluid dynamics, helicopter rotor aerodynamics, and aircraft complex form factor high precision aerodynamics.[148]

Example 2: NUAA College of Automation Engineering Collaboration with University of Virginia on Near Space Hypersonic Vehicle Research

An article of obvious national security concern within the corpus of NUAA articles is a 2018 publication discussing hypersonic vehicles, which the PLA seeks to develop to counter US military dominance. The article entitled "Research Progress of Adaptive Control for Hypersonic Vehicle in Near Space" named three authors affiliated with NUAA and one author affiliated with the University of Virginia.[149] Supplemental information obtained on two of the coauthors confirm their extensive work on PRC defense projects and weapons systems.[150] Additionally, the article names a research funding source associated with an apparent collaborative effort between NUAA and the missile production and design entity CALT.

The College of Automation Engineering website lists several "weapons science and technology" (兵器科学与技术) disciplines and faculty assigned to those disciplines. Two of the article's coauthors are assigned

147. "赵宁 [Zhao Ning]," 教师个人主页 [Faculty Pages], 南京航空航天大学 [Nanjing University of Aeronautics and Astronautics], accessed June 15, 2020, http://faculty.nuaa.edu.cn/zn1/zh_CN/index.htm.

148. "赵宁 [Zhao Ning]," 百度百科 [Baidu Baike], accessed June 15, 2020, https://baike.baidu.com/item/%E8%B5%B5%E5%AE%81/17017884.

149. 甄子洋 [Zhen Ziyang] et al., "基于自适应控制的近空间高超声速飞行器研究进展 [Research Progress of Adaptive Control for Hypersonic Vehicle in Near Space]", 宇航学报 [*Journal of Astronautics*] 39, no. 4 (April 2018): 355–367, http://doi.org/10.3873/j.issn.1000-1328.2018.04.001.

150. The third NUAA-affiliated coauthor appears to be a graduate student based on an announcement of candidates accepted into an NUAA master's degree program (http://cae.nuaa.edu.cn/2016/0919/c5375a92404/page.htm).

to the "weapon systems and applications engineering disciplines" within the college. Other weapons science disciplines within the same department include weapons firing theory / techniques, and artillery, automatic weapons, and ammunition engineering.[151]

The College of Automation Engineering hosts CVs for both coauthors on its faculty webpages. The first is a professor and vice dean of the college's graduate school, where he conducts research on carrier-based aircraft, large passenger aircraft, hypersonic flight vehicles, drones/UAVs, and aircraft guidance and control. This researcher has overseen 863 Program topics and PLA Air Force Equipment Development Department preliminary research projects.[152]

The second coauthor is also a professor and vice dean of the College of Automation Engineering and conducts research on carrier-based aircraft and UAV take-off (from ships) guidance and control, drone swarm formation coordination, control and strategic decision making, hypersonic flight vehicles, fighter aircraft, large passenger aircraft, guided missiles, and related advanced flight controls. From February 2015 to February 2016, he was a visiting scholar at the University of Virginia's Department of Electronic and Computer Engineering, where a third coauthor had an affiliation.

Furthermore, the second coauthor's CV notes coauthorship of numerous Chinese- and English-language publications, many of which relate to drones/UAVs and aircraft carrier-related technologies. Some examples include the following:

151. "兵器科学与技术 [Weapons Science and Technology]," 南京航空航天大学自动化学院 [Nanjing University of Aeronautics and Astronautics School of Automation], Internet Archive, archived September 7, 2019, accessed June 15, 2020, https://web.archive.org/web/20190907133433/http://caegl.nuaa.edu.cn/list/471.

152. "江驹 [Jiang Ju]," 南京航空航天大学自动化学院 [Nanjing University of Aeronautics and Astronautics School of Automation], Internet Archive, archived September 13, 2019, accessed June 15, 2020, https://web.archive.org/web/20190913213002/http://caegl.nuaa.edu.cn/showSz/471-1073.

- "Self-Organization Method for Multiple Reconnaissance - Attack UAVs under Adversarial Environment," *Aerospace Science and Technology*, 2016.
- "Observer-based backstepping longitudinal control for carrier-based UAV with actuator faults," *Journal of Systems Engineering and Electronics*, 2017.
- "Multivariable Adaptive Distributed Leader-Follower Flight Control for Multiple UAVs Formation," *The Aeronautical Journal*, 2017.
- "Take-off and Landing Control for a Coaxial Ducted Fan Uncrewed Helicopter," *Aircraft Engineering and Aerospace Technology*, 2017.
- "Modeling, Control Design and Influence Analysis of Catapult-Assisted Take-Off Process for Carrier-Based Aircrafts," *PIME Part G: Journal of Aerospace Engineering*, 2018.
- "Cooperative Search-Attack Mission Planning for Multi-UAV Based on Intelligent Self-Organized Algorithm," *Aerospace Science and Technology*, 2018.

Additionally, this coauthor claims to have won several defense-related awards, including four separate "National Defense Science and Technology Progress Awards" in 2010, 2011, 2012, and 2017. These awards related to aircraft guidance and control techniques, load simulators, aircraft carrier technologies, and ship-based drone technologies. Lastly, this coauthor has managed research projects involving near space flight vehicle control techniques and what appears to have been the "CASC First Academy Higher Education Joint Innovation Fund" (航天一院高校联合创新基金) grant that funded the collected article on hypersonic flight vehicle controls at issue here.[153]

The bibliographic record belonging to that article lists the "First Academy Higher Education Joint Innovation Fund (CALT201603)" as a

153. "甄子洋 [Zhen Ziyang]," 南京航空航天大学自动化学院 [Nanjing University of Aeronautics and Astronautics School of Automation], Internet Archive, archived September 14, 2019, accessed June 15, 2020, https://web.archive.org/web/20190914053954/http://caegl.nuaa.edu.cn/showSz/471-1060.

funding source.[154] The "CALT" prefix in the funding code refers to the China Academy of Launch Vehicle Technology, profiled above. CALT is also known as the CASC First Academy (中国航天科技集团有限公司第一研究院, or "航天一院" for short).[155] In short, the extensive defense research undertaken by both NUAA coauthors, coupled with their apparent partnership with CALT, suggests that the research in the identified article may be intended for military-use hypersonic vehicles.

D. Secondary Search: Claimed US Funding Support to NUAA Dissertation

A second set of searches of CNKI bibliographic records identified one doctoral dissertation published in 2016 at NUAA that credits the US NSF for funding support. According to an announcement on NUAA's website, the author[156] was approved for a six-month study at Stanford University, and a Stanford University page confirms that he was a visiting student at the Structures and Composites Laboratory at the university's Department of Aeronautics and Astronautics.[157] Assuming his only affiliation in the US was at Stanford, then it is reasonable to conclude he was involved in an NSF-funded research project there and incorporated that into his doctoral studies at NUAA. He was a

154. The funding information was only listed in Chinese, as "一院高效联合创新基金 (CALT201603)."

155. "本院概况 [School Overview]," 中国运载火箭技术研究院 [China Academy of Launch Vehicle Technology], accessed June 14, 2020, http://www.calt.com/n481/n489/index.html.

156. No English appears in the dissertation. An approximate translation of the title is "Research on Adaptive Tracking Techniques of Delayed Nonlinear System Parameter Identification and Damage Detection" (基于自适应追踪技术的迟滞非线性系统参数识别与损伤检测研究).

157. "关于公布博士生出国短期访学项目资助名单的通知 [Announcement of the Publication of the List of Funded Doctoral Candidates in the Short-Term Study Abroad Program]," 南京航空航天大学研究生院 [Nanjing University of Aeronautics and Astronautics Graduate School], March 17, 2014, http://www.graduate.nuaa.edu.cn/2014/0317/c2146a52124/page.htm.; "Tengfei Mu," Stanford Engineering Structures and Composites Laboratory, http://web.stanford.edu/group/sacl/people/mu.html.

nominee for the 2018 "Most Beautiful Commercial Flyer" (最美商飞人) award for his work as a manager at the Shanghai Aircraft Design and Research Institute of the Commercial Aircraft Corporation of China (COMAC), China's leading contender to break the grip that Boeing and Airbus have on the global market for widebody commercial aircraft.[158]

X. Conclusions and Recommendations

The surveyed scientific publications reveal not just collaboration between US research institutions and PRC defense-affiliated entities, but also pathways through which those entities can build their human capital, harvest US S&T research at its source, and divert it to PRC defense research and weapons program development. The risks to national security are serious since such diversions could erode or eliminate US military superiority with lethal consequences in the event of an armed conflict. Regardless of whether US-based researchers or their employing institutions intend such an outcome, S&T collaborations with the PRC's Seven Sons universities have jeopardized the integrity and security of US research and the federal funding that supports it. The US research enterprise does not have these problems in hand, despite repeated assurances to the contrary.

It is beyond the scope of this chapter to determine if US university administrators wittingly authorized any of the research collaborations reported in the collected corpus or if any prior vetting or approval procedures were followed. To the extent that any research identified in this corpus was considered fundamental in nature, it may not have violated US export control laws or been subject to other regulatory controls that would have restricted the underlying collaborations. Moreover, if US-based researchers failed to disclose foreign collaboration

158. "'携手筑梦 · 感动有你' 2018 年度最美商飞人来了 ['Working Together to Build Dreams, Moving You': The Most Beautiful Commercial Flyer of 2018 Is Here]," 中国航空新闻网 [China Aviation News Network], January 28, 2019, http://www.cannews.com.cn/2019/0130/189051.shtml.

(e.g., as required by US employers or by federal granting agencies), those omissions may amount to administrative or regulatory noncompliance rather than unlawful activity.

Profiles of the seven PRC universities and related entities reveal a host of concerns, some of which are common to most or all of the universities. Examples include:

- Although many articles in the corpus are English-language publications, the most revealing information on the PRC-based entities came from Chinese-language sources. This complicates the efforts by US research institutions and government agencies to evaluate risks to research partnerships with the Seven Sons universities.
- Likewise, some of the Seven Sons universities host subdivisions and national laboratories that conduct defense research using innocuous-sounding English names, and/or provide sparse information on their structures or missions in English-language sources. This obfuscation of ties to PRC defense programs inhibits the ability of US institutions to conduct adequate due diligence on partnerships.
- All of the Seven Sons universities state that they promote or implement national military-civil fusion policies. Consequently, US institutions should assume that these universities actively seek ways to develop defense applications in otherwise benign research fields, creating risk assessment challenges.
- Many of the Seven Sons universities have documented partnerships with PLA entities and/or oversee classified programs on behalf of the PRC government.
- Several of the Seven Sons universities have partnerships with the PRC's defense industrial base, including state-owned weapons design and production conglomerates, which may lead to additional economic concerns over potential future intellectual property rights, patents, etc.
- Five of the Seven Sons universities (HIT, NWPU, BIT, NUAA, and NJUST) published graduate theses and dissertations that

credit US government funding support. The authors were visiting students at US institutions and were typically funded by the CSC. This raises questions about whether a) the PRC government is intentionally placing students into key US research programs to gain access to federally funded research; and b) whether US institutions should be training students from institutions that are closely tied to the PRC military and who may incorporate the research that they pursue in the United States into PRC programs that could adversely impact US national security.

Robust implementation of Presidential Proclamation 10043 will make future collaborations with Seven Sons affiliates of the sort documented in this chapter more difficult. But to declare victory and move on would be hasty. Our findings stand as monuments to a colossal failure of vision that has prevented the US research enterprise from appreciating the risks that such collaborations posed and from adopting appropriate safeguards of its own accord. Too little has changed in that regard, and many of the same vulnerabilities persist.

The next chapter moves beyond the empirical record established here to propose a new paradigm for preserving research integrity and security from the perspective of active members of the academic research community. For the purposes of closing out this chapter, we therefore offer a limited set of recommendations that hew closely to our findings.

1. Expand the scope of this report.

- Other articles within the collected corpus merit scrutiny to identify potential risks to US entities. Further studies using the methodology detailed in the Appendix may identify US research collaborations with other PRC institutions that support the PRC's defense programs, especially those beyond the immediate compass of Presidential Proclamation 10043. This methodology could also be applied to collaborations with institutions and researchers from other nations.

- The economic implications of US-China research collaboration should be explored more fully. As PRC universities have partnerships with state-owned enterprises in both civilian and military sectors, further investigation is needed to determine if US taxpayers are funding technologies that are patented or commercialized by PRC universities or partner companies.

2. Expand vetting and due diligence of collaborations with PRC partners.

- US research institutions should determine if the US-based coauthors were recipients of or worked on federal grants that related to the research published in the scientific literature this report identifies.
- US research institutions should compile information on all PRC organizations that have demonstrable connections to the PRC's defense research and industrial base. They should obtain this information primarily through PRC-based vernacular information sources and create collective information sharing mechanisms that can be used to enhance vetting of visiting PRC students and scholars, as well as ramp up due diligence on proposed or existing research partnerships with the PRC.
- US research institutions should partner / share information with foreign allies to enhance those nations' due diligence and risk assessments since the PRC's Seven Sons universities collaborate with many nations, not just the United States.

3. Enhance administrative oversight.

- Benign research cannot be separated a priori from potential dual-use applications conducted at foreign institutions that support defense research such as the Seven Sons universities. US research institutions should mandate disclosures and preapprovals for all forms of S&T collaboration with PRC institutions—even when the research is considered fundamental in nature or published openly—and undertake disciplinary measures when individuals fail to seek approvals. Effective oversight depends on comprehensive reporting and periodic review.

4. Create or revise common moral and ethical standards with respect to research collaboration in academia.

- US research institutions should create a common framework to determine when research collaborations, student and researcher exchanges, and other forms of partnership may contribute to the military or domestic repressive capabilities of authoritarian regimes, violate democratic values or human rights, or involve unethical research practices.
- US research institutions should develop, maintain, and share lists of foreign partners (distinct from governmental lists) that they consider off limits for collaboration based on agreed-upon standards and documented evidence of programs, activities, or associations that are inimical to US interests and values.

APPENDIX TO CHAPTER 1

Sources and Methodologies

Academic literature is a rich but underutilized resource for investigating PRC science and technology (S&T) organizations, researchers, and programs. While some studies have focused on international publications in the English language, Chapter 1 identifies publications tied to PRC defense and weapons programs that have appeared in English-*and* Chinese-language sources. Scrutiny of both language spaces is essential to enhancing our understanding of not just the nature and scale of S&T research in the PRC, but also the risks that it may pose to US national security and economic interests and the integrity of the research conducted at US institutions.

The chapter surveys S&T collaborations between US research institutions (academia and government laboratories) and seven PRC universities that have the core mission of supporting the PRC's defense research and industrial base (the "Seven Sons of National Defense" 国防七子). By searching online bibliographic metadata, it assembles a corpus of English- and Chinese-language S&T publications with coauthors from one or more of the Seven Sons universities and at least one US institution. That metadata comprises article title, authors, affiliated institutions, publication source or date, and funding information (when available).

This methodology is generalizable. It can be applied to research collaborations between the United States and its allies and partners on the one hand and additional institutions from the PRC or third countries on the other.

Sources of Bibliographic Metadata

Chapter 1 rests primarily on searches of the bibliographic metadata available on the China National Knowledge Infrastructure (CNKI) platform, one of the most comprehensive online aggregators of peer-reviewed academic journals, conference proceedings, theses, and dissertations in the PRC. As of mid-2020, its main China Academic Journals database offered full-text and full-image access to more than nine million articles from almost seven thousand academic journals published in the PRC since 1994.[1]

CNKI hosts a smaller number of international journals, as well as publication records from Elsevier, but metadata for the latter can differ in the level of detail. For instance, CNKI provides the full names of Chinese authors using Chinese characters, whereas Elsevier's ScienceDirect website may only list authors' transliterated last names and first/middle initials or a Western first name provided by the author. CNKI also usually includes the official name of associated PRC institutions in characters (some of which have misleading or truncated English translations) and PRC-based research grant or funding project names. That information is often absent from international databases such as Scopus and Elsevier. However, CNKI does not contain the entirety of the PRC's published scientific record; therefore, the corpus collected in this chapter cannot be considered an exhaustive sample of all potentially relevant articles.

The Tongfang Knowledge Network, a PRC state-owned technology group founded by Tsinghua University, develops and owns CNKI's databases. It is supported by the Ministry of Science and Technology, Ministry of Education, the General Administration of Press and Publications, and the CCP's Central Propaganda Department.

CNKI employs several websites or mirrors; www.cnki.net was primarily used for this chapter. Searches on CNKI's website were limited to publications covering scientific and engineering disciplines and

1. "China National Knowledge Infrastructure (CNKI) Frequently Asked Questions," East View Information Services, accessed June 14, 2020, https://www.eastview.com/resources/cnki-faq/.

therefore excluded holdings in economics, law, history, and other social sciences.

Search Process

Searches were conducted in the following CNKI-designated journal categories:

(A) Mathematics / Physics/ Mechanics / Astronomy
(B) Chemistry / Metallurgy / Environment / Mine Industry
(C) Architecture / Energy / Traffic / Electro-mechanics, etc.
(D) Agriculture
(E) Medicine and Public Health
(I) Electronic Technology and Information Science

Metadata attributes (e.g., author, institution, and funding source) were searched using the "advanced search" feature available on the Chinese-language interface of CNKI's web portal. The search criteria were:

- Articles published between January 1, 2013 and March 31, 2019 in order to spotlight recent activity.
- Chinese names of each of the Seven Sons universities and the Chinese term for "United States" (美国) in the author affiliation fields.
- Chinese names of each of the Seven Sons universities in the author affiliation field and the United States (美国) in the funding support field.[2]

Data Conditioning

CNKI's web interface supports exporting search results into a spreadsheet (.xls) file. Users can manually select which attributes to export. For the purposes of Chapter 1, attributes selected for export included authors, affiliations, title, journal source, year/date of publication, and funding source (if provided).

2. Searches and data conditioning process were repeated for each of the Seven Sons universities; hence seven distinct searches were conducted and the data was compiled separately.

The exported raw data required significant conditioning, such as parsing some of it into separate cells, and standardizing the minor English-language name variants for a given organization or unit.

Search results in CNKI also included many English-language publications from international sources, nearly all of which also appeared in Elsevier's ScienceDirect website. If additional bibliographic information was found via Elsevier that did not appear on CNKI's portal, that information was merged into the spreadsheet.

After all relevant data was collected and conditioned, the records were sorted chronologically and according to the number of articles published by each institution.

Supplemental Research

Supplemental internet research was conducted on an opportunistic subsample of authors, which provided additional detail on their affiliations, backgrounds, and sources of research funding. This detail appears in the featured case studies. The sources for that research include the institutional websites of PRC universities, research grant and funding programs, and government organizations and companies, as well as faculty profile pages, journals, and university libraries.

CHAPTER TWO

Global Engagement: A New Paradigm for Managing Risk

KEVIN GAMACHE AND GLENN TIFFERT

I. Introduction

American research institutions operate in a hyper-globalized environment with a wide degree of autonomy. This plays to their many strengths, but it also exposes them to risks that they are ill-equipped to handle. Chapter 1 of this report documents one urgent category of those risks, but there are a great many others that touch nearly every discipline of knowledge, including: censorship, espionage, IP theft, foreign surveillance and intimidation of US campus communities, and foreign interference in research and academic affairs.[1] Here we take up the question: What is to be done?

In general, the response to these risks has been to recommend better training and stricter compliance and to reach for incremental legislative or regulatory fixes. While prudent in a narrow sense, this approach

1. Glenn D. Tiffert, *Compromising the Knowledge Economy: Authoritarian Challenges to Independent Intellectual Inquiry*, National Endowment for Democracy, April 2020, https://www.ned.org/sharp-power-and-democratic-resilience-series-compromising-the-knowledge-economy; Anastasia Lloyd-Damnjanovic, "A Preliminary Study of PRC Political Influence and Interference Activities in American High Education," *Woodrow Wilson International Center for Scholars*, 2018, https://www.wilsoncenter.org/publication/preliminary-study-prc-political-influence-and-interference-activities-american-higher.

is nevertheless myopic, fragmented, and reactive. It obviates the need for strategic thinking, cedes the initiative, and keeps our institutions on the backfoot, ever playing catch-up.

Over time, the shortcomings of this approach have grown too obvious to ignore. Some risks are not responsive to compliance-driven remedies and therefore smolder, for instance self-censorship and the weaponization of student enrollments.[2] For others, successive regulatory measures have deposited layers of well-intentioned disclosure and reporting mandates, each with its own demands and destination. Likewise, lists drawn up by government agencies with different jurisdictions and missions impose a profusion of legal regimes on their enumerated entities and technologies. In the last several months alone, two more such lists have appeared on the horizon, courtesy of Section 1281 of the 2020 National Defense Authorization Act and Presidential Proclamation 10043.[3]

These interventions map unevenly onto a research enterprise that includes private firms, national laboratories, private universities, and multi-campus state university systems with diverse risk profiles and capacities. The cumulative result is a patchwork of poorly integrated, ill-fitting solutions that are updated irregularly, create gaps of their own, and make compliance progressively more burdensome and prone to failure. Even assuming perfect implementation, gains may be short-lived because determined adversaries can adapt faster than government rulemaking can keep pace, for instance by exploiting the spaces between

2. Sheena Chestnut Greitens and Rory Truex, "Repressive Experiences among China Scholars: New Evidence from Survey Data," *The China Quarterly*, 2019, 1–27, https://doi.org/10.1017/S0305741019000365; Tiffert, *Compromising the Knowledge Economy*, 6.

3. *National Defense Authorization Act for Fiscal Year 2020*, Public Law 116-92, § 1281; US President, "Proclamation 10043 of May 29, 2020: Suspension of Entry as Nonimmigrants of Certain Students and Researchers From the People's Republic of China," document 85 FR 34353, *Federal Register* 85, no. 108 (June 4, 2020), https://www.federalregister.gov/documents/2020/06/04/2020-12217/suspension-of-entry-as-nonimmigrants-of-certain-students-and-researchers-from-the-peoples-republic.

the rules, obfuscating identities or working through surrogates.[4] The gains may also be illusory and breed complacency to the extent that such circumvention strategies succeed.

More to the point, this system can operate perfectly and still prejudice the interests of the United States.[5] As Chapter 1 has shown, research institutions are obliged to observe the law, but if the law marks a path for them to collaborate with a given entity, then they are free to take it irrespective of the ramifications for national security and economic competitiveness. Until June 5, 2020, only two of the PRC's Seven Sons of National Defense universities were on the Department of Commerce's Entity List, and while that number has since doubled, it hardly matters if the collaboration at issue falls within the list's fundamental research exemption. And the Seven Sons are just the tip of the spear; within the PRC alone there are dozens of other universities and research institutes at the national, provincial, and municipal levels that are deeply involved in military research, including some of the country's most highly-regarded universities, such as Tsinghua University and the University of Science and Technology of China.[6] Add in other countries like Russia and Iran, and the scope of the problem grows daunting.

We believe that continuing down the current road will yield diminishing returns and breed harmful dynamics between US research institutions and their regulators. In light of recent shifts in government policy, the

4. Linda Lew, "More 'Eyebrows on Fire': Another Chinese University Dodges Export Controls on US Software," *South China Morning Post*, June 25, 2020, https://www.scmp.com/news/china/diplomacy/article/3090615/more-eyebrows-fire-another-chinese-university-dodges-export?utm_source=copy_link&utm_medium=share_widget&utm_campaign=3090615.
5. Amy Hawkins, "Banned but Not Broken," *The Wire China*, May 31, 2020, https://www.thewirechina.com/2020/05/31/sensetimes-american-axis.
6. Alex Joske, *Picking Flowers, Making Honey; The Chinese Military's Collaboration with Foreign Universities*, Report No.10 (Canberra: Australian Strategic Policy Institute, 2018), https://www.aspi.org.au/report/picking-flowers-making-honey; Alex Joske, *The China Defence Universities Tracker*, Report No. 23 (Canberra: Australian Strategic Policy Institute, 2019), https://www.aspi.org.au/report/china-defence-universities-tracker.

discretion to pursue foreign engagements depends more than ever on new thinking—on research institutions reinventing their internal risk assessment and management processes to deliver higher quality, granular decisions. As evidence of foreign interference and exploitation accumulates in the research enterprise, external pressure to curtail its autonomy and openness in the name of national security and economic competitiveness will intensify, and bluntly prescriptive proposals will come increasingly to the fore. That outcome is avoidable, but only if we change the paradigm.

In this chapter, we propose the concept of a Global Engagement Risk Assessment & Management Program (GERAMP), which provides an organizational and operational framework for how research institutions should assess and manage foreign engagement risk. Second, we propose the establishment of a Global Engagement Review Office (GERO) to provide administrative leadership, oversight, and coordination of the GERAMP and to liaise with relevant federal entities. Third, and most fundamentally, we recommend that research institutions redefine their posture by adopting Operational Security (OPSEC) as the governing paradigm for foreign engagement risk. Fourth, we propose a Global Engagement Maturity Model (GEMM) through which institutions can formalize and optimize their internal capabilities to assess and manage foreign engagement risk. And fifth, we recommend the constitution of a new government-sponsored entity that would contribute unique research and analytic capacity on foreign engagement risk and establish a unified point of contact about it for the research enterprise.

II. Key Principles and Commitments

The recommendations in this chapter are guided by and consistent with a set of principles and commitments that are fundamental to the manner in which the research enterprise operates in the United States. These principles and commitments include:

- *Institutional autonomy and openness.* Academic independence and open flows of people, information, and ideas are integral to the success of the US research enterprise.

- *Empowerment*. Empowering research institutions to manage their foreign engagements with greater rigor and better information is essential to upholding their autonomy and safeguarding research integrity and security.
- *Strategic competition*. It is not in the national interest for US research institutions to support the defense R&D or industrial base of strategic competitors such as the PRC, even if that research is designated fundamental and not subject to export controls or other restrictions pursuant to National Security Decision Directive (NSDD) 189.[7]
- *Values*. US institutions should not collaborate on research with entities that support the surveillance capabilities of authoritarian regimes or the capacity of those regimes to violate democratic values or human rights.
- *Unacceptable risks*. While foreign state-directed influence over US research and individuals recruited through foreign state talent programs are not synonymous with espionage or intellectual property theft, they represent unacceptable risks. These efforts serve national strategies to acquire sensitive US information and technology. Similarly, foreign activities targeting US research can threaten US national or economic security even if there is no involvement or control by a foreign state entity.
- *Inclusivity*. Strategic competitors, such as the PRC, co-opt, incentivize, direct, and/or coerce individuals to transfer technology and intellectual capital irrespective of the ethnicities and nationalities of those individuals. For instance, the PRC targets members of the ethnic Chinese diaspora, individuals who do not claim Chinese ethnicity, and PRC and US citizens alike *after* they obtain expertise and/or placement and access to critical US research or technologies. Focusing primarily on students and scholars in the

7. The White House, *White House Directive on Fundamental Research Exemption*, National Security Decision Directive-189, September 21, 1985, https://www.aau.edu/key-issues/nsdd-189-white-house-1985-directive-fundamental-research-exemption.

United States who are foreign nationals is therefore wholly inadequate to the relevant risks. Because any person can facilitate the unauthorized transfer of technology and intellectual capital, due diligence must be performed on every participant in a foreign research collaboration.

- *Transparency, integrity and reciprocity*. Research institutions should not compromise their standards of transparency, integrity, and reciprocity to facilitate foreign engagements. They must be prepared to pause, throttle back, or terminate engagements if those standards are not met.
- *Partnership*. Safeguarding national security and economic competitiveness are chiefly the responsibilities of the US government. Nonetheless, cooperation between research institutions and federal agencies is integral to the success of those efforts and can greatly enhance them.
- *Greater investment*. Increased US government funding for domestic research and innovation is necessary to safeguard research integrity and security. Strategic competitors, such as the PRC, will continue to offer opportunities to US entities that may not be in the long-term national interests of the United States. The US government and research sector must also devote greater effort to *domestic* commercialization of R&D.
- *Incentivized performance*. Government funding decisions should reward institutions that implement robust research integrity and security programs and penalize those that do not.

III. Key Constraints

Foreign efforts to interfere with or exploit research activities can take many forms, from critical skills acquisition and espionage to funding arrangements that unduly influence the conduct of research, lead to the loss of future value, and erode control over intellectual property. However, serious constraints limit the capacities of the US government and US research institutions to assess and mitigate the risks posed by foreign engagements. These constraints include the following:

- *Disparate missions*. Research institutions and the government understand their missions and constituencies differently. This can generate friction, mistrust, and gaps in mutual understanding.
- *Incomplete tools*. Research institutions have not been sufficiently responsive to foreign engagement risks because they lack incentives to think outside of the box of their formal compliance mandates. Meanwhile, criminal law cannot compensate for a dearth of civil remedies because, strictly speaking, many risks do not lead to prosecutable crimes.[8] Absent a new paradigm, acute risks will continue to fall through the cracks.
- *Barriers to information sharing*. The US intelligence community relies heavily on classified information to identify threats posed by foreign entities. This severely limits its ability to share information with the research community. Likewise, the FBI and other federal law enforcement components are often unable or unwilling to share timely or sufficiently detailed information from investigations. Meanwhile, research institutions guard their autonomy and worry that involving law enforcement and the intelligence community in internal matters might redound upon vulnerable members of their communities and the climate for academic freedom.
- *Regulatory disorder*. Legal mandates and reporting requirements are often inconsistent, poorly coordinated, burdensome, and confusing. For instance, federal funding agencies may request the same or similar data in different ways, when uniform collection would be more reliable and efficient. Regulatory terms may also lack clear definitions, which compromises implementation.
- *Weak governance*. Some institutions or unauthorized personnel within them enter into foreign contracts and other commitments without first performing rigorous due diligence and risk assessments. Many also have weak compliance cultures that undermine

8. Margaret K. Lewis, "Criminalizing China," *Journal of Criminal Law and Criminology* 111, no. 1 (Seton Hall Public Law Research Paper, forthcoming 2020), https://ssrn.com/abstract=3600580.

the implementation of existing institutional policies and processes and impair the fulfillment of regulatory mandates.

- *Institutional incapacity*. The resources, domain knowledge, language skills, and leadership available to identify, evaluate, and manage the risks implicated in a lawful foreign engagement vary greatly from one research institution to another. It is unrealistic to expect ordinary administrators, research program managers, development officers, and grant reviewers to possess them in sufficient measure.
- *Governmental incapacity*. Area expertise, critical language skills, and the domain knowledge to make informed technical assessments of frontier science and technology are in short supply in government.[9] Rulemaking is fragmented and cumbersome, and lags behind the best available threat information. For instance, the US government has routinely issued visas to students and researchers to work in critical STEM fields who are directly tied to foreign military programs or other organizations on the Department of Commerce's Restricted Entity List. Research institutions may wrongly assume that the admitted individuals are low-risk.

IV. Basic Steps for Addressing the Problem

Due diligence is the cornerstone of any risk assessment and management program. In the context of foreign engagements, institutions and researchers must ensure that all of the participants in a prospective collaboration are clearly documented irrespective of whether the collaboration will be formal or informal. They must also verify that the collaboration's nature, scope, and purpose are well-defined and transparent, consistent with relevant laws and regulations, undertaken with full knowledge and consent, and in a manner that avoids harm to core values and national interests. At a minimum, this requires robust commitments such as these:

9. Jude Blanchette and Seth G. Jones, "The U.S. Is Losing the Information War with China," *Wall Street Journal*, June 16, 2020, https://www.wsj.com/articles/the-u-s-is-losing-the-information-war-with-china-11592348246.

- *Know your partners.* Institutions and researchers must understand who their prospective partners are and not rely on how those partners represent themselves. Background research should draw on multiple information sources, in cooperation with government agencies as necessary. For an institutional partner, this will ordinarily include analysis of its past activities, the sectors it operates in or is associated with, its beneficial owners, and the commercial and ethical standing of its governing body.

  Vetting of individuals should determine whether an individual and their associates are from reputable organizations, possess relevant qualifications, and have any unexplained gaps or items of concern in their backgrounds. High-risk collaborators sometimes supply sanitized CVs that omit important publications, affiliations, and awards, or mistranslate them into English. Background research can bring more complete, native-language versions of their CVs to light. Searching their publication records in their native languages can also expose valuable information. The depth of this background research will depend on the nature of the collaboration, but it should include all of the key participants, not just the principal investigators, because experience has shown that graduate students and postdoctoral scholars are a significant threat vector. Insider threat is not limited by ethnicity, institutional affiliation or country of origin.
- *Know your funders.* Research institutions are struggling to manage the risk associated with sponsored research and philanthropic giving, and they are suffering significant reputational harm in the process.[10] Entanglements with Huawei and SenseTime in particular demonstrate poor due diligence and risk forecasting.[11] Sponsored research and philanthropic gifts open channels for foreign entities

10. Susan Svrluga, "Epstein's Donations to Universities Reveal a Painful Truth About Philanthropy," *Washington Post*, September 8, 2019, https://www.washingtonpost.com/local/education/epsteins-donations-to-universities-reveal-a-painful-truth-about-philanthropy/2019/09/04/e600adae-c86d-11e9-a4f3-c081a126de70_story.html.
11. Hawkins, "Banned but Not Broken."

to access and influence research and academic affairs and impinge on institutional autonomy.[12] The financial shock of COVID-19 has sharpened these vulnerabilities. Greater safeguards and stricter oversight, with formal representation from area and subject matter specialists who can put foreign funders into context, are broadly necessary.

- *Take contracts seriously*. A foreign entity may propose to formalize a collaboration using its own contract while the US partner may lack the legal training to adequately comprehend the terms of that document and its omissions. To protect their interests, institutions should adopt checklists and model templates to guide the negotiation of all collaboration agreements. Prior to signature, authorized personnel should review and approve the final texts to ensure that they satisfactorily address, as appropriate: dispute resolution; choice of law; governing language; potential threats to research integrity, intellectual property, and reputation; and applicable regulatory requirements and standards of data governance, ethics and human rights.[13]
- *Train*. Institutions should sensitize their personnel to potential risks when collaborating with a foreign partner, train them in

12. John Fitzgerald, "How Bob Carr Became China's Pawn," *Australian Financial Review*, November 8, 2018, https://www.afr.com/policy/what-you-should-know-about-bob-carr-and-china-20181105-h17jic; Primrose Riordan, "London School of Economics Academics Outraged by Proposed China Programme," *Financial Times*, October 27, 2019, https://www.ft.com/ content/2dd5ed50-f538-11e9-a79c-bc9acae3b654; Josh Rogin, "University Rejects Chinese Communist Party-linked Influence Efforts on Campus," *Washington Post*, January 14, 2018, https://www.washingtonpost.com/opinions/global-opinions/university-rejects-chinese-communist-party-linked-influence-efforts-on-campus/2018/01/14/c454b54e-f7de-11e7-beb6-c8d48830c54d_story.html; Gordon Lubold and Dustin Volz, "U.S. Says Chinese, Iranian Hackers Seek to Steal Coronavirus Research," *Wall Street Journal*, May 14, 2020, https://www.wsj.com/articles/chinese-iranian-hacking-may-be-hampering-search-for-coronavirus-vaccine-officials-say-11589362205.

13. Frank Bekkers et al., "Checklist for Collaboration with Chinese Universities and Other Research Institutions," *HCSS Global Trends*, The Hague Centre for Strategic Studies, January 31, 2019, https://hcss.nl/report/checklist-collaboration-chinese-universities-and-other-research-institutions.

applicable laws, policies, and processes, and identify internal resources for assistance. For example, foreign partners may have undisclosed relationships, operate in different ethical and political environments, and be ignorant of US legal requirements. Observance of US norms governing informed consent and human subjects research may be uneven. Foreign state actors may reap project data and use it for unanticipated ends. Insiders may transfer technology and intellectual capital without proper authorization. Researchers should possess sufficient background information to weigh and prepare for those contingencies.

Informal collaborations are vital to the advancement of knowledge. They emanate from the freedom of inquiry, a core academic value that requires support. At the same time, informal collaborations present nontraditional intelligence collectors with soft targets for exploitation. Researchers must be vigilant against the risks that informal collaborations may present and act responsibly, ethically, and in good faith. Expanded Responsible Conduct of Research (RCR) training can help them to do so. It can also clarify the scope of a researcher's authority to enter into commitments and the processes to be followed in bringing a collaborative opportunity to fruition.

- *Iterate and adapt*. Laws, regulations and government policy evolve. Likewise, the scope of a collaboration, its participants, their behavior, and other circumstances may change, which can alter its original risk profile. Effective due diligence must periodically review ongoing collaborations and formal agreements, reevaluate risk, and adjust safeguards as necessary. It must also ensure that ongoing collaborations and formal agreements meet the latest guidance and legal requirements and bring them into compliance if they do not.

Foreign exploitation of the US research enterprise under the cover of lawful activity is a present danger.[14] Chapter 1 has shown that even

14. US Department of Justice, *Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions since 2018*, 2020, https://www.justice.gov/opa/page/file/1223496/download.

openly published research of a basic or fundamental character is susceptible to that threat. This should not surprise us. If the value of the American research enterprise was reducible to the information content of its published work, then most foreign students and scholars would never seek US partners; they would simply stay at home and read more. They seek collaboration to tap US resources, such as expertise, laboratories, and data, and to gain intangible benefits. In the United States, they can master the art of science through exposure to a highly successful culture of knowledge production; hone practical skills such as how to operate complex apparatuses, perform difficult experiments, and manage research groups; explore the frontiers of their disciplines; collaborate with world-class colleagues across fields; and develop professional networks that span the globe. All of this makes them better at what they do, a highly desirable outcome unless it prejudices US national security and economic interests or ethical and human rights norms.

To illustrate that point, US research institutions should welcome materials scientists and high-energy physicists from most foreign institutions and nations, but not those with active weapons research programs mobilized against US strategic interests. Likewise, collaborating with AI researchers or geneticists from countries with authoritarian surveillance states and weak human subjects protections is not equivalent to collaborating with those from democracies. Different standards and levels of scrutiny should apply. Context matters.

In principle, research institutions are best placed to make these decisions for themselves. But because their performance has fallen short of necessity, their credibility is increasingly at issue. Reclaiming it depends urgently on enhancing their internal controls in ways that are alive to the full spectrum of potential risks that their foreign engagements might entail and on developing processes and tools to make better decisions.

A. Think Strategically

A comprehensive Global Engagement Risk Assessment & Management Program (GERAMP) would achieve those objectives. Such a program would rigorously assess the types and degrees of risk implicated in a

given venture and mitigate them to acceptable levels by suggesting proportionate governance and oversight strategies.

A GERAMP involves many considerations, but several are key. First, it should exercise *comprehensive oversight* over all of the institution's international engagements. Its associated policies and processes should foster cultures of integrity, safety, and security in order to protect the people, information, and assets that form the backbone of our academic and research ecosystems. Second, these policies and processes must be accompanied by regular *training in practical measures* to mitigate foreign engagement risk in informal and formal research activity; uphold core institutional values; protect affiliates and intellectual property; and support compliance with policies, laws and regulations.

Third, *transparent reporting* requirements are essential to effective risk management, as are processes that deliver reported information to decision makers in a timely and actionable manner and that archive this information for convenient, future reference. Policies governing conflicts of interest and commitment can catalyze that capacity by requiring prompt disclosures of external affiliations, relationships, and financial commitments. They have the added benefit of clarifying the responsibilities that affiliates have to their home institutions.

Fourth, when administrators perform a risk assessment, they should *document in detail* the information that they evaluated in order to guide not just future decisions but also re-examinations of past ones.

Fifth, institutions must incorporate into their risk reporting cycles *ongoing reviews* of their internal security strategies, policies, and processes, especially as these relate to foreign interference.

Implementing an effective GERAMP can play a major role in enhancing the security of an institution's personnel, facilities, and intellectual capital. For such a program to be effective, personnel must be aware of existing threats, be able to implement countermeasures when appropriate, and be observant of nontraditional collection activities directed at their institution. This is possible only if all members of the institution are cognizant of the range of threats to the research enterprise and actively support the risk assessment and management program.

What Forms Can Countermeasures Take?

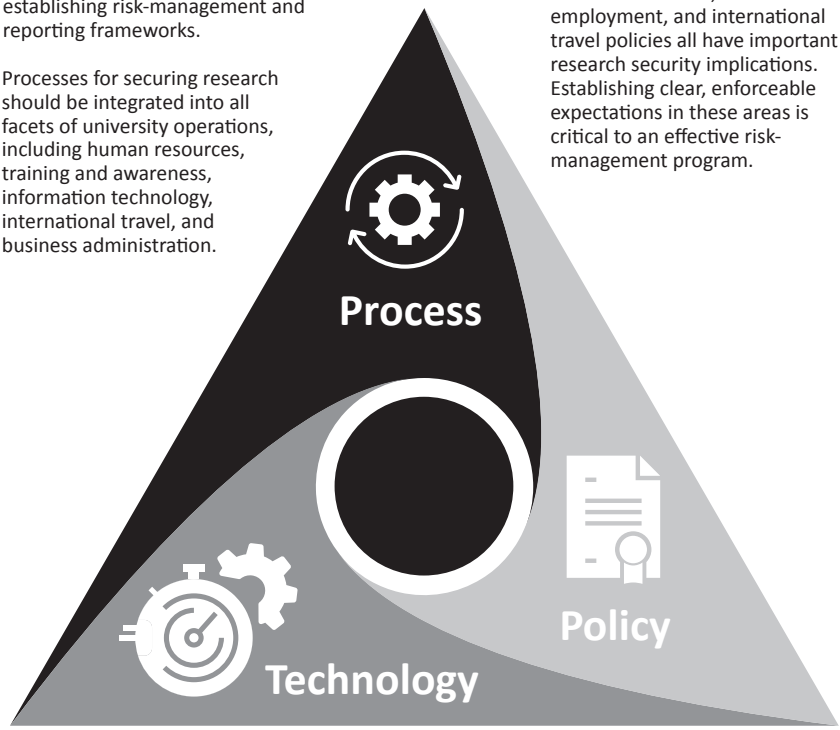
Process Solutions

Process solutions include such actions as vetting visiting scholars, monitoring computer networks for illicit exfiltration of research data, incorporating data-loss prevention systems on networks, and establishing risk-management and reporting frameworks.

Processes for securing research should be integrated into all facets of university operations, including human resources, training and awareness, information technology, international travel, and business administration.

Policy Solutions

Conflict of commitment, financial conflict of interest, external employment, and international travel policies all have important research security implications. Establishing clear, enforceable expectations in these areas is critical to an effective risk-management program.



Technology Solutions

Incorporating technical solutions into your risk-management process, such as secure computing enclaves that meet federal requirements, can provide a solid foundation for securing data while minimizing the burden on researchers.

Figure 1. A Structured Approach to the Problem.

A GERAMP integrates mutually *reinforcing policy*, *process*, *and technology solutions* throughout a research institution's operations (Fig. 1). Key areas include: human resources, research and instruction, facilities security, information technology, international travel, development, and business administration.

To varying degrees, many research institutions already possess the elements of such a program.[15] But these frequently lack a strategic focus. The GERAMP confers conceptual and operational coherence upon them and brings them into alignment. It also establishes a methodology for identifying critical gaps and for ongoing optimization and growth.

It is beyond the scope of this chapter to supply an exhaustive list of such solutions, and institutional needs will vary. But for illustrative purposes, *clear policies* governing conflicts of commitment, financial conflicts of interest, external employment, international travel, and access to facilities and network resources are basic to effective risk management. Policies governing institutional accountability, the authority to contract, the duty of personnel to act in an institution's best interests, and the protection of dual-use technologies and controlled unclassified information (CUI) are valuable enhancements.

Processes are structured pathways through which policies are implemented. A GERAMP would, for example, establish processes to identify possible downstream applications of research undertaken in collaboration with foreign entities or research that might be a target for foreign interference or misappropriation. It would systematize the vetting of foreign entities across an institution, the monitoring of computer networks for unauthorized exfiltration of research data, and the implementation of data-loss prevention.

---

15. "University Actions to Address Concerns About Security Threats and Undue Foreign Government Influence on Campus," Association of Public & Land-Grant Universities, May 2020, https://www.aplu.org/members/councils/governmental-affairs/CGA-library/effective-science-and-security-practices---what-campuses-are-doing/file.

To those ends, research institutions could jointly establish and administer regional vetting centers staffed in part by cleared personnel authorized to enhance open-source vetting with insights drawn from sensitive or classified information. These regional centers would rationalize administrative spending, spread costs, and help to equalize the uneven distribution of actionable information, resources, and capacities across the research enterprise.

Regional vetting centers would be a platform through which member institutions could access expertise in critical languages and area knowledge. They would provide members access to open-source datasets for the purpose of conducting enhanced vetting of personnel seeking to access sensitive research. They would also be a ready source of advice and assistance in the vetting process.

In addition, regional vetting centers would provide centralized points of contact to liaise with the government on sensitive technologies, emerging threats, and new priorities in regulation and enforcement, as necessary. This would deepen mutual understanding and relationships of trust between government and research institutions, break down barriers to information sharing, and equip individual institutions to make better risk assessment and management decisions on their own terms.

The requirements to protect federally sponsored research have increased significantly over the past five years. Standards such as NIST Special Publication 800-171 Rev. 2 have imposed new regulatory burdens and financial costs on research institutions.[16] Incorporating *technological solutions* into the GERAMP can alleviate those hardships. For example, some institutions have established NIST 800-171-compliant Secure Computing Enclaves (SCEs) to house all of their federally funded research and to safeguard sensitive data.[17] These enclaves provide a

16. National Institute of Standards and Technology, U.S. Department of Commerce, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, February 2020, https://doi.org/10.6028/NIST.SP.800-171r2.

17. The Texas A&M University System Research Security Office Secure Computing Enclave, 2020, https://rso.tamus.edu/home/research-security/secure-computing-enclave.

preapproved secure infrastructure for internet connectivity, resource sharing, encryption, authentication schemes, and outside communications. They are physically separated from the institution's larger network yet operate transparently to minimize the burdens on their users.

Establishing SCEs at a regional level across the United States would allow member institutions to supply their research communities with security as a service at economies of scale. This would realize cost savings by reducing the need for institutions to duplicate one another's capital investments in compliant cyberinfrastructure. Member institutions would administer the enclaves jointly, with federal support for the purpose of strengthening the protection of the nation's most important research. Other technological solutions could also mitigate foreign engagement risk, such as the following:

- Robust access and device registration protocols that enforce minimum security standards and best practices on users of an institution's internal networks.
- Hardware encryption and high-performance VPNs to provide secure authentication and data protection on personally owned computing devices. This ensures that personnel are consistently using secure, managed computing platforms, even when they are working remotely or are outside of internal networks.
- Integrating commercial compliance management databases and private-sector threat management solutions into a research institution's due diligence program. These databases include products for management of export control processes, commercial sources for background checks, and more free-form databases that facilitate analysis of research relationships, collaboration, and sources of funding.

B. Establish a Global Engagement Review Office (GERO)

Safely navigating foreign engagement risk begins with a strategic program backed by formidable investments in institutional capacities, such as mastery of pertinent regulatory regimes, knowledge of foreign languages, and

access to advanced subject matter expertise. But it also requires a stable, accountable authority with substantial institutional capital that can marshal those resources effectively across multiple constituencies.

A GERO could achieve that goal. In a typical university setting, this office would report and make recommendations directly to the provost and would serve as the institution's focal point for coordination and oversight of all matters related to foreign engagement. It would regularly convene and chair a body similar to an institutional review board that would include: the university's research security officer; authoritative representatives from the offices of the provost and vice presidents for research and international affairs, from the council of principal investigators, and from the office of general counsel; and, depending on the matters before it, relevant foreign area and subject matter experts and senior representatives from the institution's development, sponsored research, and government relations offices. More specifically, the office would exercise unified leadership over the following domains:

1. Strategic Assessment and Management of Foreign Engagement Risk

- Institute a Global Engagement Maturity Model (GEMM, discussed below) to formalize the implementation and optimization of the GERAMP.
- Supervise GERAMP implementation, monitoring, and enhancement in coordination with other stakeholders (e.g., information technology and human resources).
- Advise institutional leadership and stakeholders on foreign engagement risk in accordance with established policies and processes.

2. Foreign Contracts, Gifts, and Compliance

- Produce up-to-date, practical guides, checklists, and templates on the institutional policies and processes governing foreign research collaborations, contracts, grants, and gifts. These will help to mitigate many of the risks posed by foreign engagements, and promote fulfillment of disclosure and reporting requirements, particularly

with respect to conflicts of interest and commitment. Train and periodically refresh personnel on these resources.[18]

- Systematically review all substantive engagements with foreign entities, whether formal or informal, for risk. The scope of this review will depend on the identity of the foreign entity and the nature of the engagement. Most cases will exit the review process at an early stage, parts of which could be implemented using online screening tools. Some cases will require higher levels of scrutiny. Archive the inputs to each review and its findings for future reference.
- Offer in-house consulting services on foreign engagement risk to empower local personnel on their own initiative to safeguard core academic values, research integrity and security, legal compliance, and institutional interests.
- Systematize data collection, metrics, disclosures, and reporting to satisfy GERAMP monitoring and compliance mandates related to foreign engagements.

3. Personnel

- Train and embed global research integrity and security officers throughout the institution as first points of contact. Depending on caseload, this role may be one of several in an individual's job description, particularly at lower levels of the institution's structure.
- Systematically vet foreign entities such as visitors, students, scholars, research collaborators, and research sponsors commensurate with the risks that they pose. Regional vetting centers could pool resources and data inputs, uniformly raise standards, and provide common points of contact for information sharing with peer institutions and the government.

---

18. In 2019, the AAU and APLU recommended a comprehensive communication campaign to raise awareness of current reporting requirements among faculty and other members of university communities. This recommendation should be expanded to encompass information and research security. Association of Public & Land-Grant Universities, https://www.aplu.org/projects-and-initiatives/research-science-and-technology/science-and-security.

- Analyze insider threats and adopt safeguards. Any person with access to technology and intellectual capital could transfer it without proper authorization. Clear procedures and training can mitigate this hazard and promptly detect its occurrence.
- Institute processes to promote and verify full disclosure of foreign interests and commitments.
- Institute processes to promptly revoke access to institutional systems and resources for affiliates upon separation.

4. Foreign Research Collaborations

- Analyze the potential end uses of research, whether fundamental or not. Identify and protect sensitive data and technologies, especially those with dual-use applications or with externalities that impinge on health and safety, core values, and ethical or human rights concerns.
- Create robust disclosure requirements for intellectual capital, particularly when it has commercial potential, so that measures can be taken early to safeguard it, such as applying for patent protection.
- Implement research communication agreements. Intellectual capital loss or property theft by untrustworthy or malign members of research teams is a persistent occurrence. Adopting a research communication agreement can mitigate this threat. Research communication agreements are used extensively in government and the private sector. They help research teams internalize sound information security practices by outlining a team's communication protocol, establishing ethical obligations to keep research materials confidential, and defining processes for sharing and releasing data.

Protecting potentially sensitive research results is especially challenging because it can be difficult to know in advance if results will be sensitive or valuable. Government program managers cannot bear the burden of determining this alone. All stakeholders have a responsibility to protect sensitive or valuable information and ensure that it is handled securely. A research communication agreement represents a middle

ground, providing a baseline layer of security that the principal investigator can augment mid-stream if appropriate.

5. Cyber

- Train personnel on cyber threat abatement and require periodic refreshers. End users are the most common vectors for cyber threats, but training can thwart these. Tech savviness is no guarantee that an individual appreciates the intricacies associated with this class of threat or the degree to which the research community is targeted.
- Implement Secure Computing Enclaves. These shared environments will rationalize expenditures and ease the uptake of best security practices without impeding research.

6. Foreign Travel

- Adopt institutional duty of care policies to protect personnel overseas.
- Institute review processes for foreign travel with respect to export controls, shipping, software use restrictions, and other security and safety concerns.
- Train affiliates located or travelling overseas in context-specific risk management and mitigation practices. Offer political risk counseling and technological support services, such as hardening smartphones, tablets, laptops, and other electronic devices against cyberattacks, cleaning them after travel to countries that are known threats, or supplying loaner devices.

7. Incident Reporting and Response

- Institute internal processes for reporting, investigating, and documenting foreign interference and exploitation.
- Supervise responses to research integrity and security incidents involving foreign entities in accordance with established incident and investigation processes.
- Recommend disciplinary processes for compliance failures of omission and commission.

- Preside over consultations with intelligence and law enforcement agencies, as necessary.

8. Sectoral Engagement

- The Academic Security & Counter Exploitation (ASCE) program was established in 2017 to help address the threat posed by foreign adversaries to US academic institutions.[19] This group initially consisted of universities conducting classified research and focused on specific processes and controls to protect sensitive information. The group has since expanded both its membership and its focus to deal with broader policy issues related to foreign interference. As of mid-2020, the group has more than four hundred members from more than 150 colleges and universities.
- The Association of University Export Control Officers (AUECO) is composed of export control officers and other compliance officers at US institutions of higher education.[20] University export control officers are primarily responsible for compliance with export, import, and trade sanctions policies such as the Entity List, but are frequently involved in other aspects of foreign engagement risk. AUECO provides a forum for information exchange and collaboration among its members and analyzes and advocates for policies and regulations of interest to higher education.
- The Council on Government Relations (COGR) is an association of leading research universities, affiliated medical centers, and independent research institutes that focus on the conduct of research at the highest standards; informed decision making on issues critical to the research and higher education community; and on deriving maximum benefit from investments in research conducted at member institutions.[21] COGR is an authoritative source of information, analysis, advice, policy perspective, and historical context for its members in the areas of research administration and compliance, financial oversight, and intellectual property.

19. Academic Security & Counter Exploitation Program, https://asce.tamus.edu.
20. Association of University Export Control Officers, http://aueco.org.
21. Council on Government Relations, https://www.cogr.edu.

9. Government Relations

- It is in the mutual interest of research institutions and the government to establish relationships of trust that can facilitate concise and accurate information sharing, appropriate oversight of federally funded research, and the early identification and protection of sensitive research. Establishing a single point of operational accountability or contact with the government for foreign engagements simplifies these tasks and helps institutions to stay abreast of trends and changing guidelines, prepare for new requirements, and avoid surprises.

Finally, the GERO would complement and coordinate with units that commonly fall under the authority of the vice provost for research to:

- Enhance export control offices at institutions that have them and create such offices at institutions that don't.
- Improve compliance with export control and related regulatory requirements and ensure successful implementation of technical control plans.
- Fully integrate protective security in planning, selecting, designing, and modifying facilities for the protection of personnel, information, and physical assets.
- Establish physical security measures that minimize or remove the risk of: a) harm to people; b) information and physical assets being rendered inoperable or inaccessible, or accessed, used, or removed without authorization.

C. Change the Paradigm

A GERO could be the cornerstone of a more robust approach to managing the foreign engagement risks that research institutions increasingly face, but without a corresponding paradigm shift from compliance-driven formalism to proactive Operational Security (OPSEC), its full potential might never be realized. OPSEC supplies a workflow for sustaining vigilance and innovation. It originated with the US military and involves five iterative steps (Fig. 2).

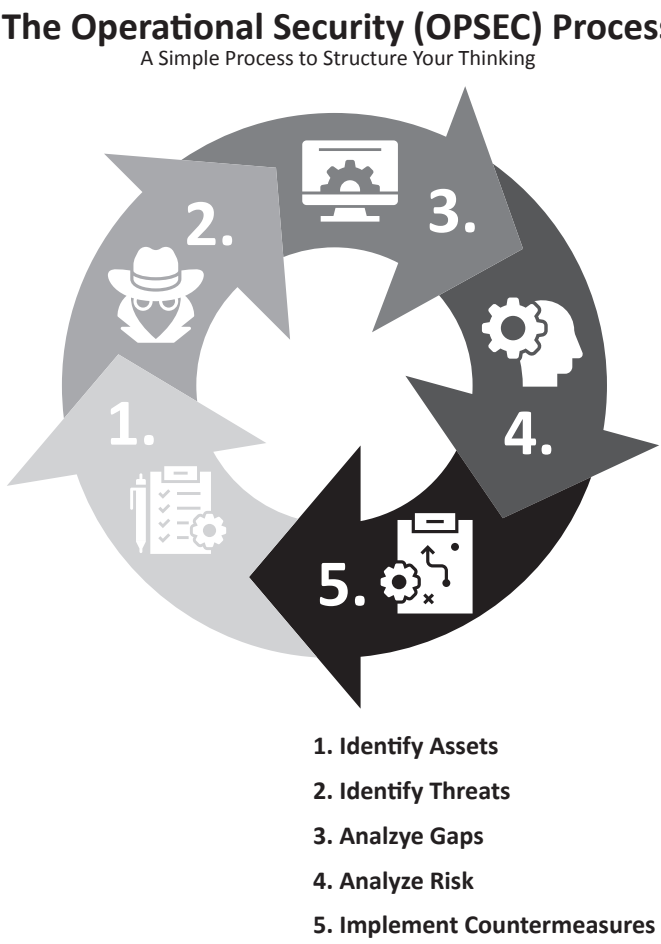


Figure 2. The OPSEC Process.

- *Identify assets.* This includes sensitive information such as research data, intellectual property, export control data, and personnel records.
- *Identify threats.* Evaluate the potential value of each category of sensitive information to third parties and institutional insiders and the threats that they may pose.
- *Analyze gaps.* Evaluate current safeguards, security gaps, and other vulnerabilities to determine what, if any, loopholes or weaknesses exist that could be exploited to gain access to sensitive information.

- *Analyze risk*. Compare threats and vulnerabilities to assess the potential risks posed by nontraditional collection activities and the likelihood of their occurrence. Nontraditional collection activities can occur during informal personal encounters over email, in labs, during conferences, and in other academic exchanges.
- *Implement countermeasures*. Formulate and execute a plan to reduce threats and mitigate risks. This might include updating hardware, creating new policies regarding sensitive information, or training affiliates on sound security policies and practices. Cost/benefit analysis can be used to evaluate potential countermeasures. Countermeasures should be straightforward, minimally invasive, and simple for affiliates to implement.

D. Create a Global Engagement Maturity Model

If the GERO drives the execution of an institution's GERAMP, then the GEMM provides the *strategic roadmap* for shepherding that program from its inception to full integration with all aspects of the institution's operations. Leading the formulation and adoption of a GEMM that reflects the institution's circumstances, in collaboration with institutional leadership and key stakeholders, should be among the first duties of the GERO. This will require substantial investment and institutional capital but will create long-term value.

1. What is Global Engagement Maturity Modeling?

The GEMM provides a formal method for assessing the policies and processes in an institution's GERAMP and ensuring that they are effective, replicable, and continuously improved. Information technology provides one path for successfully automating and integrating those elements into the institution's overall operational infrastructure. Institutions adopt a GEMM with a graduated set of risk assessment and management levels defined by progressively more demanding ("mature") requirements (Fig. 3).

The GEMM is a variant of the capability maturity models (CMM) used extensively in the private sector, particularly in the software industry. Both the Department of Homeland Security and the National

Global Engagement Maturity Model

The Research Security Capabilities Maturity Model provides an objective methodology for assessing an organization's overall security program maturity.

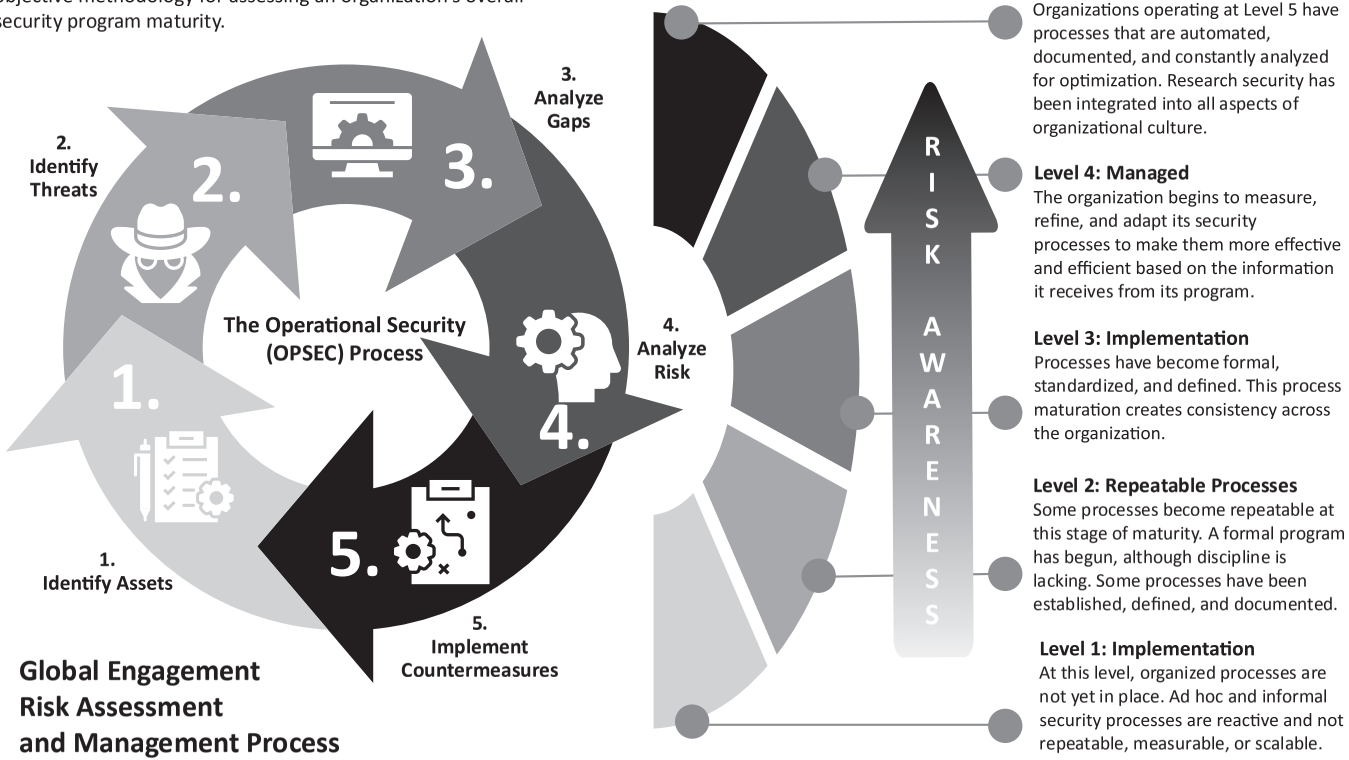


Figure 3. Global Engagement Maturity Model.

Institutes of Standards and Technology offer guidance on building and integrating CMMs.[22]

Adopting a GEMM offers several benefits. First, it promotes a shared vocabulary and conceptual understanding of foreign engagement risk assessment and management. Second, it lays out a roadmap with clear benchmarks for performance and improvement. Third, it helps an institution to identify and remediate vulnerabilities and areas that are reactive to security threats in order to achieve a stronger, proactive posture. Finally, a GEMM would communicate to funding agencies a grant-receiving institution's level of preparedness and the corresponding types of work that it can perform effectively and securely.

2. What does a Global Engagement Maturity Model look like?

A GEMM comprises five distinct maturity levels, each defined by a corresponding set of key process areas that, when implemented together, satisfy the goals defined for that level. As an institution advances from one maturity level to the next, its GERAMP will move from unorganized and unstructured to disciplined, structured, and continuously optimized. Policies supply the overarching guidance for the program and will evolve to support its maturing structure. Processes are the step-by-step methods that fulfill policy requirements and contribute to the program's success. They will evolve as the program achieves higher degrees of optimization.

Level 1: Initial Policies

Institutions enter this level with no standardized processes in place. They are ad hoc, informal, reactive and not repeatable, measurable, or scalable. This level of maturity is characterized by the following:

22. Department of Homeland Security, *Cybersecurity Capability Maturity Model White Paper*, May 2014, https://niccs.us-cert.gov/sites/default/files/Capability%20Maturity%20Model%20White%20Paper.pdf?trackDocs=Capability%20Maturity%20Model%20White%20Paper.pdf; National Institute for Standards and Technology, Information Technology Laboratory Computer Resource Security Center, June 22, 2020, https://csrc.nist.gov/Projects/Program-Review-for-Information-Security-Assistance/Security-Maturity-Levels.

- Formal, up-to-date, documented policies that are readily available to employees and expressed as "shall" or "will" statements.
- Policies that establish a continuing cycle of risk assessment and implementation and employ monitoring for effectiveness and compliance.
- Policies covering specific assets or all major facilities and operations institution-wide.
- Policies that have been approved by key stakeholders.
- Policies that delineate the structure of the GERAMP, clearly assign GERO responsibilities, and lay the foundation necessary to reliably measure progress and compliance.
- Policies that identify specific penalties and disciplinary actions for non-compliance.

Institutions at Level 1 of the GEMM should focus on developing basic policies necessary to establish repeatable processes in preparation for advancement to GEMM Level 2.

Level 2: Repeatable Processes

At this level, a formal program has been initiated but discipline is lacking. Some processes have been established, defined, and documented and are repeatable. This level of maturity is characterized by the following:

- Formal, up-to-date, documented processes to implement the security controls identified in Level 1 policies.
- Processes to clarify where, how, when, and on what a control is to be applied and who is to apply it.
- Processes that document the implementation of and the rigor with which a control is to be applied.
- Processes that clearly define research security responsibilities and expected behaviors for: a) institutional leadership and administration; b) employees and affiliates (e.g., faculty, staff, and students); c) security administrators (e.g., IT, research security); d) processes that list appropriate individuals as points of contact for further information, guidance, reporting, and compliance.

Institutions at Level 2 of the GEMM should focus on developing standard processes through greater attention to documentation, standardization, and integration in preparation for advancement to GEMM Level 3.

Level 3: Implementation

At this level, processes are formalized, standardized, and defined. This promotes consistency across the institution. At this level of maturity:

- Processes are communicated to the individuals who must comply with them.
- Research security processes and controls are implemented in a consistent manner everywhere that they apply and are reinforced through training.
- Ad hoc, individual, or case-by-case approaches are discouraged.
- Policies are approved by key affected parties.
- Initial testing is performed to ensure controls are operating as intended.

Institutions at Level 3 of the GEMM should begin to focus on monitoring and controlling processes through data collection and analysis in preparation for advancement to GEMM Level 4.

Level 4: Managed

At this level, the institution begins to measure, refine, and adapt their GERAMP processes to make them more effective and efficient based on feedback generated by their program. At this level of maturity:

- Tests (including self-assessments performed by staff, contractors, or other designated parties) are conducted routinely to ensure that all policies, processes, and controls are performing as intended and that they meet the appropriate level of the GEMM.
- Information gleaned from records of potential and actual foreign interference and other related security incidents and from alerts, such as those issued by IT security administrators, qualify as test results. This information can identify specific vulnerabilities and provide insights into threats and risks.

- Independent audits, such as those arranged by funding agency Inspectors General, provide valuable feedback about an institution's performance but are not substitutes for routine and rigorous internal testing.
- Prompt and effective remediation is taken to address identified vulnerabilities.
- Evaluation requirements, including requirements regarding the type and frequency of testing, are documented, approved, and effectively implemented.
- The frequency and rigor with which individual processes and controls are tested depend on the risks posed by them not operating effectively.

Institutions at Level 4 of the GEMM should begin to focus on constant optimization by monitoring feedback from current processes and by innovating to better meet specific needs in preparation for advancement to GEMM Level 5.

Level 5: Integration

At this level, an institution's processes are automated, documented, and constantly analyzed for optimization. Risk assessment and management are part of the overall culture. However, reaching this level does not mean that the institution's maturity has peaked. It means that it is monitoring, testing, and adapting its processes constantly to make them better. At this level of maturity:

- There is an active and effective institution-wide GERAMP.
- The GERAMP comprises consolidated practices that are integral to the institution's culture.
- Implementation of the GERAMP is second nature.
- Policies, processes, implementations, and tests are continually reviewed and optimized.
- Decision making is based on risk and mission impact.
- Security vulnerabilities are studied and managed.
- Evidence-based re-evaluations of threats are continually conducted and controls are adapted to evolving research security environments.

- Additional research security measures and opportunities for innovation are identified as needed.
- Costs and benefits of research security are measured as precisely as practicable.
- Status metrics for the GERO are established and met.

E. A New US Government-Sponsored Entity

US research institutions have a long way to go before they regain the initiative in their management of foreign engagement risk, and they cannot do it alone.[23] Government support is essential but currently scoped too narrowly to assist with the classes of the threat that this report explores. The open and collaborative nature of the US research enterprise creates an exceptionally soft target space that in many instances makes recourse to clandestine foreign operations such as espionage unnecessary. In the lightly policed realms of fundamental and applied research, a universe of risk flourishes within the bounds of the law and therefore outside of the counterintelligence and law enforcement frames of reference conventionally used by the government.

In principle, the public nature of this risk should make it easier to recognize and abate. But in practice, foreign adversaries prey on the credulity and incapacity of their hosts. They obfuscate their identities; mask references to defense-related partnerships and research projects by using alternative, innocuous or vague English-language translations or by omitting them altogether from their English-language materials; and employ other means of concealment.[24] US research institutions generally lack the internal capabilities to detect and penetrate those

23. White House Office of Science and Technology Policy, *Enhancing the Security and Integrity of America's Research Enterprise*, June 2020, https://www.whitehouse.gov/wp-content/uploads/2017/12/Enhancing-the-Security-and-Integrity-of-Americas-Research-Enterprise-June-2020.pdf.
24. Robert Delaney, "US Ties Activities of Arrested Chinese Military Officer to Those by Defendant in Boston Case," *South China Morning Post*, June 25, 2020, https://www.scmp.com/news/china/military/article/3090497/us-ties-activities-arrested-chinese-military-officer-those?utm_source=copy_link&utm_medium=share_widget&utm_campaign=3090497.

cloaks although they may hide in plain sight. As the journalist and author John Pomfret has observed with respect to the PRC, "The Chinese language is the first layer of encryption."[25] Analogous claims could be made of other critical languages, such as Farsi and Arabic.

To overcome these impediments, we recommend the constitution of a government-sponsored entity devoted to research and analysis of foreign engagement risk in the US research enterprise. The structure and legal authority such an entity would operate under, especially as it relates to privacy law, are to be defined by the executive and legislative branches. Nevertheless, we suggest an interagency or hybrid form. The entity's mission will necessarily intersect with the portfolios of education, defense, intelligence, law enforcement, and research funding agencies but must transcend their individual perspectives, integrate their information streams, and provide an urgently needed, unified point of contact for the research enterprise.

The entity would interface directly with our proposed GEROs and regional vetting centers to establish mutually beneficial relationships of trust, promote proactive postures of integrity and security, and empower research institutions to exercise their discretion with greater wisdom. While the entity could supply classified information as needed to vetting personnel who have the appropriate clearances, by working predominantly in an open-source environment, it would facilitate information sharing and foster more collaborative dynamics between government and the research community than current counterintelligence and law enforcement-driven initiatives support. More specifically, the entity would:

- Establish a central office with regional satellites across the United States funded and administered by the government and staffed by area specialists, linguists, and officials experienced in identifying

25. John Pomfret, "What America Didn't Anticipate About China," *The Atlantic*, October 16, 2019, https://www.theatlantic.com/ideas/archive/2019/10/chinas-cultural-power/600049.

and mitigating foreign engagement risks to US research, especially with respect to technology transfer and the PRC.

- Fill protection gaps by focusing on entities and activities earlier in the R&D and technology lifecycles, which generally fall outside of regulatory oversight.
- Provide compliance and vetting support to federal agencies that fund the research enterprise and establish mechanisms for periodic monitoring to ensure continued compliance with federal grant and contracting requirements.
- Serve as a principal point of contact and conduit for GEROs and regional vetting centers to exchange information and obtain strategic threat assessments, tactical due diligence, and vetting support.
- Combine the research and analytic capabilities of the US government, think tanks, and academia to publish studies, assessments, and policy recommendations for clients in the research enterprise and government.
- Review open-source publications in key linguistic and geographic spaces to identify high-risk foreign engagements, especially those related to military R&D or emerging civilian technologies with potential dual-use or high-value commercial applications.
- Serve as an authoritative source to advise research institutions on emerging technologies important to national security.
- Collect and analyze information on all identifiable state-sponsored talent recruitment programs to determine the extent of their activity in the United States.
- Build databases derived from publicly available information on: entities that support the defense research and industrial base of strategic competitors, entities that are tied to foreign state-directed technology transfer missions and covert influence operations in the United States, and entities that support the surveillance and security apparatuses of states that engage in systematic human rights abuses. These databases could be designated controlled unclassified information.
- Create a model for other nations, help them to develop similar capabilities, and assemble coalitions.

Figure 4. Thinking about Global Engagement.

V. Conclusion

The excellence of the US research enterprise is inseparable from its commitments to openness and academic independence, its institutional autonomy, and its discretion to operate in a globalized world. However, in a climate of sharpening strategic competition, these qualities also engender vulnerabilities that are increasingly prejudicial to national and economic security.

Evidence points to serious structural and conceptual flaws in the ways that research institutions and government each approach foreign engagement risk. Although incremental reforms may eke out better performance, the current system is decentralized and permissive by design and was never equipped to coherently navigate among the countless shades of gray that now beset it. Asked to fight a battle that it cannot win, its insufficiencies are corroding trust and exhausting patience among policymakers. The danger is that the remedies they ultimately devise may leave the research enterprise and the nation weaker and more isolated.

This chapter offers a way out of that breakdown (Fig. 4). It asks the research community and government to reinvent their approaches to foreign engagement risk so that they can meet one another in the middle, each bringing to the table what it does best. *First*, a research institution's GERAMP creates a strategic framework for rigorously assessing risk and mitigating it through proportionate governance. *Second*, its GERO operationalizes that framework, providing unified administrative leadership, oversight, and coordination across the institution. The GERO liaises with government directly and through joint regional vetting centers. *Third*, OPSEC primes institutions to use the GERO to reclaim the initiative by shifting from compliance-driven formalism to a proactive, adaptive posture. *Fourth*, the GEMM provides a structured methodology for continuous improvement. And *fifth*, a government-sponsored entity contributes its unique research and analytic capabilities to this apparatus and supplies a unified point of contact on foreign engagement risk.

The goals? To empower research institutions and scholars to pursue foreign engagements with the confidence that they can make better and

more granular decisions, to acknowledge and honestly grapple with the potential tensions between those engagements and national interests, and to deepen mutual respect and collaboration between the research enterprise and the government. All of this will admittedly require new investment, but much can be achieved by resolutely changing the paradigm to align and harness existing assets more effectively. It is imperative that we pull out of the trajectory that we are now on; the stakes are too high not to.

CONTRIBUTORS

Larry Diamond is a senior fellow at the Hoover Institution and at the Freeman Spogli Institute for International Studies (FSI) at Stanford University. He also chairs the Hoover Institution Project on Taiwan in the Indo-Pacific Region and has co-edited three books on democracy in Taiwan, including the forthcoming *Dynamics of Democracy in Taiwan: The Ma Ying-jeou Years*. He co-leads the Global Digital Policy Incubator, part of Stanford's Cyber Policy Center, and previously directed FSI's Center on Democracy, Development, and the Rule of Law. During 2017–18, he co-chaired, with Orville Schell, a Hoover Institution–Asia Society working group, which produced the report *China's Influence and American Interests: Promoting Constructive Vigilance* (published by the Hoover Institution Press in 2019). He is the founding co-editor of the *Journal of Democracy* and also serves as senior consultant at the International Forum for Democratic Studies of the National Endowment for Democracy.

Kevin Gamache is chief research security officer for the Texas A&M University System. He is responsible for ensuring A&M System member universities are compliant with US government requirements for protecting sensitive federal information. He established and leads the Academic Security and Counter Exploitation (ASCE) program, an association of US universities established to help heighten security awareness in academia. His leadership on behalf of the academic

security community resulted in the A&M System receiving the James S. Cogswell Award from the Defense Security Service in 2015. In 2017 and 2019, the A&M System received the Defense Counterintelligence and Security Agency's Award for Excellence in Counterintelligence. He received a PhD from Texas A&M University and a master of science degree from the Industrial College of the Armed Forces. He retired from the United States Air Force in 2005 with the rank of colonel after twenty-four years of service.

H. R. McMaster is the Fouad and Michelle Ajami Senior Fellow at the Hoover Institution, Stanford University. He is also the Bernard and Susan Liautaud Fellow at the Freeman Spogli Institute and a lecturer at Stanford University's Graduate School of Business. He serves as the Japan Chair at the Hudson Institute and chairman of the Center for Political and Military Power at the Foundation for Defense of Democracy. He was the twenty-sixth assistant to the president for National Security Affairs. McMaster served as a commissioned officer in the US Army for thirty-four years after graduating from West Point. He holds a PhD in military history from the University of North Carolina at Chapel Hill. He is author of *Battlegrounds: The Fight to Defend the Free World* and *Dereliction of Duty: Lyndon Johnson, Robert McNamara, the Joint Chiefs of Staff and the Lies that Led to Vietnam*.

Jeffrey Stoff is a Chinese linguist and analyst working in the Department of Defense (DoD) specializing in technology transfer and critical technology protection issues. He has worked closely with federal agencies on national and economic security issues and supports interagency outreach efforts to the public and private sectors. Over his seventeen-year career in the US government, Stoff has advised the National Security Council; the Office of Director of National Intelligence (ODNI); DoD senior leaders and policy and intelligence components; the FBI; the departments of State, Commerce, Energy, and Agriculture; the National Science Foundation; and the National Institutes of Health. Stoff received ODNI awards in 2018 and 2019, including the National Counterintelligence and Security Center Director's Award for Excel-

lence. Stoff earned a master's degree in Pacific international affairs at the University of California, San Diego.

Glenn Tiffert is a historian of modern China and a research fellow at the Hoover Institution, where he manages its projects on China's Global Sharp Power, and on Taiwan in the Indo-Pacific Region. He works closely with academic and government partners to document and build resilience against authoritarian interference with democratic institutions, and serves on the executive committee of the Academic Security and Counter Exploitation (ASCE) program, an association of US universities established to help heighten security awareness in academia. Most recently, Tiffert was a contributor to the Hoover–Asia Society report *China's Influence and American Interests: Promoting Constructive Vigilance* (published by the Hoover Institution Press in 2019) and is the author of the 2020 National Endowment of Democracy report *Compromising the Knowledge Economy: Authoritarian Challenges to Independent Intellectual Inquiry*. Tiffert earned his PhD from the University of California–Berkeley. He is a specialist in Chinese legal and political history, and has pioneered the application of machine learning and natural language processing to their study.

INDEX