S. HRG. 118–404

THE DEPARTMENT OF ENERGY'S LEAD ROLE IN CONDUCTING ADVANCED COMPUTING RESEARCH, APPLICATION, AND SECURITY

HEARING

BEFORE THE

COMMITTEE ON ENERGY AND NATURAL RESOURCES UNITED STATES SENATE

ONE HUNDRED EIGHTEENTH CONGRESS

SECOND SESSION

SEPTEMBER 12, 2024

Printed for the use of the
Committee on Energy and Natural Resources

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
56–727 WASHINGTON : 2025

COMMITTEE ON ENERGY AND NATURAL RESOURCES

JOE MANCHIN III, West Virginia, *Chairman*

RON WYDEN, Oregon
MARIA CANTWELL, Washington
BERNARD SANDERS, Vermont
MARTIN HEINRICH, New Mexico
MAZIE K. HIRONO, Hawaii
ANGUS S. KING, JR., Maine
CATHERINE CORTEZ MASTO, Nevada
JOHN W. HICKENLOOPER, Colorado
ALEX PADILLA, California

JOHN BARRASSO, Wyoming
JAMES E. RISCH, Idaho
MIKE LEE, Utah
STEVE DAINES, Montana
LISA MURKOWSKI, Alaska
JOHN HOEVEN, North Dakota
BILL CASSIDY, Louisiana
CINDY HYDE-SMITH, Mississippi
JOSH HAWLEY, Missouri

RENAE BLACK, *Staff Director*
SAM E. FOWLER, *Chief Counsel*
SARAH KESSEL, *Professional Staff Member*
ALYSE HUFFMAN, *Professional Staff Member*
JUSTIN J. MEMMOTT, *Republican Staff Director*
PATRICK J. MCCORMICK III, *Republican Chief Counsel*
DEREK FISHER, *Republican Professional Staff Member*
CHAD THORLEY, *Republican Director of Oversight*

CONTENTS

OPENING STATEMENTS

WITNESSES

ALPHABETICAL LISTING AND APPENDIX MATERIAL SUBMITTED

THE DEPARTMENT OF ENERGY'S LEAD ROLE IN CONDUCTING ADVANCED COMPUTING RESEARCH, APPLICATION, AND SECURITY

THURSDAY, SEPTEMBER, 12, 2024

U.S. SENATE,
COMMITTEE ON ENERGY AND NATURAL RESOURCES,
Washington, DC.

The Committee met, pursuant to notice, at 10:00 a.m. in Room SD–366, Dirksen Senate Office Building, Hon. Joe Manchin III, Chairman of the Committee, presiding.

OPENING STATEMENT OF HON. JOE MANCHIN III, U.S. SENATOR FROM WEST VIRGINIA

The CHAIRMAN. The Committee will come to order.

First of all, we would like to welcome our friend and colleague, Senator Durbin, for being here in our Committee and we appreciate very much having you.

Before we begin, I want to acknowledge the terrible loss of former Director of Los Alamos National Laboratory, Charles McMillan, who died in a car accident last week. He was going to be here to testify for us today and we are very sorry for his family and we express our deepest condolences. Charlie was a true patriot to this country who made extraordinary contributions to our nuclear weapons programs and other critical scientific missions at our national labs for over 40 years.

This morning we are here to discuss where we are and where we are going in the field of advanced computing, which touches on a wide range of technologies and applications across every one of our lives. We will also discuss legislation our members have introduced in three specific areas: artificial intelligence, quantum computing, and cybersecurity. Computing technology is advancing rapidly across the globe, and America must proceed with both ambition and caution, particularly when it comes to our national security and public safety. The DOE has a long legacy in computational science, dating back to the Manhattan Project in the 1940s, which relied on computational modeling.

Today, the labs currently operate the fastest two supercomputers in the entire world. The opportunities that high-performance computing provides are endless. In my State of West Virginia, it was recently announced that a new supercomputer, the Rhea, will be installed in the city of Fairmont to improve drought, flood, and wildfire predictions and forecasting. Like during the Manhattan Project, we are now engaged in a new kind of technological race,

one that requires us to innovate with similar urgencies and vigilance. We are watching our adversaries ramp up their investments in advanced computing technologies and even deploy them in battlefields across the world.

The chart behind me, and I am going to keep this chart up too, but I want to explain this chart.

[The chart referred to follows:]

Technology	Countries Ranked by Their Share (%) of Quality Research Papers Study funded by U.S. Department of State		
Artificial Intelligence	 China **37%**	 United States **13%**	 Great Britain **4%**
Advanced Data Analytics	 China **31%**	 United States **15%**	 India **6%**
Quantum Computing	 United States **34%**	 China **15%**	 Great Britain **6%**
Machine Learning	 China **33%**	 United States **18%**	 India **5%**
Cybersecurity Technologies	 China **23%**	 United States **17%**	 India **8%**
High Performance Computing	 United States **29%**	 China **26%**	 South Korea **6%**
Quantum Communications	 China **31%**	 United States **17%**	 Great Britain **8%**

The CHAIRMAN It is really amazing. This is not in dollars and cents, so forget about the amount of money, because we don't really have that. What we can tell you is, it has been scientifically proven that this is the authentic things that they have done, and we know that China, in artificial intelligence, has 37 percent more capabilities and authenticity on what they have been able to report than what we do, at 13. It shows you how far we are behind. Advanced analytics—31 percent for China, 15 percent U.S. Quantum computing—we are still ahead 34 to 15. Machine learning—China. Cybersecurity technology—China. High-performance computing—we are still ahead, barely, but we are there. And then when it comes down to quantum communications, it shows you the difference.

This is where we are, and we know this has been proven and this is where they are at as far as their capacity and authenticity of what they are doing. Would you all agree on that? Okay. So we will keep that one up. Put that chart up over there.

We are using published research paper data in place of spending because the U.S. Government does not trust how China is reporting their expenditures. As the chart showed, America is at real risk of falling behind to China in this race, and it is becoming increasingly apparent that whoever leads in the development of these technologies will secure the unequivocal lead in scientific and technology innovation writ large. For the United States to maintain our position as a global leader, we must accelerate our efforts. The stakes are nothing short of economic prosperity and national security. Our national laboratories have spent decades building a workforce and infrastructure to answer the challenging questions about how to safely deploy these emerging technologies in a way that sets an example for the rest of the world.

While we are proud that our private sector is making incredible strides developing and deploying advanced computing, this does not replace the need for government research and development. Complex societal challenges, like advanced manufacturing, nuclear security, and genomics are a few areas of application where there is not yet an established commercial market. And this is why Senator Murkowski and I have introduced bipartisan legislation to reinforce the artificial intelligence research and development programs at our DOE labs. The bill authorizes the Frontiers in Artificial Intelligence for Science, Security and Technology, or the FASST Act, as an initiative at the Department of Energy which will give the United States the tools to deliver secure and dependable AI solutions.

This bill would create AI research and innovation hubs at our labs that will harness testbeds for the development of AI platforms, develop foundational models for various applications for energy and national security, verify the safety of new large language models, and establish a risk evaluation program to respond to security risks. It is just common sense to use our nation's brain trust at our national labs and their state-of-the-art facilities that we have already built and maintain to safely advance AI while safeguarding taxpayer dollars.

Industry and the science community alike have publicly supported our bill. I would like to submit, for the record, the supportive statement of Hewlett Packard Enterprise, AMD, Intel,

ARM, Micron, and the Energy Sciences Coalition. Without objection, so be it.

[Letter of support for the FASST ACT follows:]

September 11, 2024

The Honorable Joe Manchin
Chairman
Senate Committee on Energy and Natural Resources
306 Hart Senate Office Building
Washington, D.C. 20510

The Honorable John Barrasso
Ranking Member
Senate Committee on Energy and Natural Resources
307 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Chairman Manchin and Ranking Member Barrasso:

As producers of the hardware that powers advances in artificial intelligence, we write in advance of the Senate Committee on Energy and Natural Resources' upcoming September 12 hearing to examine the Department of Energy's (DOE) role in advanced computing research. As you prepare to discuss the role of advanced computing and artificial intelligence (AI) in maintaining the United States' global leadership, we want to express our support for the bipartisan DOE AI Act, introduced by Chairman Manchin and Senator Murkowski earlier this year. This critical legislation is a timely and necessary step to position the U.S. at the forefront of AI innovation, leveraging the DOE's national laboratories and infrastructure to support national and economic security in the United States.

The DOE AI Act's authorization of the Frontiers in Artificial Intelligence for Science, Security, and Technology (FASST) initiative is a landmark move that will enhance the development of AI-driven solutions for national security, scientific discovery, and technological innovation. This initiative will establish AI research clusters, develop next-generation AI computing platforms, and manage vast AI training datasets—supporting our national security and enabling the U.S. to lead in areas such as fusion energy, and cancer-fighting treatments.

Federal AI needs, critically, cannot be met by commercially available AI systems, as the foundational models to tackle federal problems often will require training using both public and government data. What's more, such applications may require the specific training of systems for discreet and necessary governmental applications. While the power of publicly available commercial AI systems is apparent, these systems are not designed or fit to take on the grand challenges pursued by scientists and public officials in the United States. The public-private partnerships contemplated by the DOE AI Act, however, can leverage the comparative advantages of both sectors to tackle these challenges. What's more, the DOE has a history of succeeding in fostering such public-private partnerships as it has done through prior programs, including the Exascale Initiative, which has produced the world's fastest supercomputer.

When funded, the investments authorized by this Act will be critical in advancing U.S. capabilities in AI, just as with the systems produced by other computing initiatives at the DOE's National Laboratories the entire federal government will be positioned to use this technology to advance missions across federal agencies. It also addresses the pressing need to train and develop the next generation of AI talent by integrating comprehensive STEM education and workforce development programs. In doing so, this legislation will ensure the U.S. remains a leader in AI research, development, and deployment for the long term.

The need for this federal investment is underscored by the publicly reported and substantial commitments made by other nations:

- China invested close to $10 billion in public AI R&D in 2018 and is projected to spend over $26 billion annually on AI by 2026, far exceeding many nations' current investments in AI.
- The European Union has committed €4 billion through 2027 to develop AI infrastructure and create "AI Factories" and "Common European Data Spaces."
- South Korea plans to invest $6.94 billion in AI by 2027 as part of its national strategy to strengthen AI capabilities.
- India recently launched the $1.25 billion IndiaAI Mission to further its AI development.
- Canada has allocated $1.7 billion for AI in its 2024 budget to expand its AI industry.
- The United Kingdom previously committed $1.72 billion to AI development, with its future strategy awaiting updates as the new administration finalizes its AI budget.

These global investments illustrate the rapidly advancing international AI landscape, reinforcing the urgency of passing the DOE AI Act to ensure the U.S. maintains its competitive edge.

We applaud your leadership in introducing this vital legislation, which will fortify America's position as a global leader in artificial intelligence. The DOE AI Act stands to deliver significant benefits for U.S. national security, economic growth, and scientific innovation. We look forward to the hearing and offer our support as the Committee works to advance this important initiative.

Sincerely,

AMD

Arm

Hewlett Packard Enterprise

Intel Corporation

Micron Technology

The CHAIRMAN. Let me also reiterate that America will need more energy to meet the growing demand from data centers and the manufacturing resurgence that has resulted from the Bipartisan Infrastructure Law, CHIPS and Science Act, and Inflation Reduction Act. For decades, power demand has been decreasing, but now we are expecting a rapid turnaround this decade. But while demand is increasing, we have 2.6 million megawatts of generation waiting an average of five years to connect to the grid, and we are also retiring baseload and dispatchable generation faster than we can replace it. This is unacceptable. If America can't build the energy infrastructure needed to support high-tech industries, companies will choose to take their business elsewhere. We simply must get common-sense policy like our bipartisan energy permitting bill enacted or we will have squandered this opportunity and really put ourselves at risk.

Today, we will be discussing quantum computing, which processes information much more quickly and efficiently than even our fastest supercomputers do today. Senator Durbin and Senator Daines recently introduced bipartisan legislation to reauthorize many quantum programs throughout the Department of Energy, and Senator Durbin is going to be joining us to speak briefly about his bill.

We can't discuss this new era of emerging technology development without considering cybersecurity and broader national security implications. These technologies can serve as assets, but also as threats to the cybersecurity posture of the United States. We have seen the devastating effects of a cyberattack on our critical infrastructure, like the Colonial Pipeline attack in 2021 that forced the shutdown of the country's most important fuel pipeline.

Last year, I joined Senator Risch in introducing the ETAC Establishment Act, which establishes the Energy Threat Analysis Center at DOE. ETAC will serve as the energy sector centralized hub in the Federal Government for cyber information, sharing threat response to better defend the U.S. energy sector against cyber threats. We must also pay attention to how we are protecting our scientific program from nefarious actors. We will not outcompete China if they are able to just steal the technology funded by our taxpayer dollars. The CHIPS and Science Act authorized improvements to our research security policies that are already being implemented by the Department. But as the threat environment becomes more complex and stakes become higher, much more must be done. During the past several months, Senator Barrasso and I have been working with our colleagues on the Intelligence Committee to strengthen our research security policies to secure the science performed in our national labs while not stifling their work or closing ourselves off to the global scientific community.

I am confident this is something we can get done in this year's National Defense Authorization Act. We have a lot to cover this morning. I am looking forward to hearing our witnesses' perspectives on specific steps we can take to ensure America is advancing all these technologies in a competitive and a responsible manner. I know we certainly do not need to start from scratch to achieve this. Instead of duplication, we can invest smartly in emerging technologies in a cost-effective way by building upon the resources

that we already have at the DOE and its national labs. This is how we will maintain our global lead in scientific innovation.

And with that, I am going to turn to my colleague and friend, Senator Barrasso, for his opening remarks.

OPENING STATEMENT OF HON. JOHN BARRASSO, U.S. SENATOR FROM WYOMING

Senator BARRASSO. Well said, Mr. Chairman. Thank you for holding today's very important hearing.

Research into advanced computing is critical—critical to maintaining America's economic growth, our national security, and our leadership in the world. The Department of Energy, through its network of 17 national labs, plays a very key role in all of those innovations. The Department has some of the most advanced computing systems in the world. In fact, the Department has the world's two fastest supercomputers and a third supercomputer among the world's top ten. These systems have pioneered advances in artificial intelligence and in quantum computing. These are two fields that the People's Republic of China does seek to dominate. For this reason, China is watching nearly every move that our national labs make. Our labs are under constant surveillance by a branch of China's intelligence network that focuses on science and technology. This branch alone consists of about 100,000 agents. Beginning under Chairman Mao, this intelligence network has supported the development of China's nuclear weapons and its missile and satellite programs. And its mission remains the same today—target foreign technologies useful to the Chinese communist regime and acquire them by any means possible.

America's open research environment is the envy of the world. It has fostered our greatest scientific achievements, yet it is a rich target for China and other adversaries. As stated by the National Academy of Sciences, "The integrity of research is based on the values of objectivity, honesty, openness, fairness, accountability, and stewardship." Contrast this with the view of China's President, Xi Jinping. He recently described science and technology development as a contest to be won. He stated, "The initiatives of innovation and development must be secretly kept in our own hands, and whoever holds the key to innovation makes an offensive move," he said, "in this chess game, and will be able to take the lead and win the advantage."

A 2022 report, titled "Los Alamos Club," by Strider Technologies, is telling. I have a copy of the report here, Mr. Chairman.

[The report referred to follows:]

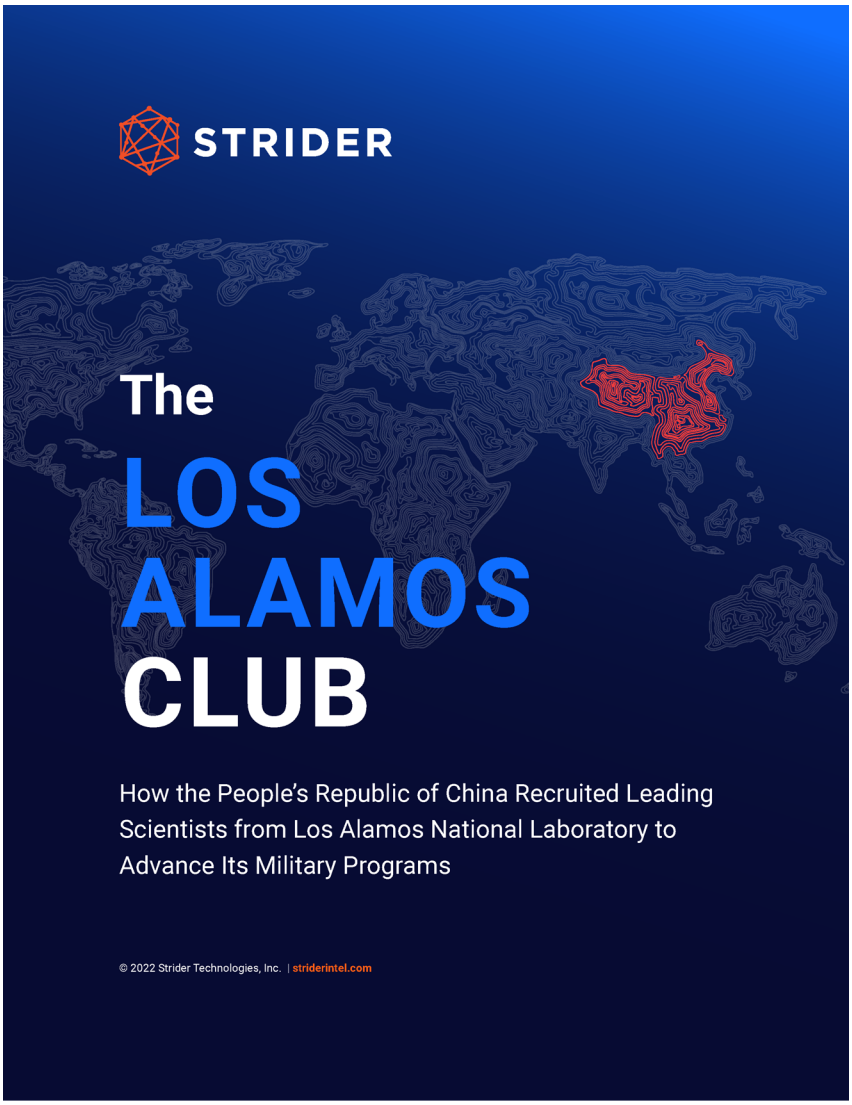

STRIDER
The
LOS
ALAMOS
CLUB
How the People's Republic of China Recruited Leading Scientists from Los Alamos National Laboratory to Advance Its Military Programs
© 2022 Strider Technologies, Inc. | striderintel.com

Table of Contents

Foreword

The inspiration for this report comes from a March 2017 article in the *South China Morning Post* titled "America's Hidden Role in Chinese Weapons Research." The article notes that so many former Los Alamos National Laboratory scientists have returned to the People's Republic of China (PRC) and are now working on military research programs that they are referred to as the "Los Alamos Club." However, no specifics about this "Club," its membership, or the programs these scientists are working on were reported.

The objective in conducting this study is to contextualize and document the ongoing efforts of the PRC government to send promising scientists to U.S. national laboratories for training while also recruiting leading scientists back to the PRC to advance its own military programs. Former Los Alamos scientists have made, and continue to make, considerable contributions to the PRC hypersonic, missile, and submarine programs that present an array of security risks for the United States and the entire free world. Better protection is needed for the institutions, research programs, and scientists advancing innovation in this era of strategic competition without harming open scientific collaboration.

This report does not suggest any illegal activities were conducted by any individual, university, professor, laboratory, or research institute named. Additionally, we do not argue that Los Alamos National Laboratory bears responsibility for, or was complicit in, the PRC's recruitment of former Los Alamos affiliates.

Executive Summary

The People's Republic of China (PRC) is employing a Talent Superpower Strategy designed to incentivize academics, researchers, and scientists to go abroad, deepen their expertise, and return to China to advance its strategic interests.

What began in the 1980s as a program to send young talent overseas has evolved to incorporate initiatives that seek to harness these individuals' efforts for China's gain and, ultimately, encourage them to return to the PRC to work in key technology sectors.

The extent to which these initiatives are active in U.S. government laboratories is unknown. However, China's recruitment of individuals who have worked at the Los Alamos National Laboratory in New Mexico reflects the ambitions of the PRC's talent strategy and its exploitation of Western commitments to global scientific collaboration. The PRC's success among former Los Alamos affiliates, along with support for China's talent programs from Chinese Communist Party (CCP) General Secretary Xi Jinping and other top CCP leaders, suggest that similar recruitment efforts may be widespread among U.S. government–funded laboratories, academic research institutions, and major centers of innovation. Moreover, the Los Alamos case shows how China's rapid advances in certain key military technologies are being aided by individuals who participated in sensitive U.S. government–funded research.

Between 1987 and 2021, at least 162 scientists who had worked at Los Alamos returned to the PRC to support a variety of domestic research and development (R&D) programs. Fifteen of those scientists worked as permanent staff members at Los Alamos. Of those fifteen, thirteen were recruited into PRC government talent programs; some were responsible for sponsoring visiting scholars and postdoctoral researchers from the PRC, and some received U.S. government funding for sensitive research. At least one of these staff members held a U.S. Department of Energy (DOE) "Q Clearance" allowing access to Top Secret Restricted Data and National Security Information.

Of the 162 returnees, at least 59 scientists were selectees of the PRC's flagship talent recruitment program—the Thousand Talents Program (TTP) and its youth branch, the Youth Thousand Talents Program (YTTP).

Ninety-eight of the scientists who returned were postdoctoral researchers, and 49 were visiting scholars. Although such individuals do not have access to the most sensitive research at Los Alamos, they still pose a risk of technology transfer and economic espionage. The DOE has acknowledged instances in which researchers elsewhere have passed dual-use and export-controlled research to the PRC via visiting students and scholars.

Since returning to China, Los Alamos alumni have helped the PRC advance key military and dual-use technologies in areas such as hypersonics, deep-earth penetrating warheads, unmanned autonomous vehicles (UAV), jet engines, and submarine noise reduction. A key member of this "Los Alamos Club" is Dr. Chen Shiyi, a world-renowned expert in fluid dynamics and turbulence who spent the 1990s at the lab. After returning to China, Chen served as president of Southern University of Science and Technology (SUSTech), where he excelled at recruiting scientists with links to Los Alamos.

One of Chen Shiyi's first hires at SUSTech was former Los Alamos scientist Zhao Yusheng. During his 18-year career at Los Alamos, Zhao received at least 28 grants totaling $19.8 million in U.S. government funding, including for sensitive research on deep-earth penetrating warheads. While at Los Alamos, Zhao sponsored a postdoctoral researcher who filed a national defense patent on similar technology after returning to the PRC. The researcher is now affiliated with the Chinese Academy of Engineering Physics (CAEP), the PRC's premier nuclear weapons R&D and production facility.

In addition to his role as a talent recruiter, Chen Shiyi has made major contributions to China's hypersonics and aerodynamics programs. Chen served as director of a state laboratory that played a key role in developing the PRC's hypersonic glide vehicle. Under Chen's leadership, the laboratory undertook projects with military organizations, defense industry enterprises, and PRC universities that collaborate closely with the People's Liberation Army (PLA). These projects have helped to contribute to the PRC passing the United States in hypersonic R&D.

He Guowei, another member of the "Los Alamos Club," has been an important figure in the PRC's efforts to develop quieter submarines that are better able to evade detection. While at Los Alamos in the late 1990s, Dr. He engaged extensively with Chen Shiyi. After he returned to the PRC, Dr. He worked at the Chinese Academy of Sciences' Institute of Mechanics (IMCAS), where his team developed computer models that help to quickly and accurately predict turbulence generated by a submarine.

In recent years, China's state-sponsored talent programs have drawn increased scrutiny from Washington not only because of counterintelligence and intellectual property (IP) theft risks, but also because these programs are leveraging taxpayer-funded research to advance the PRC's economic development and military modernization.

The U.S. government has begun to take steps to mitigate the risks posed by the PRC's Talent Superpower Strategy. However, more can be done by government-funded laboratories, research institutions, and private industry to identify potential counterintelligence and IP theft risks posed by individuals whose talent the PRC is seeking to leverage in its race for scientific and technological dominance. Moreover, it is an urgent national security imperative for like-minded nations to work together to protect their innovation centers and compete with China to attract, retain, and protect leading talent.

GO GLOBAL

Play a "Useful Role" in Serving the Motherland

The PRC's Talent Superpower Strategy & Its Targeting of Los Alamos National Laboratory

The People's Republic of China (PRC) is employing a "Talent Superpower Strategy" (人才强国战略) designed to incentivize academics, researchers, and scientists to go abroad, deepen their expertise, and then work to advance China's strategic interests. What began in the 1980s as policy to encourage young talent to go overseas and enhance their skill set has since evolved to include initiatives and programs that ultimately seek to exploit their efforts in vital technology sectors for China's gain, whether they return to China or stay overseas.

This report documents the ambitions of the PRC's talent strategy and its exploitation of Western commitments to global scientific collaboration. It does not argue that Los Alamos National Laboratory bears responsibility for, or was complicit, in the PRC's recruitment of former Los Alamos affiliates. Yet the PRC's success, along with support for China's talent programs from Chinese Communist Party (CCP) General Secretary Xi Jinping and other top CCP leaders, suggest that similar recruitment efforts may be widespread among U.S. government–funded laboratories, academic research institutions, and major centers of innovation. Moreover, the Los Alamos case shows how China's rapid advances in certain crucial military technologies are being aided by individuals who participated in sensitive U.S. government–funded research.[1]

Building a Global Hub & Spoke Talent Network

How China's Talent Initiatives Leverage Overseas Institutions to Train and Recruit Talent

On June 23, 1978, Deng Xiaoping opened a new chapter in the PRC's drive to acquire foreign technology by declaring "thousands, or even tens of thousands, should be sent abroad rather than only a handful."[2] In 1993, resisting the impulse to turn inward in the wake of the Tiananmen Square Massacre, the CCP Central Committee issued a landmark edict that kept the PRC on the path of economic opening to the outside world.[3] The decision also set the overall policy direction to "support of overseas study, encourage returning to China, freedom to come and go" ("支持留学、鼓励回国、来去自由"的方针),"[4] themes that were reiterated many times in the years that followed.[5] In 2013, General Secretary Xi Jinping updated this formulation by adding a phrase that called on overseas scholars to **"play a useful role"** (发挥作用) in serving China's national strategies. Xi has called on the country to "do everything possible to create the conditions for overseas scholars who return to China to have ample scope to exercise their abilities and for overseas scholars who remain overseas to have a gateway to serve their country."[6]

As the number of overseas academics and researchers grew, the PRC implemented policies that financially incentivized overseas researchers to leverage their host institutions to train talent sent from China. In 2001, the PRC Personnel Department, Ministry of Education, Ministry of Science and Technology, Ministry of Public Security, and Ministry of Finance jointly issued a document titled, "Some Opinions on Encouraging Overseas Scholars to Serve Their Country."[7] The document details "funding support" (经费支持) and "remuneration" (报酬) to "overseas scholars to serve the motherland through various methods while they are studying or working overseas" in order to "fully exploit overseas talent resources."[8] The document specified seven services for which PRC scholars working overseas could be rewarded, including leveraging overseas institutes to help train talent.[9]

THE 7 SERVICES

1. Accept concurrent part-time technical work positions in China.
2. Coordinate research cooperation between overseas and Chinese entities.
3. Conduct research overseas that is commercialized by Chinese entities.
4. Commercialize patents and technology by establishing enterprises in China.
5. Leverage overseas institutes to help Chinese employers train their talent.
6. Introduce foreign technology into Western China.
7. Establish "intermediary organizations" to facilitate the introduction of foreign technology to China and create more methods to serve the country in addition to those listed above.

With a large and growing pool of researchers, academics, and scientists studying overseas, the PRC in the 1990s began to implement programs designed to encourage their return to China. In 1994, the Chinese Academy of Sciences (CAS) initiated the Hundred Talents Program (百人计划), an initiative specifically dedicated to the recruitment of overseas experts. Inspired by the success of the Hundred Talents Program, the PRC Ministry of Education in 1998 created the Changjiang Scholars Award Program (长江学者奖励计划) to recruit overseas talent to work in PRC research institutions. A decade later, the Thousand Talents Program (TTP) launched. Today, the PRC operates a constellation of more than 470 distinct talent programs at the central, provincial, municipal, and even institutional level that are aimed at recruiting top talent, especially overseas talent, for key PRC institutions.[10]

Previous research by Strider has detailed how PRC talent programs and funding schemes support the development of China's quantum research programs by sending scientists to top research labs around the world for training and then recruiting those scientists to return to China.[11] This approach is not limited to the quantum sector. Indeed, state-sponsored study abroad programs (公派) and other components of the CCP's Talent Superpower Strategy provide government financial incentives for scholars to use foreign institutes to help the PRC train talent.[12]

In the case of Los Alamos, at least 10 postdoctoral researchers and visiting scholars were funded by the PRC government's State-Sponsored Overseas Joint Training Doctoral Program (国家公派联合培养博士). Applicants to this program are given preference if their research aligns with specific technology needs outlined in PRC government plans or the personnel needs of state laboratories.[13] Those who are selected are contractually required to return to China.[14]

Under this program, the joint training is coordinated by a doctoral advisor in the PRC and a host supervisor abroad, who is likely aware of an applicant's PRC government backing.[15] At Los Alamos, for example, an online advertisement was posted in 2017 under the name of a permanent staff member for a postdoctoral position at the lab's Center for Integrated Nanotechnologies (CINL). The Chinese-language version of the advertisement specifically sought out participants of the PRC government's State-Sponsored Overseas Joint Training Doctoral Program;[16] the English version of the job posting, however, did not.

NEW MEXICO

Los Alamos National Laboratory

The Los Alamos National Laboratory in New Mexico is the U.S. Department of Energy's premier research institution. Its mission—*"to solve national security challenges through simultaneous excellence"*—includes designing nuclear warheads, ensuring the safety and effectiveness of the U.S. nuclear stockpile, and finding innovative solutions to emerging threats in the cyber, space, and new technology domains.

At Los Alamos, permanent staff members are well positioned to identify, select, and train promising talent who could later return to China. These staff members are responsible for reviewing postdoctoral curriculum vitae (CV) and identifying candidates with skills matching Los Alamos research programs.[17] Over the span of their careers, Los Alamos permanent staff—including those who eventually return to the PRC—often mentor dozens of postdoctoral researchers. For example, Dr. Zhao Yusheng, who served as a member of the permanent staff from 1996 to 2012, supervised and sponsored at least 25 postdoctoral researchers, at least eight of whom were from the PRC and later returned.[18]

Close interactions between PRC universities and the Ministry of State Security suggests that some postdoctoral researchers and visiting scholars are vetted by China's security services before going abroad.[19] While they do not have access to the most sensitive research at Los Alamos, they still pose risks of technology transfer and economic espionage. The Department of Energy (DOE) has acknowledged instances where researchers elsewhere have passed dual-use and export-controlled research to the PRC via visiting students and scholars.[20]

The "Los Alamos Club"

Former Los Alamos Affiliates
Advancing China's Military Modernization

Overseas applicants who are inducted into a PRC talent program are typically contractually obligated (often unbeknownst to their overseas host institution) to host visiting scholars and postdoctoral researchers from the PRC and train them in their area of expertise.[21] In effect, PRC talent programs are ever-expanding recruitment networks. Once inducted, participants are incentivized and obligated to identify top talent for placement in desirable research positions at their host institution and for eventual recruitment back to the PRC.

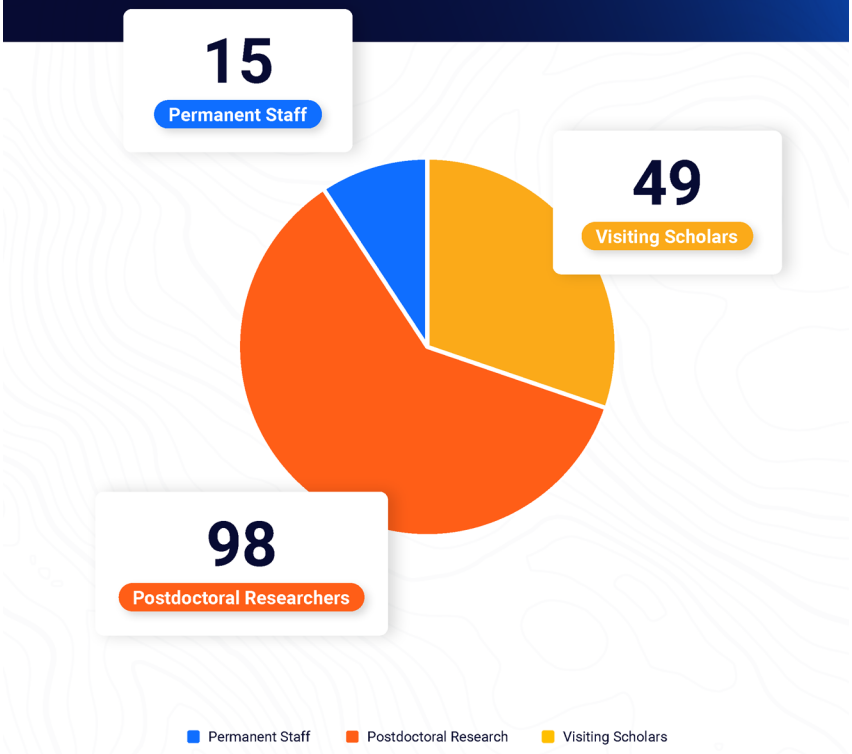
For example, at least two Los Alamos scientists have served as CAS Overseas Review Experts (中国科学院海外评审专家) prior to returning to the PRC. Established in 1999, the CAS Overseas Review Experts system is designed primarily to "encourage excellent individuals who are studying abroad to return to China and serve their motherland" and to "promote the recruitment of overseas talents and intelligence."[22] Those hired as overseas review experts must "have the intention to actively service the science and technology cause of the motherland."[23]

One of the most high-profile elements of the talent strategy has been the TTP, which was established in 2008 to recruit leading scientists, academics, and entrepreneurs to advance the PRC's interests. Oversight of the TTP fell under the CCP Central Committee Organization Department, a secretive party organ controlling personnel appointments within the Party. In 2019, the PRC folded all TTP programs into the "High-End Foreign Expert Recruitment Plan" (高端外国专家引进计划) managed by the PRC Ministry of Science and Technology.

Of the 162 Los Alamos scientists who have returned to China, at least 17, including 13 permanent staff members, were selected into the TTP. Members of the TTP receive RMB 1,000,000 (approximately USD $155,000) and a research subsidy of RMB 3 million to 5 million (approximately USD $465,000 to $775,000).[24] Forty-two scientists were selected for the TTP's youth branch, the Youth Thousand Talents Program (青年千人计划) or YTTP. Established in 2011, the YTTP recruits outstanding scientists under the age of 40 with the potential to greatly contribute to the achievements of PRC science and technology (S&T) and industrial objectives. YTTP selectees receive a one-time grant of RMB 500,000 (approximately USD $77,500), a research subsidy of RMB 1 to 3 million (approximately USD $155,000 to USD $465,000), and appointments at PRC institutions.[25]

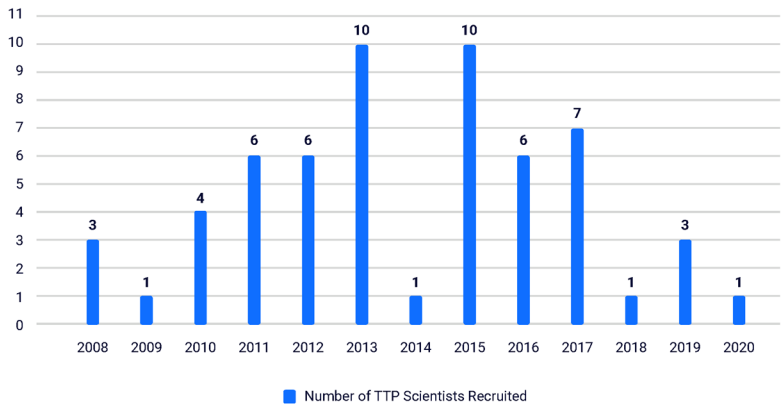
Los Alamos Scientists Who Returned to the PRC

BY EMPLOYMENT TYPE



Los Alamos Scientists Recruited into the Thousand Talents Program

BY YEAR



Recruitment from Los Alamos soared with the introduction of YTTP, which expanded the scope of potential recruits and peaked between 2013 and 2016, when upwards of 10 Los Alamos scientists returned to the PRC each year as TTP selectees.

- The ability to track TTP recruitment has declined since 2017. In October 2018 information related to the TTP began to disappear from Chinese open-source publications, probably because of increased scrutiny by the United States[27]
- It is possible that the TTP's growth has declined in recent years as other PRC talent-recruitment tactics have evolved. The DOE began blocking scientists from participating in foreign government talent-recruitment programs in 2019.[28]

SUSTech & Dr. Chen Shiyi

A Source of Expertise Driving the Development of Key PRC Military and Dual-Use Technologies

Former Los Alamos scientists are playing a key role in advancing China's science and technology programs, including military initiatives. In a 2017 article titled "America's Hidden Role in Chinese Weapons Research," the Hong Kong-based *South China Morning Post* reported that, "while the numbers remain unknown, so many scientists from Los Alamos have returned to Chinese universities and research institutes that people have dubbed them the 'Los Alamos Club.'"[29] While the total number of individuals who have returned to China following stints at U.S. government–funded labs is unclear, the individuals who have been identified are contributing to meaningful advances in China's military modernization, presenting a range of security challenges to the United States and its allies. The careers of a few of the scientists who previously worked at Los Alamos illustrate the ways and means by which PRC government programs recruit foreign-trained experts for strategic initiatives.

A central figure of the Los Alamos Club is Dr. Chen Shiyi (陈十一). Dr. Chen arrived at Los Alamos in 1990 and became one of the first PRC nationals to receive the Oppenheimer Fellowship, a distinguished fellowship reserved for the top postdoctoral applicants.[30] He served as deputy director of the lab's Center for Nonlinear Studies (CNLS) from July 1997 to January 2000. Chen joined Johns Hopkins University in 2001 and served as chair of the Department of Mechanical Engineering from 2002 to 2004 before becoming the Alonzo G. Decker Chair in Engineering and Science in 2005.[31] That same year, he returned to the PRC to establish Peking University's (PKU's) engineering college. Chen became a CAS Academician in 2013—a position reserved for those who make the greatest contributions to PRC scientific research. From 2015 to 2020, he served as president of Southern University of Science and Technology (SUSTech) in Shenzhen, China.

SOUTHERN UNIVERSITY OF SCIENCE AND TECHNOLOGY (SUSTECH)

Building "China's Stanford" in 10 Years on Recruitment from Los Alamos

- SUSTech is a public research university established in Shenzhen in 2010 by the Shenzhen municipal government. Nearly all SUSTech's direct financial support comes from the Shenzhen municipal government. Its stated ambition is to become "China's Stanford."
- At least 15 Los Alamos alumni are currently employed at SUSTech. For a relatively new institution, it employs a disproportionately high number of world-class scholars, most of whom were recruited via PRC government talent programs, transforming it into an important S&T center within the PRC.
- According to a report by a PRC Ministry of Education media outlet, more than 40 percent of SUSTech faculty are members of the TTP and the YTTP.

As head of SUSTech, Dr. Chen excelled at recruiting scientists with Los Alamos links to the university. Many of these returnees had personal and professional ties to Chen. For his achievements, the Shenzhen municipal government honored Chen in 2017 with the title of "Shenzhen Talent Ambassador" (深圳人才大使).[32] SUSTech currently hosts at least 15 Los Alamos alumni.

HYPERSONICS

In addition to helping turn SUSTech into a premier research university in China, Chen Shiyi is a world-renowned expert in fluid dynamics and turbulence who has made major contributions to China's hypersonic missile and aerodynamics programs. He is a key figure in a PRC defense innovation system intentionally designed to blur the lines between civilian and military research.

Chen Shiyi joined PKU's State Key Laboratory of Turbulence and Complex Systems (LTCS) in 2005 and was its director from 2011 to about 2020.[33] He continued to lead LTCS during his 2015–2020 tenure as SUSTech president. Established in 1995, LTCS conducts fundamental and applied research on turbulence, aerospace mechanics, and complex flows. Chen is currently honorary director of the laboratory and vice director of LTCS' Academic Committee.[34] LTCS is organized around the staff, equipment, and facilities of PKU's College of Engineering, where Chen served as inaugural dean between 2005 and 2013.

Under Chen's leadership, LTCS played a key role in developing the PRC's hypersonic glide vehicle.[35] According to the LTCS website, the lab "actively participated in the development of national strategic equipment and hypersonic wind tunnels."[36] This is a reference to PKU's quiet hypersonic wind tunnels,[37] the first of which was one of only three in the world when it was built between 2010 and 2011.[38] Compared with conventional hypersonic wind tunnels, quiet wind tunnels more accurately simulate in-flight conditions for objects flying at hypersonic speeds.

- Using data from PKU's quiet hypersonic wind tunnels, LTCS claimed that it made contributions that were "invaluable in the design of hypersonic vehicles."[39]
- According to the PKU College of Engineering's Hypersonic Quiet Wind Tunnel Laboratory (高超声速静风洞实验室)—a facility used by LTCS staff—research using wind tunnels built during Chen's time as PKU engineering dean and LTCS director "made important contributions" that allowed "[the PRC] to surpass the U.S. in airbreathing [hypersonic] vehicle research and development."[40]

HYPERSONICS (CONT.)

LTCS occupies a central role in a wider network of organizations involved in PRC hypersonic and defense aerodynamics research. During Chen's tenure as director, LTCS undertook major national projects with military organizations such as the National University of Defense Technology (NUDT) and the China Aerodynamics Research and Development Center (CARDC), defense-industry enterprises such as China Aerospace Science and Technology Corporation's (CASC) 11th Academy, as well as members of the Seven Sons of National Defense, a grouping of PRC universities that collaborate closely with the PLA.[41]

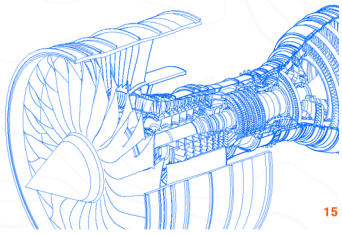
- In 2013, Chen and LTCS cohosted a symposium with NUDT's Defense S&T Key Laboratory of Hypersonic Ramjet Technology (高超声速冲压发动机技术国防科技国家重点实验室) on engine detonation, a field relevant for hypersonic propulsion.[42]
- Shortly after Chen stepped down as director in 2020, LTCS began discussions to establish a joint state laboratory with CASC's Third Academy, the PRC's premier enterprise engaged in cruise missile design and production.[43]

As recently as March 2020, Chen was serving as a member of the academic committee of the CARDC State Key Laboratory of Aerodynamics.[44] In this position, Dr. Chen was responsible for managing research objectives and annual work plans. CARDC, also known as the PLA's 29th Testing and Training Base (Unit 63820), is the PRC's largest aerodynamics research and testing institute and serves as China's primary hypersonic test facility.[45] The laboratory conducts aerodynamic modeling in areas such as hypersonic boundary layer transition, weapons bay aeroacoustics, and advanced fighter maneuvers.[46] Since 1999, CARDC has been on the U.S. Department of Commerce's Entity List, a trade-restriction list of individuals and entities conducting activities deemed contrary to the national security or foreign policy interests of the United States.[47]

JET ENGINES

Chen Shiyi also served on an Expert Steering Group of a major National Science Foundation of China (NSFC) research plan on jet engine development in China. The NSFC is a PRC government body that advances basic research in support of PRC strategic needs. NSFC Expert Steering Groups usually consist of seven to nine experts responsible for overall project guidance, implementation, and review of NSFC research plans.[48] In 2014 NSFC launched the Fundamental Research on Turbulent Combustion for Engines Major Project Research Plan (面向发动机的湍流燃烧基础研究重大研究计划), an eight-year research effort aimed at resolving key technological bottlenecks in indigenous engine development, a longstanding impediment in PRC domestic civilian and military aircraft design and production.[49]

- The organizations charged with conducting the research for this NSFC project include three PLA institutions—NUDT, Air Force Engineering University (AFEU), and CARDC—along with two state-owned defense-industry giants—China Academy of Aerospace Aerodynamics (also known as the CASC 11th Academy) and the Shenyang Aeroengine Research Institute (also known as the AVIC 606 Institute).[50]
- CARDC organizes the project's annual conferences on NSFC's behalf, while its Air-breathing Hypersonic Technology Research Center (吸气式高超声速技术研究中心) hosts the project's web page.[51] [52]
- Shan Xiaowen, a SUSTech professor and former Los Alamos permanent staff member, contributed to the project in 2017 by leading an examination into the effects of combustion on turbulence under engine conditions.[53]



DEEP-EARTH PENETRATING WARHEADS

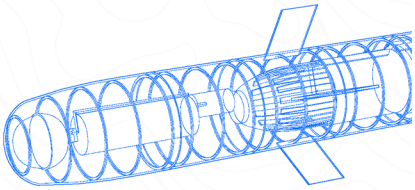
One of Chen Shiyi's first hires as the president of SUSTech was his former Los Alamos colleague, Zhao Yusheng (赵予生). During his 18-year career at Los Alamos, Zhao received at least 28 grants totaling $19.8 million in U.S. government funding for sensitive research.[54] From 2004 to 2005, Zhao led a DOE–Department of Defense (DOD) project entitled "Nanostructured Superhard Noses for Deep-Penetrating Warheads."[55] Zhao was also granted a DOE "Q Clearance"—allowing access to Top Secret Restricted Data and National Security Information—and led the lab's team researching high-pressure materials.[56]

- Zhao left Los Alamos in 2010 to lead the University of Nevada, Las Vegas (UNLV) High-Pressure Science and Engineering Center (HiPSEC)—a position that also required a Q Clearance—where he received approximately $2.9 million in DOE funding for research into new battery materials.[57]
- Zhao was inducted into the TTP in 2016 and returned to China, where he has since served in several SUSTech leadership roles, including associate vice president, dean of its Academy of Advanced Interdisciplinary Studies, director of its Office of Research, and chair professor in SUSTech's Physics Department.[58]

Further review suggests that one of the 25 postdoctoral researchers Zhao sponsored at Los Alamos, He Duanwei (贺端威), likely leveraged or replicated Los Alamos research on materials for use in hypersonic, deep-earth penetrating warheads after he returned to the PRC in 2006. Dr. He worked as a postdoctoral research associate at Los Alamos from 2000 to 2003, with some information suggesting he remained employed at the lab until 2005.[59] In a 2004 edition of a Los Alamos publication, *Nuclear Weapons Journal*, Zhao described how research on superhard nanocomposites was "highly promising for hypersonic high-speed penetration" and noted that "super-hard materials in warhead penetrators [would] significantly enhance technological advantages of U.S. weaponry."[60] Dr. Zhao claimed that this research was conducted with the U.S. Navy.[61] Three years later, in 2007, Dr. He filed a national defense patent in China on a similar technology for an "ultra-thick penetrating warhead"[62]

- Following the approval of the patent in 2011, Dr. He co-led a Major National Defense Special Project (国防重大专项) subproject on synthesizing superhard nano-polycrystalline diamonds in China.[63]
- The project involved a scientist working for the Chinese Academy of Engineering Physics' (CAEP) Laboratory of Shock Wave Physics and Detonation Physics (冲击波物理与爆轰物理实验室).[64]
- CAEP is the PRC's nuclear weapons R&D and production facility. The CAEP Laboratory of Shock Wave Physics and Detonation Physics is also known in Chinese-language sources as the National Defense Key Laboratory of Shock Wave and Detonation Physics (冲击波物理与爆轰物理国防重点实验室).[65]

Dr. He currently serves as director of the Sichuan University Institute of Atomic and Molecular Physics (四川大学院子与分子物理研究所), where he also heads the High Temperature and High Pressure Physics Laboratory (高压科学与技术实验室), which is jointly administered by CAEP.[66] Both Sichuan University and CAEP are subject to U.S. government export controls for their role in China's nuclear program. Dr. He also leads the high-pressure physics group at the Ministry of Education Key Laboratory of High Energy Density Physics and Technology (高能量密度物理及技术教育部重点实验室), a defense-oriented laboratory whose website states that its research is conducted in pursuit of the PRC's Medium and Long-Term Defense S&T Development Plan.[67]



UNMANNED AUTONOMOUS VEHICLES

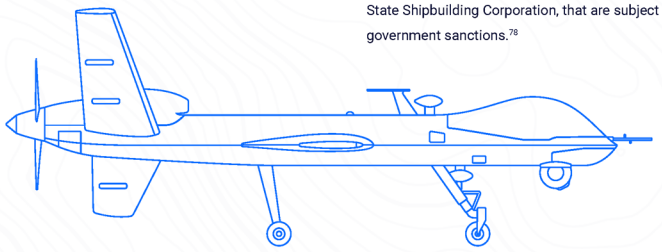
In 2016, Chen Shiyi recruited Shan Xiaowen (单肖文) to serve as chair professor in SUSTech's Department of Mechanics and Aerospace Engineering. Dr. Shan became head of the SUSTech Intelligent Aviation R&D Center in 2019, which focuses on unmanned aerial vehicle (UAV) technologies. Under Shan's leadership, the center produced a prototype Vertical Take-Off and Landing (VTOL) UAV with both civil and military applications.[68] The center is located in the same state-organized industrial cluster that hosts testing and production facilities for military drones, an example of PRC efforts to integrate civilian research with military end users.[69]

- Shan worked at Los Alamos from 1991 to 1998, first as a postdoctoral researcher and then as a permanent staff member. He collaborated with Chen in the early 1990s on Lattice Boltzmann methods (LBM), a form of computational fluid dynamics commonly used in the aerospace industry.[70]
- After becoming a member of the Los Alamos permanent staff, Shan conducted research as a visiting fellow at the U.S. Air Force Research Laboratory.[71] Dr. Shan returned to the PRC in 2011 as a TTP selectee and joined the Commercial Aircraft Company of China (COMAC) as director of aerodynamics at the company's Beijing Research Center. In this capacity, he led the preliminary design of the PRC's first domestically produced wide-body commercial aircraft, the C919, a project notorious for allegations of industrial espionage.[72]

DR. CHEN CONTINUES TO SUPPORT CHINA'S DEFENSE INDUSTRY VIA NEW TECH COMPANY

Dr. Chen remains active in China's defense innovation ecosystem. Since stepping down from his position as SUSTech president in 2020, Chen established a computer-aided engineering software company called Shenzhen Shifeng Technology Co., Ltd. (深圳十沣科技有限公司, aka TenFong). Chen linked the company's establishment to wider efforts in the PRC to create industrial software independent from foreign suppliers.[73] Chen's company has a number of links to the PRC defense industry:

- In late 2021, Shenzhen Shifeng was one of three companies vying for a contract to upgrade heat-flow-analysis software for the China Airborne Missile Academy (中国空空导弹研究院).[74]
- In June 2022, the company acquired Nanjing Youyi Intelligent Technology Co., Ltd. (南京友一智能科技有限公司).[75] Youyi's product line includes FlightSim, a simulation software with advertised applications in ballistic missile flight modeling, including simulation of coordinated salvo launches.[76]
- Shenzhen Shifeng's Xi'an branch is led by Qu Kun (屈昆) and Cai Jinsheng (蔡晋生), professors at Northwestern Polytechnical University, a Seven Sons school, who have headed multiple classified defense aerospace projects in China.[77]
- Shenzhen Shifeng has entered into cooperative ventures with at least two companies, Qihoo 360 and China State Shipbuilding Corporation, that are subject to U.S. government sanctions.[78]



THE LOS ALAMOS CLUB

Beyond SUSTech

Los Alamos alumni who are not connected with SUSTech are also contributing to research in highly strategic technology and contributing to PRC defense research, but the scope and scale of these efforts is unclear. These individuals include visiting scholars, postdoctoral researchers, and permanent staff.

At least 13 either work for or have participated in research sponsored by defense organizations such as the Central Military Commission (CMC) and SASTIND.

At least seven have ties to the Chinese Academy of Engineering Physics (CAEP), the primary R&D and production facility for the PRC's nuclear weapons program.

At least four former Los Alamos postdoctoral researchers currently work at the State Key Laboratory of Electronic Thin Films and Integrated Devices (SKLETFID), two of whom received national defense S&T awards for their contributions. The facility received more than half of its funding from defense entities between 2012 and 2017. SKLETFID's accomplishments include producing multispectral camouflage materials for an unnamed stealth fighter, developing advanced sensors for aircraft engines, and providing infrared detectors for PLA aircraft.

One former Los Alamos permanent researcher led research for both the U.S. military and the PLA while concurrently employed as a professor at a U.S. university and as a Thousand Talents selectee at Nanjing University of Science and Technology (NJUST). NJUST is a member of the Seven Sons of National Defense, a group of universities that collaborate closely with the PLA.

- Between 2009 and 2015, the individual received approximately $1.8 million from the U.S. Army Research Office, the U.S. Army Research Laboratory, the U.S. Air Force Office of Scientific Research, and the U.S. Air Force Small Business Innovation Research (SBIR) Program for research on advanced materials.
- While conducting research on advanced materials for the U.S. military, this individual presided over a 390 million RMB project from the CMC S&T Commission's Major Frontier Innovation Program (军委科技委前沿创新重大项目) that made breakthroughs in titanium aluminide (TiAl) alloys, a lightweight material with applications in defense aerospace.
- The former Los Alamos researcher collaborated on this project with a researcher who had previously spent time at Oak Ridge National Laboratory as a visiting scholar. The former Oak Ridge visiting scholar later won the PRC's highest-level defense S&T prize in 2021 for a separate project.

He Guowei & China's Submarine Noise-Reduction Programs

Former Los Alamos visiting scholar He Guowei (何国威) is a key figure in the PRC's efforts to deploy quieter submarines that are better able to evade detection—a hallmark of the world's most modern navies.

Dr. He was a visiting scholar at the Los Alamos CNLS in the late 1990s when Chen Shiyi served as deputy director of the CNLS lab and it is possible that Chen recruited He to come to Los Alamos.[79] The two cooperated extensively at the lab, publishing seven articles together between 1998 and 1999.[80]

- Dr. He joined the staff of the Chinese Academy of Sciences Institute of Mechanics (IMCAS) in 1991 as a postdoctoral researcher and rose through the ranks to become director of its State Key Laboratory of Nonlinear Mechanics (LNM) in 2006.[81]
- In the interim, He was a visiting scholar at the French National Centre for Scientific Research (1995–1997), at Los Alamos (1997–2000), and at the Institute for Computer Applications in Science and Engineering (ICASE) at the NASA Langley Research Center (2000) before returning to the PRC as a selectee of the CAS Hundred Talents Program.

He's team at the IMCAS LNM developed computer models that help to quickly and accurately predict turbulence generated by a submarine.[82] As of 2019, He continued to pursue research in the "intelligent identification theory of submarine turbulence noise" at IMCAS.[83] Most of the PRC's other preeminent experts in submarine noise reduction technology are PLA scientists.[84]

Conclusion

China's recruitment of individuals who have worked at the Los Alamos National Laboratory reflects the evolution of the PRC's overall talent strategy and shows how China's rapid advances in certain key military technologies are being aided by individuals who may be applying knowledge obtained while participating in sensitive U.S. government–funded research.[85] The PRC's success at Los Alamos, and support for China's talent programs by Xi Jinping and other top CCP leaders, suggest that similar efforts may be widespread at other U.S. government–funded laboratories, research institutions, and major centers of innovation.

The U.S. government has begun to take steps to mitigate these risks. In recent years, the PRC's state-sponsored talent programs, such as the TTP, have drawn increased scrutiny from Washington not only because of counterintelligence and intellectual property (IP) theft risks, but because these programs are leveraging taxpayer-funded research to advance the PRC's economic development and military modernization. According to a 2019 Senate report, PRC talent programs violate U.S. research values, target U.S. basic research, and erode U.S. economic competitiveness. That same year, the DOE issued guidance prohibiting involvement by its employees or contractors in foreign talent-recruitment plans.

- Several persons connected to the TTP have been indicted by the U.S. Department of Justice. In May 2022, a federal judge sentenced Xiaorong "Shannon" Yu, a chemical engineer and TTP applicant, to 14 years in prison for conspiring to steal trade secrets for the benefit of a PRC-based company.
- In December 2021, a federal jury found Harvard chemist Charles Lieber guilty of making false statements and tax offenses related to his participation in the TTP and his undisclosed affiliation with a PRC university.

However, more can be done by government-funded laboratories, research institutions, and private industry to identify potential counterintelligence and IP theft risks posed by individuals whose talent the PRC is seeking to leverage in its race for science and technology dominance. Moreover, it is an urgent national security imperative for like-minded nations to work together to protect their innovation centers and compete with China to attract, retain, and protect leading talent.

Appendix

Former affiliates of Los Alamos are central to the networks of scientists engaged in China's defense modernization and pursuit of civil-military fusion. This appendix offers additional insight and context into the personalities, relationships, and organizations in China involved in that work.

Chen Shiyi and Defense Aerodynamics

While Chen Shiyi guided LTCS and PKU participation in the PRC's development of hypersonic glide vehicles, the LTCS's leadership included military scientists linked to CARDC.

- **Zhang Hanxin** (张涵信), a CARDC researcher and former CARDC deputy chief engineer, served as the LTCS academic committee director when Chen joined LTCS in 2005. Chen served as Zhang's deputy on the LTCS academic committee, and in 2006, Chen hired Zhang as an LTCS adjunct professor.[87] At that time, Zhang held a specialized technical major general rank and was well known in PRC aerodynamics circles for his national defense contributions, notably "developing three major software systems for the aerodynamic design of aircraft, tactical missiles, and re-entry warheads."[88]
- **Deng Xiaogang** (邓小刚) currently serves under Chen on the LTCS academic committee.[89] Deng is a CAS Academician who led the PLA's NUDT from 2017 to 2019. Deng held the rank of specialized technical major general and was chief engineer at CARDC, where he served as the inaugural director of the center's State Key Laboratory of Aerodynamics[91] and "presided over the development and testing of hypersonic wind tunnels and resolved problems in the development of many major weapons and equipment, including…advanced fighter jets, missiles, and hypersonic vehicles."[92] In 2020, the PLA elevated Deng to vice president of the Academy of Military Sciences, the PLA's highest-level research institute.[93]

Chen Shiyi and Defense Aerodynamics (Cont.)

In addition, Chen has worked closely with senior PLA scientists on multiple Expert Steering Groups for NSFC Major Research Plans（重大研究计划). NSFC Expert Steering Groups usually consist of seven to nine experts responsible for overall project guidance, implementation, and review of NSFC research plans.[94]

In 2017, Chen was tapped to head the Expert Steering Group for the NSFC Major Research Plan for Generation, Evolution, and Action Mechanism of Turbulent Structures (湍流结构的生成演化及作用机理重大研究计划). Chen's fellow Expert Steering Group members included several PLA and PRC defense-industry scientists, including:[95]

- **Sun Mingbo** (孙明波), an expert in hypersonic propulsion technologies, is a professor at NUDT and director of the university's Key Laboratory of Hypersonic Ramjet Technology (高超声速冲压发动机技术重点实验室).[96]
- **Shen Qing** (沈清) leads the Science and Technology Committee of the CASC 11th Academy.
- **Deng Xiaogang** (See bio on previous page).

In 2014, the NSFC launched the Fundamental Research on Turbulent Combustion for Engines Major Project Research Plan (面向发动机的湍流燃烧基础研究重大研究计划).[97] Once again, Chen participated in the plan's Expert Steering Group alongside military scientists:

- **Gan Xiaohua** (甘晓华), an aeroengine specialist, serves as head of the Expert Steering Group, Chinese Academy of Engineering (CAE) Academician, and chief engineer at the PLA Air Force Equipment Academy (中国解放军空军装备研究院).[98] In 2010, Gan received a personal commendation by General Secretary Hu Jintao for his role in developing the J-20 stealth fighter's thrust vectoring engines. In 2014, Chen hired Gan as an adjunct professor at LTCS. In May 2017, Chen appointed Gan as a chair professor in SUSTech's Department of Mechanics and Engineering.[99]
- **Le Jialing** (乐嘉陵), is deputy head of the Expert Steering Group, CAE Academician, and former CARDC researcher on the aerodynamic design of strategic missiles, launch vehicles, and hypersonic vehicles. Le concurrently acts as the National Defense S&T Key Laboratory of Hypersonic Ramjets (高超声速冲压发动机国防重点实验室) academic committee director and as a researcher at the Academy of Military Sciences (军事科学院, AMS), the PLA's highest-level research institute. When Xi Jinping visited AMS in May 2018, Le was part of a small group of defense researchers to receive a private audience with the General Secretary.[100]

Xu Ping and Wang Hsing-lin: Case Studies in Sending Talent Abroad

In 2005, **Xu Ping** (徐平) was identified and honored as an Outstanding Graduate of the Harbin Institute of Technology (HIT) by the PRC's Commission for Science, Technology and Industry for National Defense (COSTIND). HIT is one of the PRC's Seven Sons of National Defense.

- During his PhD program at HIT, Xu also served as PRC government State-Sponsored Overseas Joint Training Doctoral Program scholar at Los Alamos from 2008 to 2009.
- After completing his doctoral program in 2010, Xu became a postdoctoral researcher at HIT until 2014 under CAE Academician Zhou Yu (周玉). At the time Zhou was leading PRC government–funded research into heat-resistant ceramic matrix composites that were later used on satellites, rockets, and hypersonic vehicles.[101]
- During this time, Xu was sponsored by Los Alamos permanent staff member Wang Hsing-lin (王湘麟) to return to the lab as a Director's Postdoctoral Fellow. After departing Los Alamos in 2013, Xu was inducted into the HIT Basic Research Outstanding Talent Cultivation Program (哈工大基础研究杰出人才培育计划) in 2014.[102]
- Xu is currently a professor and vice dean of the HIT School of Chemistry and Chemical Engineering.[103] Zhou served as the president of HIT from 2014 to 2021.

Xu's 2012 sponsor, Wang Hsing-lin, is the longest tenured Los Alamos researcher to go to the PRC as a TTP selectee. Wang spent 21 years, from 1995 to 2016, at Los Alamos' Chemistry Division, first as a postdoctoral researcher and then as a member of the permanent staff.[104] [105]

- During his Los Alamos tenure, Wang also served as a subject-matter expert at the DOD Homeland Defense and Security Information Analysis Center (HDIAC).[106]
- In 2016, Wang was recruited into the TTP and returned to the PRC as a chair professor of the Department of Material Science and Engineering at SUSTech under Chen Shiyi.[107]

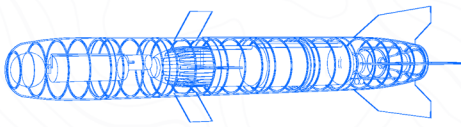
He Guowei and the PLA Navy

Several PLA scientists serve alongside Dr. He on the Academic Committee of the Shanghai Jiaotong University State Key Laboratory of Ocean Engineering (海洋工程国家重点实验室, SKLOE). These include:

- **He Lin** (何琳), a CAE Academician, specialized technical rear admiral, and professor at the PLA Naval University of Engineering, where he established the National Defense S&T Key Laboratory of Submarine Acoustic Stealth Technology (潜艇声隐身技术国防科技重点实验室) in 2011.
- **Wu Yousheng** (吴有生), a CAE Academician who as of 2020 directed the PRC's Central Military Commission S&T Commission Naval Warfare Expert Group.[108]
- **Qiu Zhiming** (邱志明), a CAE Academician and weapons researcher at the PLA Naval Research Academy who designed the Type 730 close-in weapon system (CIWS) and made technical breakthroughs in vertical launching systems (VLS).[109]
- **Zhu Yingfu** (朱英富), a CAE Academician who was chief designer for both the PRC's first guided missile destroyer with true air defense capability and its first aircraft carrier.[110]
- **Yang Desen** (杨德森), a CAE Academician and Harbin Engineering University professor who directs the National Defense S&T Key Laboratory of Underwater Acoustic Technology (水声技术国防科技重点实验室) and was a member of the PLA General Armaments Department Submarine Vibration Dampening and Noise Reduction Technology Expert Group.[111]

The SKLOE is emblematic of how research at certain PRC labs straddle the line between civilian and military research. Highlighting its dual-use missions, its website declares that it "is positioned to pay equal attention to applied basic research, national defense scientific research, [and] civilian scientific research."[112] Some of its research is clearly military oriented:[113]

- Development of hydrodynamic and hydro-ballistic models for underwater launch of submarine-launched missiles.
- A classified project from 2014–2015 on maritime sensing technology sponsored by a unit of the former PLA General Staff Department.
- A NSFC Key Project entitled "Collaborative Monitoring of Underwater Moving Targets Based on Dynamic Multi-source Information."
- A classified project from 2017–2019 sponsored by the former PLA General Armaments Department.
- Research pertaining to submarine maneuverability and stealth, including vibration and noise reduction.



Footnotes

[1]These activities are not limited to U.S. national laboratories, or even to the U.S. In early 2022, an investigation by Deutsche Welle found that dozens of PRC researchers sponsored by the German government to study in Germany now conduct military research. See "How a Humboldt Commission fellow joined China's military commission," Deutsche Welle, March 20, 2022, https://www.dw.com/en/how-a-humboldt-foundation-fellow-joined-chinas-military-commission/a-61858074.

[2]"6月23日，一个值得中国人记住的日子 [June 23, a Day Worth Remembering for Chinese People]," 中国网教育频道 [China Net Education Channel], June 26, 2019, accessed June 1, 2022, http://edu.china.com.cn/2019-06/26/content_74923429.htm.

[3]"中共中央关于建立社会主义市场经济体制若干问题的决定 [Decision of the CPC Central Committee Regarding a Number of Issues Concerning the Establishment of a Socialist Market Economy]," Central Committee of the Communist Party of China, November 14, 1993, accessed May 4, 2022, http://www.people.com.cn/item/20years/newfiles/b1080.html.

[4]"中共中央关于建立社会主义市场经济体制若干问题的决定 [Decision of the CPC Central Committee Regarding a Number of Issues Concerning the Establishment of a Socialist Market Economy]", Article 43. Article 43 of the Decision also calls for "adopting various forms, encourage overseas talent to serve the motherland" (采取多种形式，鼓励海外人才为祖国服务) alongside the policy direction.

[5]For example, "'九五'期间人事系統留学人员工作规划 [The Personnel System Work Plan for Overseas Students During the 'Ninth Five-year Plan' Period]," Section 2(3); 留学人员回国工作"十一五"规划 [Eleventh "Five-year Plan" for Overseas Students Returning to Work in China], Section 2(1) and "留学人员回国工作'十二五'规划 [Twelth "Five-year Plan" for Overseas Students Returning to Work in China]," Section 2(1).

[6]"习近平在欧美同学会成立100周年庆祝大会上的讲话 [Xi Jinping's Speech at the Celebration of the 100th Anniversary of the European and American Alumni Association]," [中华人民共和国中央人民政府] The Central People's Government of the People's Republic of China, October 21, 2013, accessed June 2, 2022, http://www.gov.cn/ldhd/2013-10/21/content_2511441.htm.

[7]In 2009, the PRC government launched a new initiative based on this 2001 policy – the 海外赤子为国服务行动计划[Homeland-Serving Action Plan for Overseas Chinese] (hereafter Serve the Homeland Action Plan), which is still implemented each year. The 2009 initiatives governing policy document, 关于实施海外赤子为国服务行动计划的通知 [Notice on Implementing the Serve the Homeland Action Plan], Section 1, cites as a "policy guarantee" the 关于鼓励海外留学人员以多种形式为国服务的若干意见 [Some Opinions on Encouraging Overseas Scholars to Serve Their Country]. The PRC Ministry of Human Resources and Social Security (MOHRSS) called the Homeland-Serving Action Plan for Overseas Chinese a "new brand" for overseas scholars serving the country in an article on its website titled: 赤子计划：树立留学人员为国服务新品牌. See "赤子计划：树立留学人员为国服务新品牌 [Homeland-Serving Action Plan: Establish a New Overseas Brand of Overseas Students Serving the Country]," Ministry of Human Resources and Social Security of the People's Republic of China, April 12, 2013, accessed June 1, 2022, http://www.mohrss.gov.cn/zyjsrygls/ZYJSRYGLSgongzuodongtai/201304/t20130412_98050.html.

[8]关于鼓励海外留学人员以多种形式为国服务的若干意见 [Some Opinions on Encouraging Overseas Scholars to Serve Their Country], Preamble.

[9]关于鼓励海外留学人员以多种形式为国服务的若干意见 [Some Opinions on Encouraging Overseas Scholars to Serve Their Country], Section 2(1-7).

[10]"'九三学社提案：人才称号过多过滥，建议关闭"僵尸'人才计划 [Jiu San Society Proposal: Talent titles are too numerous and too excessive, it is recommended to close 'zombie' talent plans]", February 28, 2018, accessed June 5, 2022, https://www.sohu.com/a/224599002_260616.

[11]Strider, "Quantum Dragon: How China Is Exploiting Western Government Funding and Research Institutes to Leapfrog in Dual-Use Quantum Technologies," published November 2019.

[12]"聚天下英才而用之 [Gather the World's Talents and Use Them]," People's Daily, September 28, 2021, accessed June 1, 2022, http://politics.people.com.cn/n1/2021/0928/c1001-32239119.html.

[13]"哈尔滨工业大学公派联合培养博士研究生选派办法 [Harbin Institute of Technology's State-Sponsored Joint Cultivation Doctorial Candidate Selection Method]," April 13, 2022, accessed June 1, 2022, https://hitgs.hit.edu.cn/2022/0414/c3333a271812/pagem.htm.

[14]"哈尔滨工业大学公派出国留学研究生管理办法（试行）[Measures for the Administration of State-Sponsored Graduate Students of Harbin Institute of Technology (Trial Implementation)]," April 13, 2022, accessed June 1, 2022, https://hitgs.hit.edu.cn/2022/0414/c3333a271812/pagem.htm.

[15]Toauto, "国家公派研究生项目英文介绍, 清华大学2008年国家公派研究生项目手册-摘 [Introduction to State-Sponsored Postgraduate Programs in English, Tsinghua University 2008 State-Sponsored Postgraduate Program Manual—Excerpt]", accessed June 4, 2022, .

[16]Aslanchen, "美国洛斯阿拉莫斯国家实验室功能薄膜材料研究组招收公派联合培养研究生 [Los Alamos National Laboratory Functional Thin Film Materials Research Group Recruits State-Sponsored Graduate Students for Joint Training]," February 12, 2017, accessed June 2, 2022, http://muchong.com/html/201706/11038429.html.

[17]"Postdoctoral Program at Los Alamos National Laboratory," Los Alamos National Laboratory, accessed June 2, 2022, https://www.lanl.gov/careers/career-options/postdoctoral-research/_assets/docs/postdoc-program-brochure.pdf.

[18]"Board of Regents Briefing Paper," Nevada System of Higher Education, June 3, 2010, accessed June 3, 2022, https://nshe.nevada.edu/tasks/sites/Nshe/assets/File/BoardOfRegents/Agendas/10/jun/Board/BOR-19.pdf.

[19]For examples of MSS engagement with PRC study-abroad programs, see "泸州市国安局到我校了解对外交流学生情况 [Luzhou Municipal Ministry of State Security came to our school to understand the situation of foreign exchange students], May 28, 2015, accessed June 5, 2022, http://www.lzljtfzx.com/content/1456.html; "国际教育与交流中心 [International Education and Exchange Center]," Pingxiang University, accessed June 4 2022, http://gjzx.pxc.jx.cn/info/1094/1152.htm; Anastasya Lloyd-Damnjanovic and Alex Bowe, "Overseas Chinese Students and Scholars in China's Drive for Innovation," U.S.-China Economic and Security Review Commission, October 7, 2020, https://www.uscc.gov/sites/default/files/2020-10/Overseas_Chinese_Students_and_Scholars_in_Chinas_Drive_for_Innovation.pdf; Nicholas Eftimiades, "China's Ministry of State Security: Coming of Age in the International Arena," University of Maryland School of Law,1992, p. 15, accessed June 2, 2022, https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1108&context=mscas.

[20]"Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans," United States Senate Permanent Subcommittee on Investigations, accessed June 3, 2022, https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf.

[21]See Supreme Judicial Court of Massachusetts, Lieber v. President & Fellows of Harvard Coll., No. SJC-13141, January 10, 2022, accessed June 1, 2022 , https://casetext.com/case/lieber-v-president-fellows-of-harvard-coll-1; "Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans," United States Senate Permanent Subcommittee on Investigations, p. 73, accessed June 7, 2022, https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans.pdf.

[22]"The Distinguished Researcher Ma Jianxing of Shanghai Institute of Materia Medica was hired as an Overseas Review Expert of the Chinese Academy of Sciences," Shanghai Institute of Materia Medica, Chinese Academy of Sciences, July 2, 2015, accessed June 4,2022, http://english.simm.cas.cn/News/Np/202011/t20201127_253738.html.

[23]"中国科学院增聘"海外评审专家" [Chinese Academy of Sciences Recruits 'Overseas Review Experts']," accessed June 6, 2022, http://www.networkchinese.com/region/china/hutasia.html.

[24]Hepeng Jia, "What is China's Thousand Talents Plan?" Nature Career Guide, January 17, 2018, accessed June 4, 2022, https://media.nature.com/original/magazine-assets/d41586-018-00538-z/d41586-018-00538-z.pdf.

[25]"青年千人计划",海外青年学子归国最佳之选! ['Youth Thousand Talents Program', the best choice for overseas young students to return home!]," Consulate General of the People's Republic of China in Munich, April 1, 2015, accessed June 10, 2022, https://www.mfa.gov.cn/ce/cgmu/chn/jy/jy3/t1251144.htm.

[26]Given that individuals can be selectees of multiple talent programs, we associate each selectee with the highest-level talent program into which they were selected into closest to their recorded return date to the PRC.

[27]"Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans," United States Senate Permanent Subcommittee on Investigations, accessed June 7, 2022, https://www.hsgac.senate.gov/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans.pdf.

[28]"Department of Energy Foreign Government Talent Recruitment Programs," U.S. Department of Energy, June 7, 2019, accessed June 7, 2022, https://www.energy.gov/sites/default/files/2019/06/f63/DOE%20O%20486.1.pdf.

[29]Stephen Chen, "America's Hidden Role in Chinese Weapons Research," South China Morning Post, March 29, 2017, accessed May 31, 2022, https://www.scmp.com/news/china/diplomacy-defence/article/2082738/americas-hidden-role-chinese-weapons-research.

[30]"Distinguished Postdoc Fellows Past and Present," Los Alamos National Laboratory, May 2014, accessed June 1, 2022, https://lanl.gov/careers/career-options/postdoctoral-research/_assets/docs/all-dist-may14.pdf. https://app.box.com/s/qe6t9ixuencnrexc0yff4d5wn46rkz0v.

[31]"CHEN Shiyi," Southern University of Science and Technology, accessed June 3, 2022, https://faculty.sustech.edu.cn/chensy/en/; See also "Shiyi Chen, PhD," Elsevier, accessed June 2, 2022, https://www.journals.elsevier.com/sustainable-horizons/editorial-board/shiyi-chen-phd.

[32]"President Chen Elected as Shenzhen 'Talent Ambassador,'" Southern University of Science and Technology School of Life Sciences, November 2, 2017, accessed June 10, 2022, https://bio.sustech.edu.cn/news/detail/938.html?lang=en-us.

[33]"陈十一 [Chen Shiyi]," Southern University of Science and Technology, accessed June 11, 2022, https://faculty.sustech.edu.cn/chensy/; Chen was still identified as director of LTCS in December 2019, see "湍流与复杂系统国家重点实验室 (LTCS) 与非线性力学国家重点实验室 (LNM) 2019联合学术年会成功召开 [The 2019 Joint Academic Annual Conference of the State Key Laboratory of Turbulence and Complex Systems (LTCS) and the State Key Laboratory of Nonlinear Mechanics (LNM) was successfully held]," 北京大学湍流与复杂系统国家重点实验室 [State Key Laboratory for Turbulence & Complex Systems], December 27, 2019, accessed June 1, 2022, https://ltcs.pku.edu.cn/xwl/tz/919995.html; Chen was still identified as director of LTCS in December 2019. By late-2020, his deputy LI Cunbiao (李存标) had taken up the directorship. See ""水蚀到烧蚀"的一次优雅碰撞 --记纽约大学张骏教授学术报告[An elegant collision of 'water erosion to ablation' -- an academic report of Professor Zhang Jun from New York University], 北京大学湍流与复杂系统国家重点实验室 [State Key Laboratory for Turbulence & Complex Systems], September 23, 2020, accessed June 2, 2022.

[34]"学术委员会 [Academic Committee]," 北京大学湍流与复杂系统国家重点实验室 [State Key Laboratory for Turbulence & Complex Systems], accessed June 10, 2022, https://ltcs.pku.edu.cn/sysgk/xzwyk/index.html.

[35]Stephen Chen, "America's Hidden Role in Chinese Weapons Research," *South China Morning Post*, March 29, 2017, accessed May 31, 2022, https://www.scmp.com/news/china/diplomacy-defence/article/2082738/americas-hidden-role-chinese-weapons-research.

[36]"高超声速静风洞的研制与流动测量技术的发展 [Development of Hypersonic Quiet Wind Tunnel and Development of Flow Measurement Technology]," 北京大学湍流与复杂系统国家重点实验室 [State Key Laboratory for Turbulence & Complex Systems], March 26, 2022, accessed June 14, 2022, https://ltcs.pku.edu.cn/kxyj/kycg/dbxcg/225069.html.

[37]"Φ120mm高超声速静风洞 [Φ120mm Hypersonic Quiet Wind Tunnel]," accessed June 17, 2022, https://www.lab.pku.edu.cn/docs/20140422025560660 80.pdf; Cunbiao Lee and Shiyi Chen, "Recent Progress in the Study of Transition in the Hypersonic Boundary Layer," National Science Review, May 7, 2018, accessed June 14, 2022, https://europepmc.org/backend/ptpmcrender.fcgi?accid=PMC8291524&blobtype=pdf.

[38]A quiet tunnel is so called because it is capable of flowing air at hypersonic velocities without the "noise" created by the turbulent boundary layer that develops at such speeds. See Eric Tegler, "To Develop Hypersonic Weapons, The U.S. Has To Build Some Fiendishly Complicated Wind Tunnels," Forbes, June 19, 2020, accessed June 16, 2022, https://www.forbes.com/sites/erictegler/2020/06/19/to-develop-hypersonic-weapons-the-us-has-to-build-some-fiendishly-complicated-wind-tunnels/?sh=66961513237e.

[39]"高超声速静风洞的研制与流动测量技术的发展 [Development of Hypersonic Quiet Wind Tunnel and Development of Flow Measurement Technology]," State Key Laboratory for Turbulence & Complex Systems, March 26, 2010, accessed June 18, 2022, https://ltcs.pku.edu.cn/kxyj/kycg/dbxcg/225069.html.

[40]"高超声速静风洞实验室 [Hypersonic Quiet Wind Tunnel Laboratory]," 北京大学昌平新校区管委办 [Peking University Changping New Campus Management Committee], accessed June 11, 2022, https://www.cpc.pku.edu.cn/kyfw/zcsys/gxy/931616.htm.

[41]"973项目专栏 [Project 973 Column]," 北京大学湍流与复杂系统国家重点实验室 [State Key Laboratory for Turbulence & Complex Systems], accessed June 11, 2022, https://ltcs.pku.edu.cn/ksdh/zdxmzl/index.html.

[42]"第二届爆轰与爆震发动机研讨会 [2nd Symposium on Detonation and Detonation Engines]," 中国力学学会 [The Chinese Society of Theoretical and Applied Mechanics], February 7, 2013, accessed June 20, 2022, http://www.cstam.org.cn:81/article/169885.html.

[43]"湍流与复杂系统国家重点实验室访问航天三院 探讨国家重点实验室联合共建 [State Key Laboratory for Turbulence and Complex Systems Visits China Aerospace Science and Industry Corporation Third Academy to Discuss the Joint Construction of State Key Laboratories], State Key Laboratory for Turbulence and Complex Systems, September 9, 2020, accessed June 1, 2022, https://ltcs.pku.edu.cn/xwl/tz/922609.html.

[44]"空气动力学国家重点实验室组织召开 学术委员会工作会议 [The State Key Laboratory of Aerodynamics Organized a Working Meeting of the Academic Committee]," 中国空气动力研究与发展中心 [China Aerodynamics Research and Development Center], March 31, 2020, accessed June 23, 2022, http://www.cardc.cn/news_read.asp?ChannelId=2&ClassId=5&Id=144.

[45]"China Aerodynamics Research and Development Center," Australian Strategic Policy Institute China Defence Universities Tracker, accessed June 20, 2022, https://unitracker.aspi.org.au/universities/china-aerodynamics-research-and-development-center/.

[46]See吴继飞 [Wu Jifei] et al., "内埋弹舱舱门气动特性研究 [Investigation on Aerodynamic Characteristics of Internal Bay's Door]," 空气动力学学报 [Chinese Journal of Aerodynamics], 2012, accessed June 1, 2022, http://journal16.magtechjournal.com/Jweb_aas/CN/abstract/abstract11223.shtml and何开锋 [He Kaifeng] et al., "先进战斗机过失速机动模型飞行试验技术 [Model Flight Test Technology for Post-Stall Maneuver of Advanced Fighter]," 空气动力学学报 [Chinese Journal of Aerodynamics], 2020, accessed June 23, 2022, http://kqdlxxb.xml-journal.net/cn/article/doi/10.7638/kqdlxxb-2019.0088?viewType=HTML.

[47]"China Aerodynamics Research and Development Center," Australian Strategic Policy Institute China Defence Universities Tracker, accessed June 20, 2022, https://unitracker.aspi.org.au/universities/china-aerodynamics-research-and-development-center. Error! Hyperlink reference not valid.

[48]"国家自然科学基金重大研究计划管理办法 [Measures for the Administration of Major Research Programs of the National Natural Science Foundation of China]," 国家自然科学基金委员会 [National Natural Science Foundation of China], May 12, 2015, accessed June 14, 2022, https://www.nsfc.gov.cn/publish/portal0/tab475/info70228.htm.

[49]"国家自然科学基金重大研究计划"面向发动机的湍流燃烧基础研究"简介 [Introduction to the National Natural Science Foundation of China Major Research Program "Basic Research on Turbulent Combustion for Engines"]," 实验流体力学 [Journal of Experiments in Fluid Mechanics], March 2022, accessed June 23, 2022, http://www.syltlx.com/cn/topic?id=3c5e939a-fff6-4aca-af99-edebae584900.

[50]"项目介绍 [Project Introduction]," 中国空气动力研究与发展中心吸气式高超声速技术研究中心 [China Aerodynamic Research and Development Center Air-breathing Hypersonic Technology Research Center]," accessed June 14, 2022, http://www.cardc.cn/gaochao/html/Project/.

[51]刘涛 [Liu Tao] and 纪军 [Ji Jun], "面向发动机的湍流燃烧基础研究"重大研究计划 2016年度项目进展交流会在成都召开 [Major Research Program 'Basic Research on Turbulent Combustion for Engines' 2016 Annual Project Progress Exchange Meeting Was Held in Chengdu]," 国家自然科学基金委员会 [National Natural Science Foundation of China], March 21, 2017, accessed June 23, 2022, https://www.nsfc.gov.cn/publish/portal0/tab445/info66169.htm.

[52]"项目介绍 [Project Introduction]," 中国空气动力研究与发展中心吸气式高超声速技术研究中心 [China Aerodynamic Research and Development Center Air-breathing Hypersonic Technology Research Center]," accessed June 14, 2022, http://www.cardc.cn/gaochao/html/Project/.

[53]"单肖文-南方科技大学-发动机条件下燃烧对湍流全尺度影响的机理研究 [Shan Xiaowen-Southern University of Science and Technology-Mechanism of Full-Scale Effects of Combustion on Turbulence Under Engine Conditions]," 中国空气动力研究与发展中心吸气式高超声速技术研究中心 [China Aerodynamic Research and Development Center Air-breathing Hypersonic Technology Research Center], February 2, 2022, accessed June 22, 2022, http://www.cardc.cn/gaochao/html/Project/2017/201802/8Qe6La2Hs6Cm63152.html.

[54]"Tenure upon Hire and Approval for Starting Salary Above Salary Schedule Maximum—UNLV," Board of Regents Briefing Paper, June 4, 2010, accessed June 11, 2022, https://nshe.nevada.edu/tasks/sites/Nshe/assets/File/BoardOfRegents/Agendas/10/jun/Board/BOR-19.pdf.

[55]"Tenure upon Hire and Approval for Starting Salary Above Salary Schedule Maximum—UNLV," Board of Regents Briefing Paper, June 4, 2010, accessed June 11, 2022, https://system.nevada.edu/tasks/sites/Nshe/assets/File/BoardOfRegents/Agendas/10/jun/Board/BOR-19.pdf.

[56]"Tenure upon Hire and Approval for Starting Salary above Salary Schedule Maximum—UNLV," Board of Regents Briefing Paper, June 4, 2010, accessed June 11, 2022, https://nshe.nevada.edu/tasks/sites/Nshe/assets/File/BoardOfRegents/Agendas/10/jun/Board/BOR-19.pdf.

[57]Dan Michalski, "Powered by Discovery: UNLV's Advanced Energy Research Team Is Changing Batteries from the Inside Out," University of Nevada, Las Vegas, December 1, 2015, accessed June 17, 2022, https://www.unlv.edu/news/article/powered-discovery.

[58]"Zhao Yusheng," Southern University of Science and Technology Faculty, accessed June 1, 2022, https://faculty.sustech.edu.cn/zhaoys/en/.

[59]Russell J. Hemley, et al., "Year Two Annual Report," Carnegie/DOE Alliance Center, September 2005, accessed June 13, 2022, https://cdac.carnegiescience.edu/sites/default/files/Report%20website.pdf.

[60]Yusheng Zhao, "Why Robust Deep-Earth-Penetrating Weapons?" Nuclear Weapons Journal, 2004, accessed June 2, 2022, https://www.lanl.gov/orgs/padwp/pdfs/7nwj1-04.pdf.

[61]Eric Canuteson, et al., "Superhard, Ultratough Nanocomposites," Los Alamos National Laboratory, accessed June 10, 2022, https://corpora.tika.apache.org/base/docs/govdocs1/002/002369.pdf.

[62]"贺端威 教授 [Professor He Duanwei]," 四川大学原子与分子物理研究所 [Institute of Atomic and Molecular Physics], Sichuan University, accessed June 20, 2022, http://iamp.scu.edu.cn/jsyjy/201806/148.html.

[63]The authors thank CAEP scientist 毕延 (Bi Yan) for valuable assistance during the course of their research. See 许超 [Xu Chao], et al., "纳米聚晶金刚石的高压高温合成 [High Pressure and High Temperature Synthesis of Nano-Polycrystalline Diamond]," August 2011, accessed June 21, 2022, https://www.wdfxw.net/doc10310326.htm.

[64]"毕延 [Bi Yan]," accessed June 19, 2022, http://a.xueshu.baidu.com/scholarID/CN-B475A9UJ.

[65]PRC defense laboratories often obfuscate their defense ties by omitting the word "national defense" from their official English-language names: "含能材料的相变 [Phase Transitions of Energetic Materials]," 爆炸科学与技术国家重点实验室 [State Key Laboratory of Explosion Science and Technology], September 28, 2017, accessed June 7, 2022, https://est.bit.edu.cn/xzyg/b106897.htm.

[66]"贺端威 教授 [Professor He Duanwei]," [Institute of Atomic and Molecular Physics], Sichuan University, accessed June 20, 2022, http://iamp.scu.edu.cn/jsyjy/201806/148.html.

[67]"转物理学院：校党委书记王建国同志一行来我院调研座谈 [Transfer to the School of Physics: Comrade Wang Jianguo, Secretary of the Party Committee of the School, and His Party Came to our School for Investigation and Discussion]," 四川大学原子核科学技术研究所 [Institute of Nuclear Science and Technology, Sichuan University], April 22, 2019, accessed June 3, 2022, https://720inst.scu.edu.cn/News/info?cid=2633&id=60&mid=60; "实验室简介 [Laboratory Introduction]," 高能量密度物理及技术教育部重点实验室 [Key Laboratory of High Energy Density Physics and Technology], accessed June 12, 2022, http://www.csjiaze-hsca.com/lhedp/sysjj.html.

[68]"无人机应用市场 [UAV Application Market]," 智能航空技术研究中心 [Intelligent Aviation Technology Research Center], accessed June 15, 2022, https://www.sustechtz.com/h5/hkzx/market1.html.

[69]"台州"无中生有"打造出全新的产业集群 蓄势待发 [Taizhou "Creates Something Out of Nothing" to Create a New Industrial Cluster Ready to Go]," 台州新闻 [Taizhou News], September 2, 2021, accessed June 22, 2022, https://tz.zjol.com.cn/tzxw/202109/t20210901_23029993.shtml.

[70]Shiyi Chen, et al., "Lattice Boltzmann Computational Fluid Dynamics in Three Dimensions," Journal of Statistical Physics, August 1992, accessed June 2, 2022, https://link.springer.com/article/10.1007/BF01341754.

[71]D.C. Montgomery, "Nonlinear Magnetohydrodynamics. Progress report, July 1, 1993—June 30, 1994," U.S. Department of Energy, 1994, accessed June 2, 2022, https://www.osti.gov/servlets/purl/10173057.

[72]"Shan Xiaowen," Southern University of Science and Technology, accessed June 21, 2022, https://faculty.sustech.edu.cn/shanxw/en/.

[73]鱼羊 [Yu Yang], "陈十一院士旗下国产CAE软件开发商获数亿元融资，产品技术已有应用成果 [Academician Chen Shiyi's Domestic CAE Software Developer Has Received Hundreds of Millions in Financing, and the Product Technology Has Been Applied]," March 10, 2022, accessed June 13, 2022, https://www.qbitai.com/2022/03/33229.html.

[74]Original tender notice: "热流场仿真分析软件升级招标公告 [Heat Flow Field Simulation Analysis Software Upgrade Tender Announcement]," 中国航空工业集团有限公司 [Aviation Industry Corporation of China Limited], December 2, 2021, accessed June 12, 2022, https://ebid.eavic.com/cms/channel/ywgg1hw/84584.htm; Tender results: "热流场仿真分析软件升级中标候选人公示 [Announcement of Winning Bidders for Heat Flow Field Simulation Analysis Software Upgrade]," 中国航空工业集团有限公司 [Aviation Industry Corporation of China Limited], December 27, 2021, accessed June 12, 2022, https://ebid.eavic.com/cms/channel/ywgg3hw/85346.htm.

[75]"关于十沣 [About Tenfong]," accessed June 14, 2022, https://www.tenfong.cn/about.html#abo_three.

[76]"FlightSim 飞行器可视化设计与仿真平台 [FlightSim Aircraft Visualization Design and Simulation Platform]," 北京友一智能科技有限公司 [Beijing Youyi Intelligent Technology Co., Ltd.], accessed May 31, 2022, https://www.aicae.cn/FlightSim; "FlightSim飞行器弹道设计实战技巧 [FlightSim Aircraft Ballistic Design Practical Skills]," accessed June 1, 2022, https://m.bookschina.com/8374518.htm.

[77]"屈崑 [Qu Kun]," 西北工业大学 [Northwestern Polytechnical University], accessed June 1, 2022, https://teacher.nwpu.edu.cn/kunqu.html; "蔡晋生 [Cai Jinsheng]," 西北工业大学 [Northwestern Polytechnical University], accessed June 1, 2022, https://teacher.nwpu.edu.cn/caijinsheng.html.

[78]"关于十沣 [About Tenfong]," accessed June 14, 2022, https://www.tenfong.cn/about.html#abo_four.

[79]"Historical Perspective," Center for Nonlinear Studies, accessed June 19, 2022, https://cnls.lanl.gov/external/History.php.

[80]"Guowei He's Research While Affiliated with Los Alamos National Laboratory and Other Places," ResearchGate, accessed June 20, 2022, https://www.researchgate.net/scientific-contributions/Guowei-He-7685635.

[81]"何国威[Guowei He]," Institute of Mechanics, Chinese Academy of Sciences, accessed June 1, 2022, http://www.imech.cas.cn/kydw/ysfc/201806/t20180607_5023674.html.

[82]Stephen Chen, "America's Hidden Role in Chinese Weapons Research," South China Morning Post, March 29, 2017, accessed June 1, 2022, https://www.scmp.com/news/china/diplomacy-defence/article/2082738/americas-hidden-role-chinese-weapons-research.

[83]"2019年力学所"大学生创新实践训练计划"申报通知 [2019 Application Notice for the 'Innovative Practice Training Program for College Students' of the Institute of Mechanics]," 中国科学院力学研究所 [Institute of Mechanics, Chinese Academy of Sciences], April 2, 2019, accessed May 31, 2022, http://www.imech.cas.cn/rczp/yjszs/201904/t20190402_5265665.html.

[84]"何琳 [He Lin]," 何梁何利基金 [The Ho Leung Ho Lee Foundation], accessed June 17, 2022, http://www.hlhl.org.cn/news/findnews/showsub.asp?id=1299.

[85]These activities are not limited to U.S. national laboratories, or even to the U.S. In early 2022, an investigation by Deutsche Welle found that dozens of PRC researchers sponsored by the German government to study in Germany now conduct military research: Sandra Petersmann, et al., "How a Humboldt Foundation Fellow Joined China's Military Commission," Deutsche Welle, May 20, 2022, accessed June 20, 2022, https://www.dw.com/en/how-a-humboldt-foundation-fellow-joined-chinas-military-commission/a-61858074.

[86]See "张涵信 [Zhang Hanxin]," 中国力学学会 [Chinese Society of Theoretical and Applied Mechanics], January 1, 2010, accessed June 14, 2022, https://www.cstam.org.cn/introduce/1246/7339 and "北京大学湍流与复杂系统国家重点实验室召开2006年度学术年会暨学术委员会议 [The State Key Laboratory of Turbulence and Complex Systems, Peking University held the 2006 Annual Academic Conference and Academic Committee Meeting]," 北京大学工学院 [Peking University College of Engineering], December 22, 2006, accessed June 2, 2022, https://www.coe.pku.edu.cn/newsfocus/fast/4918.html.

[87]"张涵信院士受聘北京大学兼职教授 [Academician Zhang Hanxin Is Employed as an Adjunct Professor at Peking University]," 北京大学工学院 [Peking University College of Engineering," December 22, 2006, accessed June 25, 2022, https://www.coe.pku.edu.cn/newsfocus/fast/4919.html.

[88]In the PLA, "specialized technical officers" （专业技术军官）are one of five active duty officer career tracks in the PLA. Specialized technical officers tend to be concentrated in equipment and R&D-related organizations. See Kevin Pollpeter and Kenneth W. Allen, eds., The PLA as Organization V2.0, Defense Group Inc., 2021, pp. 23-24; "张涵信 [Zhang Hanxin]," The Chinese Society of Theoretical and Applied Mechanics, January 1, 2010, accessed June 5, 2022, https://www.cstam.org.cn/introduce/1246/7339; 湍流与复杂系统国家重点实验室召开2008年学术委员会会议 [The State Key Laboratory of Turbulence and Complex Systems held the 2008 Academic Committee Meeting]," Peking University College of Engineering, January 14, 2009, https://www.coe.pku.edu.cn/newsfocus/fast/4680.html; [任玉新] Ren Yuxin, "[怀念空气动力学前辈张涵信先生] In Memory of Aerodynamics Elder Mr. Zhang Hanxin," [清华大学怀念师友] Tsinghua University in Memory of Teachers and Friends, Winter 2021, pp. 122–124, accessed June 1, 2022, https://www.tsinghua.org.cn/__local/7/7A/F5/5891883B47E65E649887657D1BA_F4726FBF_1F5C35.pdf.

[89]"学术委员会 [Academic Committee], 北京大学湍流与复杂系统国家重点实验室 [State Key Laboratory for Turbulence & Complex Systems], accessed June 10, 2022, https://ltcs.pku.edu.cn/sysgk/xzwyk/index.html.

[90]"邓小刚 [Deng Xiaogang]," Baidu Baike, accessed May 23, 2022, https://baike.baidu.com/item/%E9%82%93%E5%B0%8F%E5%88%9A/10650911.

[91]"邓小刚 [Deng Xiaogang]," Sichuan University College of Computer Science, September 6, 2021, accessed May 30, 2022, https://cs.scu.edu.cn/info/1249/16117.htm.

[92]战忽局编外工作室 [Zhan Hu Bureau Extra-Staff Studio], "风洞将军邓小刚，转岗军科院副院长，为高超音速武器研制贡献巨大 [Wind tunnel general Deng Xiaogang, who switched posts to become Academy of Military Sciences Vice President, made great contributions to the development of hypersonic weapons]," May 8, 2020, accessed June 1, 2022, https://www.163.com/dy/article/FC4L8EHN0535CD6Z.html

[93]战忽局编外工作室 [Zhan Hu Bureau Extra-Staff Studio], "风洞将军邓小刚，转岗军科院副院长，为高超音速武器研制贡献巨大 [Wind tunnel general Deng Xiaogang, who switched posts to become Academy of Military Sciences Vice President, made great contributions to the development of hypersonic weapons]," May 8, 2020, accessed June 1, 2022, https://www.163.com/dy/article/FC4L8EHN0535CD6Z.html

[94]"国家自然科学基金重大研究计划管理办法 [Measures for the Administration of Major Research Programs of the National Natural Science Foundation of China]," National Natural Science Foundation of China, May 12, 2015, accessed June 2, 2022, https://www.nsfc.gov.cn/publish/portal0/tab475/info70228.htm.

[95]"数理科学部公布重大研究计划项目评审专家名单 [The Mathematical and Physical Sciences Department announces the list of review experts for major research projects]," October 10, 2021, accessed June 4, 2022, https://news.sciencenet.cn/htmlnews/2021/10/466834.shtm.

[96]"第十六届中国青年科技奖特别奖获奖者：孙明波 [The 16th China Youth Science and Technology Award Special Award Winner: Sun Mingbo]," 中国科协培训和人才服务中心 [CAST Center for Professional Training and Services], April 1, 2022, https://mrczx.cast.org.cn/index/article/id/392.

[97]"重大研究计划"面向发动机的湍流燃烧基础研究"项目启动会在绵阳召开 [The Kick-off Meeting of the Major Research Program Basic Research on Turbulent Combustion for Engines' was held in Mianyang]," 中国空气动力研究与发展中心吸气式高超声速技术研究中心 [China Aerodynamic Research and Development Center Air-breathing Hypersonic Technology Research Center], March 26, 2015, accessed June 22, 2022, http://www.cardc.cn/gaochao/html/News/201503/3Pp3Rd7By2Xw33183.html.

[98]"甘晓华 [Gan Xiaohua]," Chinese Academy of Engineering, accessed June 1, 2022, https://www.cae.cn/cae/html/main/colys/71311121.html.

[99]Shu Shan [书山], "俄称中国歼-20达不到5代机标准只能算4代半(图)[Russian claims that China's J-20 can only be counted as a four and a half generation if it can't reach the fifth generation standard]," Sina.com, January 25, 2011, accessed June 3, 2022, http://mil.news.sina.com.cn/2011-01-25/0950629811.html; "湍流与复杂系统国家重点实验室2013年度学术年会暨学术委员会会议在北京大学召开[The 2013 Annual Academic Conference and Academic Committee Meeting of the State Key Laboratory of Turbulence and Complex Systems was held at Peking University]," State Key Laboratory of Turbulence and Complex Systems, January 23, 2014, https://ltcs.pku.edu.cn/xwl/tz/910547.html.

[100]"习主席在视察军事科学院时的重要讲话在全军和武警部队引起强烈反响 [Chairman Xi's important speech during his inspection of the Academy of Military Sciences caused a strong reaction from whole military and the armed police force]," May 17, 2018, http://news.haiwainet.cn/n/2018/0517/c3543307-31318297.html.

[101]"周玉院士牵头的国家自然科学基金委创新研究群体再获延续资助_哈尔滨工业大学 [The innovation research group of the National Natural Science Foundation of China led by Academician Zhou Yu has received renewed funding_Harbin Institute of Technology]," FreeKaoYan.com, accessed June 4, 2022, http://school.freekaoyan.com/heilongjiang/hit/dongtai/2018/04-10/1523339429787623.shtml.

[102]"Xu Ping [徐平], Harbin Institute of Technology, updated July 28, 2022, accessed June 1, 2022, http://homepage.hit.edu.cn/pingxu.

[103]"Home," Ping Xu @ Harbin Institute of Technology, September 20, 2011, https://pingxu.weebly.com/; "Xu Ping [徐平]," Harbin Institute of Technology, updated July 28, 2022, accessed June 1, 2022, http://homepage.hit.edu.cn/pingxu.

[104]"Wang Hsinglin," Southern University of Science and Technology, accessed June 1, 2022, https://faculty.sustech.edu.cn/wangxl3/en/.

[105]"Hsing-lin Wang," Journal of Materials Science and Nanotechnology, accessed June 1, 2022, http://www.annexpublishers.co/editorial-board/member/460/HSING-LIN-WANG-Journal-of-Materials-Science-and-Nanotechnology/.

[106]"Wang Hsinglin," Southern University of Science and Technology, accessed June 1, 2022, https://faculty.sustech.edu.cn/wangxl3/en/.

[107]Ibid.

[108]"中国船舶力学与船舶工程专家吴有生院士做客我校名家讲坛 [Academician Wu Yousheng, an Expert in Mechanics and Ship Eengineering from the China State Shipbuilding Corporation, was a Guest at our School's Famous Expert Forum], https://www.just.edu.cn/news/2020/0831/c8158a268644/page.htm" Jiangsu University of Science and Technology, August 31, 2020, accessed June 2, 2022, https://www.just.edu.cn/news/2020/0831/c8158a268644/page.htm.

[109]"邱志明 [Qiu Zhiming]," Chinese Academy of Engineering, accessed June 2, 2022, https://www.cae.cn/cae/html/main/colys/80521618.html.

[110]"朱英富 [Zhu Yingfu]," Shanghai Jiao Tong University School of Naval Architecture, Ocean & Civil Engineering, accessed June 1, 2022, https://naoce.sjtu.edu.cn/xz_sy/5173.html.

[111]"[杨德森]Yang Desen," X-MOL, accessed May 30, 2022, https://www.x-mol.com/university/faculty/300719.

[112]"海洋工程重大力学问题 [Major Problems in Mechanics in Marine Engineering]," State Key Laboratory of Ocean Engineering, accessed June 1, 2022, https://oe.sjtu.edu.cn/list.php?id=3&t=1.

[113]"海洋工程重大力学问题 [Major Problems in Mechanics in Marine Engineering]," State Key Laboratory of Ocean Engineering, accessed June 1, 2022, https://oe.sjtu.edu.cn/list.php?id=3&t=1.

Senator BARRASSO. It says between 1987 and 2021, the Chinese Communist Party targeted over 160 Chinese nationals working at Los Alamos National Laboratory. Upon returning to China, these researchers helped them advance key military technologies using knowledge financed by us, by the American taxpayers. Today, thousands of non-U.S resident Chinese nationals still work at our national labs, and I believe the majority of these foreign nationals strive to further scientific innovation and collaborate in good faith. Make no mistake, they are beholden to an authoritarian regime, and the Chinese Communist Party is ruthless. Some of these Chinese nationals will see no other choice but to support the Chinese Communist Party through theft of American research and technology because if they don't comply, their families back in China may be punished.

Others will be tempted through bribery. Earlier this year, a Chinese national and former software engineer at Google was arrested for stealing on behalf of a Chinese firm which was paying him secretly. The U.S. Justice Department has charged this individual with stealing software used to orchestrate Google's supercomputers at the cutting edge of machine learning and AI technology.

In 2020, Congress required the Department of Energy to devise a study of counterintelligence efforts at our national labs. The Department hired MITRE, a government contractor, to conduct this study. In April 2023, MITRE produced an unclassified report. Upon receiving the report, the Secretary of Energy then decided to classify it. The Secretary reassigned the Director of the Department's Office of Intelligence and Counterintelligence without an explanation. I have asked the Department to declassify the MITRE report and for the Department to come clean with the American people. The U.S. Department of Energy has refused. One can draw many different conclusions from the Department's stonewalling. The Department may simply want to hide its failures from the public, but whatever the reason, it is clear that the Department of Energy and our national labs have failed to take the China threat seriously.

Mr. Chairman, we can't let our research and technology fall into the hands of China's brutal dictatorship. The Department must dramatically increase its efforts to protect our research from our adversaries, and Congress must step in if the Department fails to do its job.

Thank you again, Mr. Chairman, for calling this important hearing, and I look forward to today's testimony.

The CHAIRMAN. Thank you, Senator.

Now we will turn to our friend and colleague, Senator Durbin.

OPENING STATEMENT OF HON. RICHARD J. DURBIN, U.S. SENATOR FROM ILLINOIS

Senator DURBIN. Do you want to go to Senator Cortez Masto first?

The CHAIRMAN. No, we will go after you, then we are going to go to the witnesses.

Senator DURBIN. I am going to be very brief.

Thank you, Chairman Manchin and Ranking Member Barrasso for this opportunity, and to all the members of the Committee.

I won't sit before you today and pretend I am Nobel Prize material for science or engineering. I am just a liberal arts lawyer. However, there are brilliant scientists in my home State of Illinois that have given me a crash course in quantum computing. I have visited Illinois' two national labs—Argonne and Fermi—many times and seen their extraordinary work. And this past summer, Argonne's Aurora supercomputer achieved exascale computing speeds, landing at the top spot among the most powerful supercomputers in the world. Achievements like this are why, more than a decade ago, I founded the Senate National Labs Caucus, along with Senator Risch. It's why I worked with so many of you on this Committee to support the Department of Energy's Office of Science. The fact is, when America invests in science, we lead the world, and nowhere is this truer than in advanced computing.

I want to say, parenthetically, thank you to Senators Manchin and Barrasso for talking about competition with China. It should be a focal point every single day for all of us. I think for a moment, and I know Senator Barrasso is an amateur historian himself—it was in my lifetime that ping-pong diplomacy took place. This primitive, backward, oxen-driven economy in China in 50 years emerged as a world competitor to the United States of America. And that is why we are meeting today to discuss it.

Senator Daines and I have introduced a bill called the Department of Energy Quantum Leadership Act, reauthorizing quantum research and development activities across DOE, expanding DOE quantum research centers, tackling supply chain and prototype challenges in the private sector, and expanding training programs for the quantum workforce. This is timely, it's important, and it's before this Committee. I urge you to enact it as quickly as possible. Let's get it passed.

The CHAIRMAN. Thank you, Senator, so much. And I would say to all of our members that we would, as a Committee, share this and keep updating it to show every legislative member—535—exactly where we stand. And if we don't start acting, and acting in unity, we are not going to be able to catch up or excel. So I think this is a stark reminder of where we are and this is very accurate, very factual. I think you all would agree that we pulled these out of what you all have looked at, and said this is where they are and this is where we are.

So we want people to understand that. So we will be sharing that without any objections from the Committee, and with that, Senator, we appreciate you coming in and sharing your thoughts.

Senator DURBIN. Thank you.

The CHAIRMAN. At this time, we are going to turn to our panel of witnesses.

We have Ms. Helena Fu, Director of the Office of Critical and Emerging Technologies at the Department of Energy.

We have Dr. Shaun Gleason, who is Director of Science-Security Initiative Integration at Oak Ridge National Laboratory.

We have Dr. Kaushik, Senior Fellow, American Policy Ventures.

And with that, we will start with Ms. Fu.

STATEMENT OF HELENA FU, DIRECTOR, U.S. DEPARTMENT OF ENERGY, OFFICE OF CRITICAL AND EMERGING TECHNOLOGIES

Ms. FU. Thank you so much.

Chairman Manchin, Ranking Member Barrasso, distinguished members of the Committee, thank you for the opportunity to testify about the Department of Energy's leadership in advanced computing research and its application and cybersecurity. I want to start by thanking this Committee for your strong support of DOE for many years. My name is Helena Fu. I serve as the Director of the DOE Office of Critical and Emerging Technologies. My office coordinates across the Department of Energy and its 17 national laboratories in artificial intelligence, biotechnology, microelectronics, and quantum information science.

Since its origins from the Manhattan Project, the entire Department of Energy complex has been working at the frontier of science, driving advances central to America's prosperity and security. Two of the most critical scientific frontiers that we currently face are artificial intelligence and quantum information science. And today, we all see the transformative potential of AI. DOE and its national labs have long invested in AI and its applications, and in addition, DOE is the leading generator of classified and unclassified scientific data through the world's largest collection of scientific experimental facilities. We build and operate, in partnership with industry, the world's fastest and most powerful supercomputers, that are both strategic assets and serve the scientific community. Our proposed Frontiers in AI for Science, Security and Technology initiative, or FASST, seeks to harness this infrastructure at DOE to deliver a step change in capability for the nation, to develop AI-ready data, and to advance the next generation of frontier-scale computing platforms. Building on this data and compute, we need to develop models that deeply understand science, math, physics, and chemistry, and we need to apply these models to solve our most pressing challenges in discovery science, in applied energy, and in national security.

Beyond AI, quantum could help unlock new forms of computing and information processing. And the National Quantum Information Act authorized DOE's five national QIS research centers. DOE is making strides in the science that could help unlock quantum's potential in computing, in simulation, in networking, and in sensing. We have created a first-of-a-kind quantum computing user access program, created testbeds and foundries, and built underground facilities to characterize devices. These investments are helping to build up the quantum ecosystem in the United States, where we are working across 115 institutions, 24 states, with trusted international partners and with other parts of the interagency. DOE is also making strategic investments in quantum computing to address nuclear security challenges, and we are exploring potential applications to our energy mission.

A resilient and secure power grid underpins and enables U.S. leadership in AI and quantum, and DOE is continuing to strengthen the energy sector's cyber defenses and invest in new capabilities, such as the Energy Threat Analysis Center, or ETAC. The ETAC pilot brings experts from government and from industry to-

gether to address the growing cyber threats to U.S. electricity, oil, and natural gas systems. The ETAC pilot has been instrumental in rapidly addressing cyber threats, such as the PRC-sponsored Volt Typhoon activity.

On a solemn note, I would like to recognize the life of Dr. Charlie McMillan, who passed away unexpectedly last week. For 35 years, Charlie worked at Lawrence Livermore National Laboratory and as Director of Los Alamos National Laboratory. He had recently come out of retirement to work with me and our labs on our AI initiative because he saw how important this was. We in the entire DOE community feel this loss keenly, and our hearts go out to Charlie's family and friends.

We are at an inflection point in AI and in quantum and cyber. The DOE, with its dedicated scientific workforce of 40,000 strong, our ability to drive mission science through deep partnerships, and the ability to work across the entire ecosystem, from discovery science to applied energy to national security—we stand ready to do our part. I want to thank the Committee for its ongoing and bipartisan support for the DOE mission, and we look forward to working with all of you. I am happy to answer your questions.

[The prepared statement of Ms. Fu follows:]

Testimony of Helena Fu

Director, Office of Critical and Emerging Technologies

U.S. Department of Energy

Before the

Senate Committee on Energy and Natural Resources

September 12, 2024

Chairman Manchin, Ranking Member Barrasso, and distinguished Members of the Committee, thank you for the opportunity to testify about the Department of Energy's (DOE's) leadership in the next generation of advanced computing research, application, and cybersecurity.

My name is Helena Fu, and I serve as the Director of DOE's Office of Critical and Emerging Technologies (CET). U.S. leadership in critical and emerging technologies such as AI, biotechnology, quantum information science, and microelectronics is key to enabling economic prosperity and maintaining our national security. These technologies are a major source of new discoveries and breakthroughs, strengthen our ability to counter national security threats, and increase access to clean, reliable, and affordable energy.

CET works to leverage capabilities and expertise across the DOE complex, including the NNSA, and the DOE's 17 National Laboratories to sustain and extend U.S. leadership in technology in support of the Department's energy, science, and national security missions. The office has primary responsibility for establishing and coordinating a strategic vision to ensure that the Department is unified and cohesive in executing its works to critical and emerging technologies. CET works with and through other DOE offices, enabling DOE leadership, as well as interagency, congressional, and external partners, to maximize the impact of DOE capabilities and investments in these key areas of national importance.

My testimony will discuss how DOE is advancing the development of the AI innovation ecosystem through its Frontiers in AI for Science, Security, and Technology (FASST) initiative, discuss the work to improve permitting with AI via DOE's VoltAIc initiative, outline the Department's ongoing, foundational efforts in quantum information science, highlight how the Department is leveraging advanced digital technologies and close industry partnerships to protect our energy infrastructure's cybersecurity, and, describe how the Department's work helps secure our national security.

Enhancing Artificial Intelligence Leadership for DOE's Science, Energy and Security Mission

As the Committee well knows, AI is a transformative technology that is evolving almost by the day. It has deep implications for all aspects of the nation's wellbeing, from its economic prosperity to its long-standing scientific leadership. DOE has a key role, together with leading science funding agencies, in ensuring that the United States does not fall behind in the accelerating race to establish global AI supremacy, and we thank Congress for the continued support it has provided to enable DOE's existing infrastructure and capabilities to be harnessed for cutting-edge AI research and development. Over

many years, this foundational work has allowed the Department to prepare revolutionary AI capabilities that our nation now requires more than ever.

- Thanks to DOE's experimental and computational capabilities, which are the world's largest collection of advanced experimental facilities, including particle accelerators and powerful light sources, we are the world's leading producer of **unclassified and classified scientific data** - the fuel that powers important AI models.
- DOE designed, developed, and operates **the world's two fastest supercomputers, with a third also currently being installed.** Some of our supercomputing assets are open and accessible to the U.S. scientific and academic community and industry via our user facilities. They provide a national capability that often supports our agency partners, and are strategic components of our national defensive capabilities.
- DOE has unparalleled experience in **mission-driven public-private collaborations**. Through the Exascale Computing Project (ECP), DOE worked with industry partners to co-design and develop critical components of the computer chips that power today's leading AI models. The ECP also helped deliver the world's first official exascale computing systems that used less than 20 megawatts of power—one tenth of what experts projected at the start of the initiative and a 400% improvement in energy utilization over our pre-exascale systems.
- And we can put all of these assets to work because of our most valuable resource at DOE: the nation's **largest skilled scientific workforce**, with over 40,000 scientists, engineers, researchers, and support personnel at our national laboratories.

DOE is already bringing our capabilities and expertise to bear in supporting the Executive Order on AI, from conducting red teaming, to evaluating the potential for AI to be misused for chemical, biological, radiological, and nuclear threats, to training an AI-ready science and engineering workforce through our National Laboratories, to building AI models to expedite environmental reviews and permitting.

Now we are at a pivotal moment. DOE and its National Laboratories recognize the immense opportunities and risks associated with AI. Other countries, including our adversaries, are already investing significantly to develop strategic national capabilities in AI. The United States must lead the world in the development of advanced AI systems for scientific, energy, and national security applications, and DOE has a critical role to play.

DOE's Frontiers in AI for Science, Security, and Technology initiative - FASST - would leverage DOE's existing capabilities, infrastructure, and partnerships to provide a national AI capability. DOE has the infrastructure needed to support frontier scale AI development for U.S. government capabilities that span from supporting open access scientific discovery to facilitating mission-driven applied energy applications and classified research and development. The National Nuclear Security Administration (NNSA), part of DOE, is uniquely positioned to both advance AI applications and identify and mitigate AI risks to NNSA's nuclear nonproliferation, counterterrorism, and counterproliferation missions. DOE aims to harness and develop AI-ready data, frontier scale compute platforms, and scientific foundation models to solve our most pressing challenges—including control and design of massive and complex systems like the electric grid, enhancing our knowledge of the subsurface for critical mineral development and accelerated modernization of the nuclear deterrent. FASST will also support further investment in improving the energy and water efficiency of AI models.

FASST is an ambitious AI initiative that would provide frontier-scale AI systems to solve critical challenges in science, energy, and national security. This kind of public capability is critical to extend the

United States' competitive edge in scientific innovation, to develop effective AI governance and safety measures, and train an AI-ready workforce. DOE is positioned to address the AI challenge from beginning to end, starting with data and ending with the development and implementation of AI applications for the critical challenges we face as a nation.

Improving Environmental Reviews and Permitting Outcomes

A core investment of the DOE's Frontiers in AI for Science, Security, and Technology initiative – FASST – instructs DOE to use AI to leverage the agency's existing world-class laboratory test facilities to improve siting and accelerate permitting decisions for clean energy deployment. Through strategic facilitation across public-private partnerships, local, state, Tribal, and federal governments, DOE is actively advancing artificial intelligence and machine learning research to improve permitting processes for Administration permitting priorities, such as energy-related projects and critical mineral infrastructure. Deploying our existing lab infrastructure and scientific expertise for AI instead of starting from scratch will reduce lengthy, time-consuming, and resource-intensive application processes. Public and private-sector clean energy investments depend on predictable project timelines and decision making.

When it comes to permitting, the Department is advancing a number of reforms and investments to help improve and accelerate permitting processes. Companies are investing hundreds of billions of dollars in manufacturing, clean energy, and infrastructure projects across America. To take advantage of this momentum, we need to improve the ways projects are sited and permitted at all levels. This moment demands efficiency without compromising environmental or community outcomes. In April, DOE announced the VoltAIc initiative to use AI to help expedite and improve siting and permitting at the Federal, state, and local level. As part of that initiative, DOE is building AI-powered tools to improve siting and permitting of clean energy infrastructure. For example, we are developing PolicyAI, a policy-specific large language model test bed that will be used to develop software to augment NEPA and related reviews. The PolicyAI research team is investigating potential uses of AI in the NEPA and permitting process, including extracting and organizing unstructured data, natural language processing, analyzing structured data to identify key performance indicators, and comment analysis and categorization.

Reauthorization of National Quantum Initiative to advance Quantum Information Science

While we are looking over the horizon toward the deployment of next-generation AI capabilities, the Department has already been pushing the boundaries of critical technology areas that our nation needs to maintain its strategic global position. Quantum Information Science (QIS) is one important area in which the Department has already invested significant resources and made correspondingly significant strides. The core of QIS uses the laws of quantum mechanics to store, transmit, manipulate, compute, and measure information. QIS could unlock forms of computing and information processing that can overcome the limitations of "classical" approaches by utilizing exotic quantum effects. Advances may help solve problems that are hard to address with even the largest supercomputers of today, enable extremely secure encryption, and could aid in understanding everything from biological systems to the nature of dark matter.

Recognizing the great potential of QIS, and aware of the growing international competition in this promising new area of science and technology, Congress passed the National Quantum Initiative Act (NQI Act), which became law in December 2018. The DOE Office of Science is a leading partner in the

National Quantum Initiative alongside other departments and agencies, and launched a range of programs in QIS. Research projects range from single investigators within specific disciplines to large integrated centers that span the Office of Science programs. QIS holds the potential to dramatically advance aspects of DOE's mission, and a major driver of DOE's quantum strategy in recent years has been the National Quantum Initiative Act.

The NQI Act authorized DOE to carry out a basic research program in QIS and DOE's Office of Science to establish and operate 2-5 National Quantum Information Science Research Centers to "conduct basic research to accelerate scientific breakthroughs in quantum information science and technology." In FY 2020, DOE's Office of Science established five National QIS Research Centers as called for in the NQI Act. These centers focus on accelerating transformational advances in basic science and quantum-based technology needed for world-leading capabilities in QIS. The National QIS Research Centers are led by five of the DOE National Labs and currently combine the expertise and resources of over 87 academic, industry, non-profit, and lab partners from 24 states, the District of Columbia, Canada, Italy, and the United Kingdom.

The National QIS Research Centers program, an investment of $575 million over five years, is co-designing algorithms, quantum devices, and engineering solutions to deliver quantum advantage in scientific applications; overcoming roadblocks in quantum state resilience, controllability, and scalability of quantum technologies; eliminating the decoherence mechanisms in superconducting 2D and 3D devices; and reducing limitations of today's Noisy Intermediate-Scale Quantum Computer systems.

The Centers have accomplished much since their inception in 2020, from establishing quantum foundries for advanced device fabrication, building underground facilities for characterizing quantum devices, developing highly successful open-source control-software, advancing innovative superconducting devices to improving the precision of critical atomic clocks.

Although the original authorization provided funding only through 2023, the Office of Science has continued to receive sufficient appropriations to support the current Centers. We will continue to fund this research, subject to appropriations, through the end of FY 2025.

At the same time, the National Nuclear Security Administration is also investing in mission-relevant quantum technologies. The Advanced Simulation and Computing (ASC) program at NNSA is making strategic investments in quantum computing to drive innovative computing designs that leverage new opportunities in the high-performance computing industry. One of ASC's guiding principles is to collaborate with vendors in co-design of all forms of computing technologies to benefit from innovation in the private sector. ASC is focused on accelerating the availability and increasing the scalability of advanced technologies in industry, with the goal of deploying quantum systems for its most demanding and complex national security challenges.

DOE is also working with other partners within the federal government. This summer, DOE and the Defense Advanced Research Projects Agency (DARPA) announced a Memorandum of Understanding to advance the field of quantum computing. The MOU establishes a framework for planning and coordinating future research, development, engineering, and test and evaluation activities related to quantum computing. Part of that work will include deep analysis of the current status of quantum computing and where it is going.

DOE continues to drive advances in quantum research and development and to explore and better understand the potential applications of QIS to all aspects of the Department's science, applied energy, and national security missions.

Advances in Computing and Impacts on Cybersecurity

While advances in computing have many beneficial uses, they may also be leveraged by those with malicious intent to disrupt systems that we all rely on every day, such as the country's energy infrastructure. The energy sector provides the power and fuel that all other U.S. critical infrastructure sectors depend on to operate. Any disruption in the energy system would have a devastating impact to national security, the U.S. economy, and the safety and livelihoods of millions of Americans.

At DOE, the Office of Cybersecurity, Energy Security, and Emergency Response (CESER) is focused on securing the Nation's energy infrastructure against all hazards, reducing the risks and impacts of cyberattacks, physical incidents and other disruptive events, and supporting state, local, tribal, and territorial governments, as well as industry, with response and restoration when a disruption occurs.

DOE is continuing to strengthen the energy sector's cyber defenses, invest in new capabilities, and reimagine how we think about cybersecurity to ensure the resilience of the nation's critical energy infrastructure. This includes enhancing cyber threat collaboration, such as through the DOE pilot of the Energy Threat Analysis Center (ETAC), which brings experts from government and industry together to analyze and address the growing cyber threats to U.S. electricity, oil, and natural gas systems.

Given that much of the nation's energy infrastructure is privately owned, meeting the shared responsibility to address threats to the sector requires government and industry to work together. The ETAC has been instrumental in addressing cyber threats, such as the PRC-sponsored Volt Typhoon activity, and other threats targeting our energy infrastructure. In addition to the private sector partnerships, we are leveraging the analytic capabilities, compute resources, and subject matter expertise of five DOE national laboratories. It will take the whole of the sector coming together to address the cyber threats that exist today, and those on the horizon.

In addition to the ETAC, DOE is prioritizing activities to harden current and future energy infrastructure. We are partnering with manufacturers to strengthen the cybersecurity of critical components in the grid and driving a paradigm shift in cybersecurity through the development of Cyber-Informed Engineering principles, and promulgating them through implementation guides. The principles set expectations for manufacturers from ideation to deployment. Most notably, the principles present a shared responsibility model by identifying the distinct roles of both suppliers and end users in meeting cybersecurity objectives. For example, supplier principles of secure development, continuous lifecycle support, and proactive vulnerability management are complemented by end user responsibilities to follow supplier guidance for secure implementation and hardening and sufficiently plan for maintenance and refresh cycles.

DOE is adept at deploying innovative solutions to complex problems and will continue to do so in service to the American people, ensuring the U.S. energy sector becomes only more secure and resilient with time.

Conclusion

As technology advances and evolves at an unprecedented pace, we appreciate the committee's steadfast work to provide the Department of Energy with the authorizations and resources we require to maintain national leadership in critical scientific and technological sectors. The scope of this challenge grows by the day, as illustrated by this hearing itself, which spans from advancing next generation AI technologies to guarding against cybersecurity threats to our energy infrastructure. The Department also knows our adversaries and competitors have an interest in stealing and undermining our pathbreaking progress on these topics. We collaborate closely across the Department on a daily basis to identify and minimize these concerns. However diverse our mission, the Department of Energy is meeting it head-on with a cohesive vision that centers on the following principles:

- **In-house technical capabilities for the national interest:** In order to understand, accelerate, and govern today's technological advancements, our government must have internal capabilities that respond to national imperatives first and foremost. Our Department, alongside our agency partners, is tasked with maintaining national security, including economic security; we cannot rely on external actors to assure our nation's energy resilience, scientific leadership, and strategic deterrence. As we execute on these missions, we simply *must* have the latest tools and brightest experts to maintain critical capabilities.

- **Dedicated and targeted public-private partnerships:** America's global leadership hinges on the strength and ingenuity of its private sector and innovation from academia. As we build internal capabilities, we must actively leverage our interagency and industrial partners and their advancements. For example, industry grounds our capabilities and strategic vision in today's rapidly changing world. That's why ETAC's technical analysts from industry and government physically sit shoulder-to-shoulder – we cannot have even small blind spots when protecting assets as critical as our electrical grid or petrochemical infrastructure. Under the National Quantum Initiative, DOE and the national labs operate the National QIS Research Centers in close partnership with industry and academia. As AI models continue to advance in their ability to reason, DOE has the scientific workforce and the scientific infrastructure to enable the development and application of AI to solve the critical national challenges at speed and at scale. Public-private partnerships are foundational to these programs, and we are eager to continue engaging with our industry partners to best accomplish the Department's diverse missions.

- **Close coordination with the interagency:** Advancing the nation's scientific and technological leadership inherently requires a whole-of-government approach. Each of the three bills establishes programs that are complementary to others across the interagency and include mechanisms to ensure coordination. For example, FASST will naturally enhance efforts in support of the Department of Commerce's AI Safety Institute's AI standardization and governance efforts, leveraging the national lab network to provide the requisite AI resources and an independent ability to detect inflection points in model capabilities. Similarly, ETAC is just one part of much larger cybersecurity apparatus distributed across the U.S. government and is built from the ground up to enhance this larger mission, leveraging actionable intelligence from across the government to better protect the nation's energy resilience and security.

The Office of Critical and Emerging Technologies and the whole of the DOE stand ready to ensure that the Department rises to the challenges posed by today's strategic technology landscape.

I want to again thank the Committee for its ongoing and bipartisan support for the DOE mission. Thank you for the opportunity to be here today, and we look forward to working with the Committee on these important issues. I am happy to answer your questions.

The CHAIRMAN. Thank you, Ms. Fu.
And now we have Dr. Gleason.

STATEMENT OF DR. SHAUN GLEASON, DIRECTOR OF SCIENCE-SECURITY INITIATIVE INTEGRATION, OAK RIDGE NATIONAL LABORATORY, OFFICE OF THE LABORATORY DIRECTOR

Dr. GLEASON. Chairman Manchin, Ranking Member Barrasso, and members of the Committee, thank you for the opportunity to speak with you today. My name is Shaun Gleason. I am currently the Director of the Science-Security Initiative Integration at the U.S. Department of Energy's Oak Ridge National Laboratory (ORNL) in Oak Ridge, Tennessee, where I have 35 years of service. I serve as a liaison between the open science and national security mission communities and I am specifically focused on emerging technologies, such as artificial intelligence, quantum science, cybersecurity, and high-performance computing across the diverse mission areas of ORNL. I am also an entrepreneur who founded a startup company that successfully transitioned a medical imaging technology to the market.

There are grand challenges where we must accelerate progress to ensure continued U.S. leadership in the emerging technologies of quantum, cyber, and AI. For example, in AI, energy efficiency is a grand challenge, as many are predicting that energy use by AI-driven data centers will approach ten percent of U.S. energy demand by 2030. While energy-efficient AI is crucial, we also need our AI systems to be safe, secure, and trustworthy. For quantum, a primary grand challenge is the ability to create reliable and affordable quantum devices that are the building blocks for quantum computers. Another grand challenge is creating a quantum internet that can reliably and securely share quantum information with many different devices over long distances. Cybersecurity is a grand challenge arms race where every defensive move inspires an adversary's offensive move and vice versa. Protecting U.S. critical infrastructure, such as the electric grid, from cyberattacks requires regional, public-private partnerships and real-world cyber testbeds that are connected to a national information coordination network.

Some of the most exciting and critical areas for revolutionary innovations are where the fields of AI, cybersecurity, and quantum intersect with one another. In the fields of cybersecurity and AI, AI is being used to create dynamic, self-learning cyber-defense tools that can adapt to the rapidly changing cyberattacks against our nation's infrastructure. AI systems themselves are uniquely vulnerable to a variety of cyberattacks that can manipulate AI into making decisions favorable to an adversary. Adversaries can create public websites filled with disinformation that are automatically scraped for data that can bias an AI model during training. To combat cyberattacks on AI systems, several of the DOE national labs, including ORNL, Los Alamos, Pacific Northwest, and Lawrence Livermore, have created internal organizations to develop cybersecurity methods specifically for the defense of AI systems.

The discoveries being made at the intersection of AI and quantum are also powerful, and the scientific community is only scratching the surface. For example, AI is being leveraged to accelerate the development of quantum computers by accelerating the

discovery of new quantum materials and generating new types of error-correcting codes for quantum computers. Conversely, quantum computers are being used to speed up AI model training algorithms and to generate realistic simulated data that can be used to train data-hungry AI models. Additional research is needed to capitalize on these opportunities.

DOE's national laboratories are also home to powerful experimental facilities that are made available to universities, industry, and other government agencies to conduct cutting-edge research. Thanks to investments by Congress through DOE's Office of Science and the National Nuclear Security Administration, the national labs have deployed the first open science exascale computers—Frontier at Oak Ridge National Lab, Aurora at Argonne, and later this year, El Capitan at Lawrence Livermore.

The combination of world-class talent, computing, and experimental facilities positions DOE to lead in AI, quantum, and cybersecurity research. Exemplifying the value of partnerships in quantum, ORNL is currently performing quantum-based secure communication experiments in collaboration with the electric power board in Chattanooga and the University of Tennessee in Chattanooga on their commercial quantum network. To maintain U.S. leadership in AI, public-private partnerships are also critical. For example, ORNL recently partnered with Advanced Micro Devices and Microsoft to develop software that can train a one trillion parameter AI model on the Frontier supercomputer.

In summary, the grand challenges before us motivate partnerships across the government, the DOE national laboratory system, industry, and academia to accelerate the pace of innovation. DOE has demonstrated its commitment to advancing research and technology transitions across all three of these important areas while trying to balance associated risks. Thank you once again for the opportunity to testify, and I welcome any questions you have on these important topics.

[The prepared statement of Dr. Gleason follows:]

Dr. Shaun Gleason
Director, Science-Security Initiative Integration
Oak Ridge National Laboratory

Testimony of Dr. Shaun Gleason
Director, Science-Security Initiative Integration
Oak Ridge National Laboratory
Before the
U.S. Senate Committee on Energy and Natural Resources
September 12, 2024

Hearing on "Department of Energy's Leadership in the Next Generation of Advanced Computing Research, Application, and Security"

Chairman Manchin, Ranking Member Barrasso, and Members of the Committee: Thank you for the opportunity to speak with you today. My name is Shaun Gleason. I am the Director of Science-Security Initiative Integration at the U.S. Department of Energy's (DOE's) Oak Ridge National Laboratory (ORNL) in Oak Ridge, Tennessee. I serve as a liaison between the open science and national security mission communities at ORNL. I am specifically focused on advancing emerging technologies such as artificial intelligence (AI), quantum science and technology, and advanced computing across the diverse mission areas of ORNL. I have been at ORNL for 35 years, and my research background is in electrical engineering with a focus on data processing, machine learning, and advanced computing platforms. I have previously served as the interim associate laboratory director for Computing and Computational Sciences and as the director of two research divisions at ORNL for which I was responsible for leading science and engineering capabilities that include quantum, AI, advanced computing, and cybersecurity for critical infrastructure. One of my director roles was entirely focused on cybersecurity for the national security mission and included sponsors such as DOE, the Department of Defense (DOD), the Department of Homeland Security (DHS), and the Intelligence Community (IC). Finally, I am an entrepreneur who founded a startup company that successfully transitioned a medical imaging technology to the market.

As an introduction to my testimony, I am not here to provide opinions on legislation or policy but rather am here to share my technical expertise relevant to the subject of this hearing and how the DOE national labs, and ORNL in particular, provide national leadership. The views I present to you are my own and have been formed by my career as a researcher, engineer, entrepreneur, and technical leader. First, I will outline a few grand research challenges in AI, quantum, and cybersecurity that hopefully will motivate continued investment by Congress to advance the frontiers of science and innovation. Second, I will describe how cybersecurity, AI, and quantum science overlap and intersect and will present some research opportunities that exist at the crossroads of these technologies. Finally, I will emphasize how national labs are uniquely equipped

to push the boundaries of innovation and the importance of government, academic, and industry partnerships to accelerate science, innovation, technology transfer, and workforce development.

Grand Challenges

Some grand challenges require us to accelerate progress immediately to ensure continued U.S. leadership in the emerging technologies of quantum, cyber, and AI. Our economic, energy, and national security *require* that we continue to invest and innovate to solve the grand challenges across these three fields.

For AI, improving energy efficiency is an imperative, because many experts are predicting that energy use by AI-driven data centers will approach 10% of total U.S. energy demand by 2030. Other reports predict that AI will contribute to reduced energy needs, by enabling improvements such as more intelligent and efficient grid operation. [“AI and energy: Will AI help reduce emissions or increase demand? Here’s what to know,” World Economic Forum, July 2024, https://www.weforum.org/agenda/2024/07/generative-ai-energy-emissions/]. Either way, we must develop and deploy new hardware technologies such as quantum and neuromorphic AI coprocessors that have potential to solve AI computational problems with a much-reduced energy footprint. Energy efficiency is also critical for deploying AI “at the edge” for remote scientific experiments, grid control endpoints, and national security missions in areas where power sources are severely limited and/or unreliable. We need not only new hardware platforms but also new algorithms, software, and computational workflows that are more energy efficient. Another grand challenge in AI is the development of AI systems that are safe, secure from cyberattacks, and privacy-preserving (i.e., they preserve the privacy of sensitive data used to train the AI model). Addressing these and other grand challenges in AI will help the U.S. maintain leadership and strengthen our economic and national security.

For quantum, the potential positive impact is transformative, and the grand challenges are numerous. A primary challenge is the ability to create reliable, accessible, and affordable quantum devices such as quantum sensors and qubits for quantum computers. Creating such quantum devices requires basic R&D in physics and materials science, quantum engineering (the ability to turn a quantum material into a functional device), and, finally, manufacturability—so that these devices can be made reliably and affordably in large quantities. Solving this grand challenge will drive a second grand challenge of creating a large-scale (1,000+ qubit), fault-tolerant quantum computer that can solve real-world problems unsolvable by classical HPC systems. Examples include complex optimization problems in physics, chemistry, medicine, and logistics. Part of the grand challenge in quantum computing is the integration of classical high-performance computing (HPC) with quantum computers functioning as

coprocessors suited for quantum computation. Such hybrid classical-quantum computers must be easily programmed to solve important problems. A third grand challenge is quantum networking, which requires a new type of network that can reliably share quantum information across many different quantum devices (e.g., quantum computers, sensors, and photon sources) over long distances (hundreds of kilometers). Some refer to this as the "quantum internet." One key to solving this grand challenge is transduction, which is a method of reliably sharing different forms of quantum information with other devices on the quantum network.

Clearly, many grand challenges exist in the cybersecurity field. Cybersecurity is an "arms race" where every defensive move inspires an adversary's offensive move, and vice versa. The U.S. needs a revolutionary leap in AI-driven, adaptive cybersecurity to propel our cyber defenses out of reach of adversaries for both information technology (IT) and operational technology (OT) systems. OT systems are collections of components such as networks, computers, control systems, and sensors that provide supervisory control and data acquisition, process monitoring, and communication for critical infrastructures such as the electric grid, oil and natural gas systems, water treatment plants, and manufacturing systems. All of these systems provide essential and, often, lifesaving services. As an example, the U.S. electric grid is arguably the largest and most complex machine in the world, with approximately 60 million transformers of roughly 80,000 different types, 70,000 substations, and 5.5 million miles of distribution lines. [AI for Energy: Opportunities for a Modern Grid and Clean Energy Economy, DOE, April 2024, https://www.energy.gov/cet/articles/ai-energy] The OT system for the U.S. grid is a mix of both decades-old hardware and software components and brand new, "smart" Internet of Things devices, which increase the cyberattack surface of the electric grid. Compared with IT systems, there is little commonality in the operating systems and chip sets used across different OT systems manufacturers, which creates cybersecurity challenges. Regional variations across the U.S. such as the type of OT equipment used, mixes of distributed energy resources (nuclear, wind, solar, hydro, coal, etc.), population density and growth patterns, geographical differences, and weather extremes preclude the implementation of a uniform, nationwide approach to securing the grid. As such, solving this grand challenge requires regional partnerships and testbeds connected to a national cybersecurity coordination network.

Research Opportunities at the Intersection of Cybersecurity, AI, and Quantum

AI, cyber, and quantum are all broad research areas, and many advances are occurring rapidly within each individual field. Some of the most exciting areas for revolutionary innovations are where they intersect with one another.

For example, if we consider the fields of cybersecurity and AI, AI is being used to create dynamic, self-learning cyber defense tools that are equipped to adapt to rapidly changing cyberattacks against our nation's critical infrastructure. As an example, ORNL has built a Cyber Operations Research Range that employs HPC to help the U.S. Navy evaluate the effectiveness of commercially available AI-based cyber defense tools before they spend precious resources to acquire them. On the flip side, generative AI is being used to rapidly create volumes of never-before-seen instances of malware and ransomware, some of which can penetrate the best deployed cyber defense tools. To illustrate this point, ORNL demonstrated that AI could be used to modify existing malicious software (malware) so that it penetrated the latest commercially available AI-based cyber defense products approximately 80% of the time. This result was shared with vendors so they could work on improving their AI-based cyber defense tools. Finally, AI systems are uniquely vulnerable to specific cyberattacks, some of which manipulate the AI system into making decisions favorable to an adversary by "poisoning" the training dataset. An example of this would be creating data-rich websites that are automatically scraped for data used to train an AI model but that contain disinformation that biases the model. Other AI system attacks can enable an adversary to steal the sensitive data (e.g., personally identifiable information) used to train an AI model. A different type of attack attempts to fool the AI model into making a decision that is favorable to the adversary. As a simple example, an adversary could paint a special pattern on a military vehicle that fools an AI system into thinking it is a civilian vehicle. To combat these types of cyberattacks on AI systems, several of the DOE national labs have created organizations that are developing cybersecurity capabilities specifically for AI systems. These include ORNL's Center for AI Security Research (CAISER), Los Alamos National Laboratory's AI Risks and Threat Assessments Group (AIRTAG), Pacific Northwest National Laboratory's Center for AI, and Lawrence Livermore National Laboratory's (LLNL's) Resilient AI for National Security (RAINS) center. These organizations provide DOE-stewarded capabilities for the mission of other agencies outside of DOE, including DOD, DHS, and the IC.

Next, if we explore the intersection between the fields of AI and quantum science and technology, AI is being leveraged to accelerate discovery of new quantum materials, hypothesize new quantum computer designs, and generate new types of error correcting codes for quantum systems, all of which are needed to accelerate the development of the next generation of quantum computers. Conversely, quantum computers are being used to speed up machine learning training algorithms to enable deployment of fast, energy-efficient quantum coprocessors that can train and evaluate large AI models more efficiently than a classical HPC system. Quantum computers can also generate realistic simulated data that can be used to train data-hungry AI foundation models. For example, quantum computers can simulate molecular

interactions and generate vast amounts of training data to train AI models for new materials discovery. The discoveries being made at the intersection of the fields of AI and quantum are powerful, and the scientific community has just begun to scratch the surface.

At the intersection of the fields of quantum and cybersecurity, many academic and national lab research institutions are developing post-quantum cryptography methods that result in encryption methods that will be unbreakable by future quantum computers. These new approaches are critical because future quantum computers are predicted to be able to break the classical encryption methods used ubiquitously in our everyday lives, including those in our computers and smart phones. After eight years of collaboration among cryptography experts around the world, the National Institute of Standards and Technology just released the first three finalized post-quantum encryption standards. [https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards]

DOE's Unique Capabilities and Critical Partnerships

The final topic of my testimony covers the unique role that DOE plays and the importance of government, national laboratory, academic, and industry partnerships to accelerate innovation and technology transition across cybersecurity, AI, and quantum. The DOE national laboratory system is uniquely positioned to solve the grand challenges and advance science and innovation at the intersections of each of these emerging technologies. The national labs employ the largest multidisciplinary scientific workforce in the nation with approximately 70,000 employees. I often share with my family and professional colleagues that I can find a scientist at ORNL with deep technical expertise in every scientific area of interest including AI, cybersecurity, and quantum. This scientific depth is magnified when you consider the scientific talent across the entire DOE laboratory system. Therefore, the labs are uniquely equipped to innovate at the intersections of these three fields.

DOE's national laboratories are also home to large and extremely powerful experimental facilities that the labs make available to universities, industry, and other government agencies to conduct cutting-edge research. Thanks to investments by Congress through DOE's Office of Science and the National Nuclear Security Administration, these user facilities, stewarded by the national laboratory system, are the most unique and powerful experimental facilities in the U.S. They include exascale supercomputers—Frontier at ORNL, Aurora at Argonne National Laboratory (ANL), and, later this year, El Capitan at LLNL—that can be used to train and test the largest AI foundation models. The national lab system is also home to several of the world's most powerful tools for studying materials, including the Linac Coherent Light Source at SLAC National Accelerator Laboratory, Spallation Neutron Source at ORNL, National

Synchrotron Light Source-II at Brookhaven National Laboratory, and Advanced Photon Source at ANL, all of which can generate uniquely valuable data to train AI models targeted for new materials discovery. The combination of world-class talent, high-performance computation, and data-generating facilities enables DOE to foster revolutionary discoveries at the intersections of AI, cybersecurity, and quantum.

Another advantage of national lab engagement in development of these emerging technologies is that DOE and its national labs have policies, procedures, tools, and infrastructure that provide layers of security enabling both classified and unclassified research on sensitive, critical, and emerging technologies. We cannot maintain U.S. leadership in fields such as AI, quantum, and cybersecurity without training our domestic workforce and leveraging the talent that exists outside the U.S., and DOE and its laboratories also take careful measures to reduce risk and protect investments in these technologies.

As an entrepreneur, I know firsthand the importance of creating and sustaining an innovation pipeline that starts with funding for fundamental R&D for new discovery, followed by industry-informed R&D to build deployable systems, followed by technology transfer and commercialization for market impact. New science and technology cannot effectively move through the pipeline without deep, mutually beneficial partnerships.

As an example of enabling partnerships in the quantum field, ORNL is performing quantum-based secure communication experiments in collaboration with the Electric Power Board of Chattanooga, the University of Tennessee at Chattanooga, and Qubitekk, Inc., a quantum networking company in California. The goal is to develop resilient quantum network communication in the presence of real-world interference sources such as wind, temperature variations, and vibration. We are leveraging the optical fiber in the EPB commercial quantum network deployed in Chattanooga. DOE's Office of Advanced Scientific Computing Research (ASCR) is investing in R&D for quantum networking at several of its national labs, including Fermi National Accelerator Laboratory, ORNL, and ANL. On the quantum computing front, ORNL is partnering with U.S.-based quantum computing companies through the ASCR-supported Quantum Computing User Program (QCUP). A goal of QCUP is to learn to integrate classical leadership computing systems such as Frontier with commercial quantum computers to enable hybrid classical-quantum computers of the future that can solve complex problems faster and with less energy demand. On a related note, Quantum Brilliance, Inc., just announced a new partnership with ORNL to deploy one of its new quantum computers in our datacenter, enabling additional research for hybrid classical-quantum computing. [https://www.hpcwire.com/off-the-wire/quantum-brilliance-partners-with-ornl-to-integrate-diamond-quantum-computing-into-hpc-systems/] These types of deep partnerships and the ability to deploy large-scale infrastructure to solve challenges are a strength of the national labs. Finally, DOE's five National Quantum Information Science

Research Centers are driving innovations in quantum computing, communication, sensing, and materials, and these centers include partnerships among 115 institutions across North America and Europe. [https://nqisrc.org/]

To maintain U.S. leadership in AI, partnerships among government, national labs, industry, and academia are also critical. DOE labs and industry each have unique and essential ingredients to accelerate AI innovation and transition into practice in a safe, secure, and trustworthy manner. DOE has world-leading facilities for HPC, unique data-generating experimental facilities, deep subject-matter expertise in science and energy, and access to classified national security challenges and associated classified datasets. On the other hand, industry is exponentially investing in rapid, agile, and innovative development of AI hardware and software. Hence, a tight partnership between DOE and industry is important to maintain U.S. leadership in AI for scientific discovery, energy innovation, and national security. Finally, AI workforce development is essential on several fronts, including development of AI researchers who work at the bleeding edge of AI innovation; AI practitioners who leverage and transition new AI tools effectively for their domain of expertise; and AI system engineers who install, maintain, and secure operational AI systems. Our university partners play an essential role in educating the next generation of AI talent and partnering with industry and national labs to provide students with internships and fellowships where they can put their AI education into practice in the laboratory and real-world systems.

An example of a public-private partnership advancing the cybersecurity of OT systems components for the electric grid is the Cyber Testing of Resilient Industrial Control Systems (CyTRICS), funded by DOE's Office of Cybersecurity, Energy Security, and Emergency Response (CESER). The CyTRICS mission is "protecting the nation's critical energy assets through cybersecurity vulnerability testing, forensic analysis, and subcomponent enumeration." [https://cytrics.inl.gov/] The CyTRICS partnership includes six national labs, led by Idaho National Laboratory (INL), and six industry partners providing OT equipment for the energy industry. CyTRICS is effective at identifying complex cyber vulnerabilities in OT equipment because of this close partnership between labs and industry. Additionally, CESER is supporting regional cybersecurity partnerships such as Auburn University's Southeast Region Cybersecurity Collaboration Center on which ORNL is a key partner. Additional regional partnerships are needed across the U.S. along with corresponding regional electric grid cyber testbeds such as those deployed at INL that enable rigorous R&D and testing of the latest cyber threats to our critical infrastructure. Regional cybersecurity partnerships across the U.S. that coordinate with one another and are also connected via a national cybersecurity coordination network will be a powerful way to mitigate cyberattacks against our electric grid. A current example of a recently launched national cybersecurity coordination network is the Energy Threat Assessment Center (ETAC) in Denver, Colorado, a

CESER-funded government-industry partnership. Tying this cybersecurity theme back to AI and quantum, we need to develop AI-driven, dynamic cyber defenses that can learn and adapt faster than our adversaries can, as well as cyber-impenetrable quantum networks focused on the unique regional needs of the electric grid across the country.

In summary, the cross-disciplinary nature of AI, quantum, and cybersecurity and the associated grand challenges before us motivate partnerships across the government, the DOE national laboratory system, industry, and academia to accelerate the pace of innovation. DOE has demonstrated its commitment to advancing basic and applied research and technology transition across all three of these important technology areas, and DOE can effectively balance the revolutionary opportunities that will come from advancement across these emerging technologies while balancing the associated risks.

Thank you once again for the opportunity to testify, and I welcome any questions you may have on these important topics.

The CHAIRMAN. Thank you, Doctor.
And now we have Dr. Kaushik.

STATEMENT OF DR. DIVYANSH KAUSHIK,
SENIOR FELLOW, AMERICAN POLICY VENTURES

Dr. KAUSHIK. Chairman Manchin, Ranking Member Barrasso, and distinguished members of the Committee, thank you for the opportunity to testify today.

We are at a critical juncture in technological history. The People's Republic of China, the PRC, is in an intense competition with the United States, aiming to dominate advanced computing and AI by 2030. Over the past seven years, they have increased their R&D budgets by ten percent annually while engaging in sophisticated espionage efforts to acquire technology. This is not just economic competition, it is a strategic effort to reshape the global order. The Department of Energy and its network of 17 national laboratories and 35 user facilities are our technological vanguard. These institutions have consistently delivered innovations underpinning American leadership, from clean rooms to platforms driving key industries today. The DOE labs' potential to drive AI innovation is enormous, with applications for national security, energy, and scientific advancement. These breakthroughs powered by DOE's supercomputing capabilities could revolutionize areas like material sciences, molecular dynamics, and power grid resilience.

This necessitates a multifaceted approach. We must enhance the security of our national lab facilities. We must maximize their operational and scientific capabilities and we must implement strategic initiatives to attract and retain the talent that wants to come here while removing those who seek to exploit our system. We must foster an environment where our scientists and engineers are encouraged to think big, push the boundaries of innovation, and be confident that their groundbreaking research is safeguarded against foreign exploitation.

The PRC has explicitly held up U.S. national laboratories as models to emulate in their five-year plans. Stating in their 13th five-year plan, and I quote: "National laboratories have become key platforms for major developed countries to seize the high ground in technological innovation. For instance, the Argonne, Los Alamos, and Lawrence Berkeley National Laboratories in the United States are all research bases focused on national missions. It is urgently needed to focus on national goals and strategic needs, target international technological frontiers, and establish a group of larger-scale interdisciplinary and integrative national laboratories." This is a direct quote from their five-year plan. Xi Jinping has since announced the creation of their own national laboratories that are explicitly designed to mimic and ultimately surpass our DOE complex. While imitation may be the sincerest form of flattery, in this context, it serves as a stark reminder of the value and the vulnerability of our national laboratories. The PRC's efforts to surpass our labs and capitalize on their advancements highlights the pressing need for a comprehensive approach to research security that preserves our competitive edge.

The bottom line is that the PRC is pursuing an aggressive campaign of technological advancement that relies on both aggressively

investing in their own R&D ecosystem and illicitly acquiring intellectual property. Furthermore, their strategy integrates civilian research with military applications, as evidenced by statements from top Chinese academic institutions, including Tsinghua University, commonly referred to as their MIT. This goes beyond normal competition. It represents a coordinated effort to challenge America's innovation leadership and reshape the global technological landscape in Beijing's authoritarian image.

The PRC's legal framework further complicates this picture. Laws such as the 2017 National Intelligence Law compel Chinese citizens and organizations to "support, assist, and cooperate with state intelligence work." This means that even well-intentioned PRC researchers may be legally obligated to share information with their government, regardless of any commitments made to U.S. institutions. Let me be clear, research security is not about stifling innovation or closing our doors to the world. It is not about—and cannot be about—targeting individuals based on their ethnicity. It is simply about ensuring that our openness is not exploited to our detriment by our adversaries. The DOE's national laboratories have long been a shining beacon for scientists and researchers worldwide. This is an asymmetric advantage that we have.

This global appeal is not just a point of pride, it is a cornerstone of our technological leadership. For instance, 59 percent of top-tier AI researchers work in the United States, but only about 20 percent of them got their undergraduate degrees here. Our nation's commitment to freedom, to free speech, to freedom of inquiry, innovation, and scientific excellence has made us the destination of choice for the world's brightest minds. We can and must maintain our leadership in scientific collaboration, but on terms that protect our national interests. We passed several laws. Effective implementation of these remains key, whether it be the research security provisions in CHIPS or in NSPM–33.

The path that I have laid out today is undoubtedly challenging and will require sustained commitment and vigilant oversight. However, the alternative—a world where the PRC dictates the rules for transformative technologies—is simply not an option that we can entertain. There is much more that I could say on these matters, but I trust that we will cover them more fully over the course of this hearing. Thank you for the opportunity to testify. I look forward to your questions.

[The prepared statement of Dr. Kaushik follows:]

Written Testimony of Dr. Divyansh Kaushik
Senior Fellow, American Policy Ventures
Submitted to the Committee on Energy and Natural Resources
United States Senate
for the Hearing to Examine the Department of Energy's Role in Advanced Computing Research

Opening Statement

Chairman Manchin, Ranking Member Barrasso, and distinguished members of the Committee, thank you for the opportunity to testify today.

We are at a critical juncture in technological history. The People's Republic of China (PRC) is in intense competition with the United States, aiming to dominate advanced computing and AI by 2030. Over the past seven years, they have increased their R&D budgets by 10% annually while engaging in sophisticated espionage to acquire technology. This is not just economic competition but a strategic effort to reshape the global order.

The Department of Energy (DOE) and its network of 17 national laboratories and 35 user facilities are our technological vanguard. These institutions have consistently delivered innovations underpinning American leadership, from clean rooms to platforms powering key industries. The DOE labs' potential to drive AI innovation is enormous, with applications for national security, energy, and scientific advancement. These breakthroughs, powered by DOE's supercomputing capabilities, could revolutionize areas like material sciences, molecular dynamics and power grid resilience.

This necessitates a multifaceted approach: enhancing the security of our national lab facilities, maximizing their operational and scientific capabilities, and implementing strategic initiatives to attract and retain the world's most brilliant minds while removing those who seek to exploit our system. We must foster an environment where our scientists and engineers are encouraged to think big, push the boundaries of innovation, and be confident that their groundbreaking work is safeguarded against foreign exploitation.

The PRC has explicitly held up U.S. national laboratories as models to emulate in their five-year plans, stating in their 13th Five-Year Plan: "National laboratories have become key platforms for major developed countries to seize the high ground in technological innovation. For instance, the Argonne, Los Alamos, and Lawrence Berkeley National Laboratories in the United States … are all research bases focused on national missions. It is urgently needed to focus on national goals and strategic needs, target international technological frontiers, and establish a group of larger-scale, interdisciplinary, and integrative national laboratories."

Xi Jinping has since announced the creation of their own national laboratories that are explicitly designed to mimic and ultimately surpass our DOE complex. While imitation may be the sincerest form of flattery,

in this context, it serves as a stark reminder of the value and vulnerability of our national laboratories. The PRC's efforts to surpass our labs and capitalize on their advancements highlight the pressing need for a comprehensive approach to research security that preserves our competitive edge.

The bottom line is that the PRC is pursuing an aggressive campaign of technological advancement that relies on both aggressively investing in their own R&D capabilities and illicitly acquiring intellectual property. Furthermore, their strategy integrates civilian research with military applications, as evidenced by statements from top Chinese academic institutions. This goes beyond normal competition; it represents a coordinated effort to challenge America's innovation leadership and reshape the global technological landscape in Beijing's authoritarian image.

The PRC's legal framework further complicates this picture. Laws such as the 2017 National Intelligence Law compel Chinese citizens and organizations to "support, assist, and cooperate with state intelligence work." This means that even well-intentioned Chinese researchers may be legally obligated to share information with their government, regardless of any commitments made to U.S. institutions.

Let me be clear: research security is not about stifling innovation or closing our doors to the world. It is also not about and cannot be about targeting individuals based on ethnicity. It's simply about ensuring that our openness is not exploited to our detriment by an adversarial nation.

The DOE's national laboratories have long been a shining beacon for scientists and researchers worldwide. That is an asymmetric advantage that we have. This global appeal is not just a point of pride; it's a cornerstone of our technological leadership. For instance, 59% of top-tier AI researchers work in the U.S., but only 20% received their undergraduate degrees here. Our nation's commitment to freedom, innovation, and scientific excellence has made us the destination of choice for the world's brightest minds. This magnetic pull of talent is not just an asset; it's a national and economic security imperative.

We can and must maintain our leadership in scientific collaboration, but on terms that protect our national interests. We have passed several laws to address these challenges, including measures in the CHIPS and Science Act, various NDAAs, and executive actions such as NSPM-33. Effective implementation of these remains key. This requires funding agencies, enforcement authorities, universities, and researchers to work closely together, with a strong emphasis on educating researchers about potential risks and best practices.

The path that I've laid out today is undoubtedly challenging and will require sustained commitment and vigilant oversight. However, the alternative—a world where the PRC dictates the rules for transformative technologies—is simply not an option we can entertain.

There is much more that I could say on these matters, but I trust we'll cover them more fully over the course of this hearing. Thank you again for the opportunity to testify and I look forward to your questions.

Background

The PRC is engaged in an intense technological competition with the United States. This is not mere economic rivalry, but a strategic effort to supplant American leadership and reshape the global order. The PRC's ambitions to dominate advanced computing and artificial intelligence by 2030 represent a serious threat to our national security, economic prosperity, and way of life.

Under Xi Jinping's iron-fisted rule, the PRC has weaponized every facet of Chinese society in pursuit of technological supremacy. Their whole-of-nation approach erases any distinction between civilian and military applications, turning every research lab, university, and tech company into a potential tool for the People's Liberation Army.

In this high-stakes competition, the DOE and its network of 17 National Laboratories, and 35 user facilities stand as America's technological vanguard. DOE's unparalleled capabilities in advanced computing and multidisciplinary research are crucial assets in maintaining our technological edge. To win this competition, it is critical that we have a multifaceted approach that involves maximizing the operational and scientific capabilities of our National Labs, enhancing research security, and implementing strategic initiatives to attract and retain the world's most brilliant minds.

DOE's Key Role in Advancing U.S. Technological Leadership

The DOE and its network of 17 National Laboratories and 35 user facilities are the crown jewels of our nation's scientific enterprise. They house computational power and multidisciplinary expertise that keep the U.S. at the cutting edge of scientific research and innovation. These institutions are fortresses of innovation, housing computational firepower that the PRC can only dream of replicating independently.

The breadth of artificial intelligence (AI) applications emerging from DOE labs is staggering, spanning critical areas from national defense to energy systems and scientific discovery. This technology is pivotal in shaping our technological and economic competitiveness, particularly in the face of intense global competition. The DOE labs, with their thousands of top-tier scientists and engineers, are uniquely positioned to drive transformative advancements that maintain our national security, propel energy innovation to benefit consumers and businesses, and push the boundaries of scientific breakthrough.

Consider the computational prowess housed within these labs. DOE currently operates some of the world's fastest supercomputers. These machines are not just scientific tools; they are strategic assets that maintain our qualitative edge and drive innovations that keep us ahead in critical technologies. The potential of these supercomputers, when coupled with cutting-edge AI research, is immense. They enable the development of sophisticated AI models that can revolutionize fields such as nuclear fusion, geothermal exploration, carbon capture, drug discovery, and their national security applications.

The impact of DOE labs extends far beyond raw computing power. They have consistently delivered breakthrough innovations that underpin American technological leadership, including:

1. The clean room, invented at Sandia, revolutionized semiconductor manufacturing—an industry crucial for technological independence and at the heart of global tech competition.
2. DOE's collaboration with NVIDIA on NVLink in 2017 helped cement U.S. leadership in high-performance computing interconnects, providing a key advantage in developing next-generation AI systems.
3. DOE-funded research laid the groundwork for programmable Graphics Processing Units (GPUs), enabling the AI revolution that is transforming our economy today.

Looking ahead, the potential for DOE labs to drive AI innovation is enormous. DOE could and should lead in the development of AI for bolstering national security, AI for unleashing energy abundance, and AI for accelerating science. These models, possible only through the supercomputing capabilities of DOE labs, could offer unprecedented insights into complex processes like molecular dynamics crucial for additive manufacturing or power grid dynamics, leading to a more resilient energy infrastructure.

Lab-driven AI investments can aid the process of fundamental scientific discovery itself. In fields like nuclear or high-energy physics, AI-powered models can efficiently capture and analyze massive datasets and drive automated experimentation. AI can also assist science to reveal how matter behaves in extreme environments, crucial for unlocking the mysteries of fusion.[1]

Take for example, how DOE is experimenting with cloud labs to automate science. The Pacific Northwest National Laboratory recently shared that their researchers are integrating AI with cloud-based laboratory environments to streamline scientific experimentation.[2] This approach involves using AI to automate and optimize various aspects of experimental processes, such as setup, monitoring, and data analysis, thereby reducing the need for manual intervention and increasing the throughput of scientific experiments. This technology can significantly enhance research efficiency in areas like biotechnology and materials science, potentially leading to faster scientific discoveries and innovations. Such capabilities could be a gamechanger for how we do science.

Similarly, in the realm of national security, DOE labs play a central role. Their work in AI could enhance U.S. stockpile modernization and surveillance of foreign nuclear activities. The development of classified AI models could significantly advance our capabilities in managing threats to national security, from maintaining space situational awareness to advancing biodefense.[3] Moreover, our National Labs are ideally suited to develop AI tools that can test and validate other AI models, especially around proliferation risks. It's important to note that these efforts are being complemented and enhanced by the work of the recently established AI Safety Institute at NIST. The collaborations between DOE and AISI to conduct critical evaluations of AI systems, particularly focusing on potential risks related to chemical, biological, radiological, nuclear, and explosive (CBRNE) threats are critical to our national security.

For energy innovation, advancements in AI at DOE labs can lead to more efficient energy production, enhanced grid security, and accelerate the design and development of next-generation nuclear reactors. For instance, AI models developed at DOE labs could revolutionize electrical grid load forecasting and

---

[1] https://engineering.princeton.edu/news/2024/02/21/engineers-use-ai-wrangle-fusion-power-grid
[2] https://www.pnnl.gov/news-media/scientists-pnnl-explore-how-ai-can-help-transform-research
[3] https://www.llnl.gov/article/51621/llnl-dod-nnsa-dedicate-rapid-response-laboratory-supercomputing-system-accelerate-biodefense

severe weather prediction, improving reliability and reducing the $150-billion annual cost of power outages to American businesses.[4]

It is also critical to recognize that building AI capabilities further requires developing the underlying infrastructure to support AI development and deployment and then also having the best talent to utilize that infrastructure. I'll come to the talent piece later, but on the infrastructure side, this means significant investment in building next-generation AI data centers and high-performance computing facilities, developing cutting edge GPUs to put in these data centers, and increasing base load power generation to power them. The recent bipartisan action by this committee on permitting reform will help address many of the regulatory hurdles currently impeding this essential infrastructure buildout.

The strategic importance of DOE labs in maintaining U.S. technological leadership cannot be overstated. As global competition in AI and other emerging technologies intensifies, these labs serve as our technological vanguard. Their unique combination of world-class talent, cutting-edge facilities, and multidisciplinary approach positions them to drive innovations that will shape the future of AI and maintain America's technological edge.

However, the very excellence that makes DOE labs the crown jewels of American scientific enterprise also makes them attractive targets for those seeking to erode our technological advantages. The labs represent a treasure trove of innovation that foreign competitors are eager to access—by any means necessary.

The Importance of Robust Research Security

As we celebrate and leverage the immense capabilities of our DOE labs, we must also recognize the critical need to safeguard them from nefarious actors. The PRC, in particular, has demonstrated a keen interest in emulating and potentially surpassing our research capabilities. Xi Jinping himself has explicitly held up DOE's National Laboratories as models to recreate, stating in the PRC's 13th Five-Year Plan[5]:

> "National laboratories have become key platforms for major developed countries to seize the high ground in technological innovation. For instance, the Argonne, Los Alamos, and Lawrence Berkeley National Laboratories in the United States, as well as the Helmholtz Research Centers in Germany, are all research bases focused on national missions. They rely on interdisciplinary approaches, extensive collaboration, and strong support to carry out collaborative innovation.
>
> Currently, China's technological innovation has entered a new stage where tracking, parallel running, and leading coexist. It is urgently needed to focus on national goals and strategic needs, target international technological frontiers, and establish a group of larger-scale, interdisciplinary, and integrative national laboratories. This will involve optimizing the allocation of human, financial, and material resources to create a new pattern of collaborative innovation.

---

[4] https://www.energy.gov/ne/articles/department-energy-report-explores-us-advanced-small-modular-reactors-boost-grid
[5] http://cpc.people.com.cn/n/2015/1103/c64094-27772663.html

> The main consideration is to set up a number of national laboratories in key innovation areas, create hubs that attract top domestic and international talent, and organize collaborative research with significant leading roles. This approach aims to build technological innovation capabilities that represent national standards, are recognized by international peers, and hold influence on the global stage, positioning China as a strategic force in capturing key international technological heights."[6]

While imitation may be the sincerest form of flattery, in this context, it serves as a stark reminder of the value and vulnerability of our National Laboratories. It's a testament to the global impact of our National Laboratories that they serve as a model for ambitious nation-states, but it also highlights the pressing need for a thoughtful, comprehensive approach to research security that preserves our competitive edge in the global scientific community. The PRC has since announced their own national laboratories explicitly designed to mimic and ultimately surpass our DOE complex.

Let me be absolutely clear: the PRC is pursuing an aggressive campaign of technological advancement that relies heavily on both investing in their own R&D capabilities (over the last seven years, the PRC has increased its R&D budget consistently by 10% year over year)[7] and expanding their intellectual property acquisition[8] and technological intelligence gathering efforts. This goes beyond normal competition; it represents a coordinated effort to challenge America's innovation leadership and reshape the global technological landscape in Beijing's authoritarian image.

The PRC's strategy of integrating civilian research with military applications is not merely theoretical—it's being actively implemented at the highest levels of Chinese academia.

In 2018, Tsinghua University's Vice President, You Zheng, penned an article that laid bare the institution's role in advancing state and military objectives, particularly in the field of AI.[9] You Zheng stated:

"In accordance with central requirements, Tsinghua University will closely integrate the national strategy of military-civilian integration and the AI superpower strategy. Tsinghua University was entrusted by the CMC [Central Military Commission] Science and Technology Commission to take responsibility to construct the High-End Laboratory for Military Intelligence (军事智能高端实验室). With regard to basic theories and core technologies, military intelligence and general AI possess commonalities. Therefore, Tsinghua University regards the construction of the High-End Laboratory for Military Intelligence as the core starting point for serving the AI superpower strategy.... Therefore, Tsinghua

---

[6]Original text: "国家实验室已成为主要发达国家抢占科技创新制高点的重要载体，诸如美国阿贡、洛斯阿拉莫斯、劳伦斯伯克利等国家实验室和德国亥姆霍兹研究中心等，均是围绕国家使命，依靠跨学科、大协作和高强度支持开展协同创新的研究基地。

当前，我国科技创新已步入以跟踪为主转向跟踪和并跑、领跑并存的新阶段，急需以国家目标和战略需求为导向，瞄准国际科技前沿，布局一批体量更大、学科交叉融合、综合集成的国家实验室，优化配置人财物资源，形成协同创新新格局。主要考虑在一些重大创新领域组建一批国家实验室，打造聚集国内外一流人才的高地，组织具有重大引领作用的协同攻关，形成代表国家水平、国际同行认可、在国际上拥有话语权的科技创新实力，成为抢占国际科技制高点的重要战略创新力量。"

[7] https://www.economist.com/science-and-technology/2024/06/12/china-has-become-a-scientific-superpower
[8] https://www.reuters.com/world/five-eyes-intelligence-chiefs-warn-chinas-theft-intellectual-property-2023-10-18/
[9]https://www.cnas.org/publications/commentary/tsinghuas-approach-to-military-civil-fusion-in-artificial-intelligence

University insists on basic research as a support in applied technology research in AI talent training and scientific research innovation, with military requirements as a guide, promoting the development of basic AI research."

This declaration reveals a troubling reality: China's top engineering and computer science institution makes no distinction between foundational AI research and its potential military applications, viewing them as intrinsically linked. The PRC extends this philosophy to the private sector, effectively coopting companies as extensions of the state apparatus. A notable example of this is Huawei, which embodies the PRC's strategy of fusing civilian technological development with state and military interests.[10]

Thus, we must recognize that the global research landscape has evolved. A recent report by independent science advisory group JASON notes that while openness in fundamental research promotes scientific discovery, the PRC's efforts to militarize civilian research and restrict information flow "may severely limit the benefits of collaborations with research organizations within the PRC."[11]

The PRC's legal framework further complicates this picture. Laws such as the 2017 National Intelligence Law compel Chinese citizens and organizations to "support, assist, and cooperate with state intelligence work." This means that even well-intentioned Chinese researchers may be legally obligated to share information with their government, regardless of any commitments made to U.S. institutions.[12]

It's important to note that navigating this landscape is challenging for research institutions across the U.S., including our National Laboratories. Collaborations between U.S. researchers, including those at DOE National Labs, and scientists from Chinese universities with defense research connections have occurred.[13] While such collaborations have decreased, they underscore the need for continued vigilance and clear guidelines.

This challenge reflects the differing approaches to research and development between the U.S. and the PRC. The PRC's holistic approach to technological development, which blurs the lines between public, private, civilian, and military sectors, creates complexities that our open research system must carefully navigate.

Our response must be comprehensive and nuanced. We must recognize the value of international collaboration while implementing robust safeguards against potential exploitation. This isn't about targeting individuals based on ethnicity, but about addressing a state-driven strategy to acquire technology through various means.

---

[10] https://www.axios.com/2019/10/17/china-technology-national-security-huawei-tiktok
[11] https://new.nsf.gov/news/nsf-announcement-jason-report-safeguarding
[12] https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf
[13] The Seven Sons (Beihang University, Beijing Institute of Technology, Harbin Engineering University, Harbin Institute of Technology, Nanjing University of Aeronautics and Astronautics, Nanjing University of Science and Technology, Northwestern Polytechnical University) are widely believed to have close scientific research partnerships and projects with the People's Liberation Army. Nearly three quarters of university graduates recruited by defense related state-owned enterprises in the PRC come from the Seven Sons. The Seven Sons devote at least half of their research budgets to military products. In 2024 alone, researchers affiliated with DOE National Labs have collaborated with scientists from Chinese universities commonly referred to as the Seven Sons of National Defence, resulting in at least 60 research publications so far.

Research security is not about stifling innovation or closing our doors to the world. It is about ensuring that our openness is not exploited to our detriment. We can and must maintain our leadership in scientific collaboration, but on terms that protect our national interests.

We have the legislative framework to address these challenges, including measures in the CHIPS and Science Act, various NDAAs, and NSPM-33.[14] The focus now should be on effective implementation.[15] This requires funding agencies, enforcement authorities, universities, and researchers to work closely together, with a strong emphasis on educating researchers about potential risks and best practices. We must demonstrate that ethical conduct and scientific excellence are mutually reinforcing, setting a global standard for responsible research practices.

The Talent Imperative: Leveraging DOE's Role in Workforce Development and Global Talent Attraction

While robust security measures are crucial, we must recognize that protecting technology is only part of the equation. To maintain our technological edge, particularly in critical areas like AI, we must capitalize on DOE's dual role as both a domestic workforce developer and an international talent attractor.

Realizing the impact of our National Labs on our strategic priorities requires integrating the best of research and development into solutions. Insulating ourselves entirely from global scientific developments is neither practical nor advisable. Our experts must understand relevant developments by scientists worldwide; a blanket prohibition on the employment of foreign nationals from specific countries with large scientific enterprises would be counterproductive to our national security mission. At the same time, restricting access to sensitive information is vital for our national security. It is about striking that balance.

The DOE's National Labs have long been a shining beacon for scientists and researchers worldwide, embodying the pinnacle of scientific pursuit and technological innovation. This global appeal is not just a point of pride; it's a cornerstone of our technological leadership. The DOE's National Laboratories interact with scientists of foreign origin in three principal ways:

1. Short-term visits by international scientists to share advances and explore collaboration opportunities.
2. As a pipeline for our future workforce, recognizing that a significant portion of higher degree holders in Science and Engineering in the U.S. are foreign-born.
3. Through the integration of foreign-born scientists who become U.S. citizens, obtain clearances, and become integral parts of our national security enterprise.

These interactions are not just beneficial; they are essential for maintaining our technological leadership and our position as the world's premier destination for scientific talent. As the National Security

[14] https://crsreports.congress.gov/product/pdf/IF/IF12589
[15] Despite OSTP's significant delays in issuing implementation guidance for NSPM 33, DOE's implementation of NSPM 33 goes beyond what the OSTP has asked for.

Commission on Artificial Intelligence noted in 2022, "The United States risks losing the global competition for scarce AI expertise if it does not cultivate more potential talent at home and recruit and retain more existing talent from abroad."[16]

The importance of our ability to attract global talent is underscored by these striking statistics:

- 59% of top-tier AI researchers work in the U.S., but only 20% received their undergraduate degrees here.
- Among the most elite AI researchers (top 0.5%), 65% work in the U.S., but only 35% earned their undergraduate degrees domestically.[17]

These figures highlight a crucial point: America's technological leadership is inextricably linked to our ability to attract and retain global talent. Our nation's commitment to freedom, innovation, and scientific excellence has made us the destination of choice for the world's brightest minds. This magnetic pull of talent is not just an asset; it's a vital national and economic security imperative.

The importance of this global talent attraction becomes even more apparent when we consider the scale of the PRC's STEM education pipeline, which produces four times as many bachelor's degree holders and twice as many PhD graduates as the U.S. Xi Jinping himself has described talent as "the first resource" in the PRC's push for "independent innovation."

We must use a scalpel to ensure we are removing the bad actors, not a sledgehammer. As former Counterintelligence Chief Bill Evanina said, "We allow 350,000 or so Chinese students here every year. That's a lot. We have a very liberal visa policy for them. Ninety-nine point nine percent of those students are here legitimately and doing great research and helping the global economy. But it is a tool that is used by the Chinese government to facilitate nefarious activity here in the U.S."[18]

Our system's fundamental strength lies in its ability to draw top talent from around the world. While we must be mindful of attempts by authoritarian regimes to exploit our openness, we should resist blunt actions that undermine our key advantages.[19] We must ensure that our National Laboratories continue to be beacons of scientific excellence, drawing the best and brightest from around the world. I suspect that Beijing remains concerned about the kinds of ideas that their innovators get infected with here being transplanted back into their system.

Ultimately, I'm confident in our ability to maintain an open society that organizes and attracts people to achieve remarkable outcomes. Our goal should be to remain the most attractive destination for global talent while implementing measured, thoughtful safeguards against potential threats. Thus, we need precision tools like those initiated by the Trump administration under NSPM-33 and Presidential

---

[16] https://reports.nscai.gov/final-report/
[17] https://fas.org/publication/unlocking-american-competitiveness-ai-eo/
[18] https://www.cnn.com/2019/02/01/politics/us-intelligence-chinese-student-espionage/index.html
[19] The PRC understands this reality all too well. They view America's ability to attract and retain Chinese talent as a direct threat to their ambitions. The head of the CCP's Central Talent Work Coordination Group has lamented that "the number of top talents lost in China ranks first in the world." A state-run consulting firm wrote in an AI policy white paper that U.S. immigration restrictions "have provided China opportunities to bolster its ranks of high-end talent." The deputy editor of China Daily USA, a government newspaper, said that expansion of the U.S. employment-based immigration system "would pose a huge challenge for China, which has been making great efforts to attract and retain talent."

Proclamation 10043 and those by Congress in the CHIPS and Science Act so that we are only targeting those 1 in 1000 individuals. And then these policies must be continuously updated and aggressively enforced, with DOE taking a leading role in identifying entities linked to the PRC's military-civil fusion strategy.

Conclusion

The U.S. finds itself in a pivotal technological competition that will shape the geopolitical landscape of the 21st century. This is not hyperbole, but a stark reality that demands our immediate and unwavering attention. The arena of this competition is not on traditional battlefields, but in laboratories and research facilities where transformative technologies such as AI, quantum computing, and advanced energy systems are being pioneered.

The PRC's relentless pursuit of technological supremacy, backed by a whole-of-nation approach and disregard for international norms, directly challenges American leadership and the values underpinning our innovation ecosystem. Their ambition to reshape the global technological landscape is a clear and present danger to our national security, economic prosperity, and way of life.

In this critical juncture, the DOE's network of 17 National Laboratories and 35 user facilities stand as America's technological bulwark. These institutions are our first line of defense against technological subversion and the vanguard of American innovation.

The urgency of our situation calls for decisive action to fully harness the potential of our DOE complex together with the private sector. This necessitates a multifaceted approach: enhancing the security of our National Lab facilities, maximizing their operational and scientific capabilities, and implementing strategic initiatives to attract and retain the world's most brilliant minds. We must foster an environment where our scientists and engineers are encouraged to think big, push the boundaries of innovation, and be confident that their groundbreaking work is safeguarded against foreign exploitation.

At the same time, American industry is already leading the way on innovation in critical and emerging technologies like AI, quantum and cyber. Their work today will determine whether tomorrow's technologies are built on democratic values or authoritarian control. Public-private partnerships are crucial in leveraging the strengths of both sectors to drive innovation, accelerate research and development, and rapidly deploy cutting-edge technologies. By combining the long-term vision and resources of the DOE with the agility and market-driven focus of American industry, we create a powerful ecosystem for technological advancement.

The road ahead that I've laid out today is undoubtedly challenging and will require sustained commitment and vigilant oversight. However, the alternative—a world where the PRC dictates the rules for transformative technologies—is simply not an option we can entertain.

By fully empowering our National Laboratories, we not only protect our technological edge but also reinforce the values of open scientific inquiry, ethical research practices, and international collaboration that have long been the hallmarks of American innovation. The DOE complex represents more than just a

collection of research facilities; it embodies our nation's commitment to pushing the boundaries of human knowledge and technological capability.

Thank you, and I look forward to your questions.

Bio:

Dr. Divyansh Kaushik is an expert in emerging technologies and national security, focusing on artificial intelligence and its implications for US-China tech competition. Previously, he served as the Associate Director for Emerging Technologies and National Security at the Federation of American Scientists (FAS). He holds a Ph.D. in Artificial Intelligence from Carnegie Mellon University. Dr. Kaushik's research has earned him thousands of scholarly citations and also led to prestigious accolades in industry and academia. As a recognized voice in discussions on AI, research security, and technological competition, he continues to contribute to leading publications, offering insights that bridge the gap between technology and policy. He is a frequent contributor to leading publications, including the Washington Post, Politico, National Defense Magazine, The Dispatch, Real Clear Defense, Daily Caller, and Forbes, amongst others.

The CHAIRMAN. Thank you.

Now we are going to begin our questions, and I will begin.

This is for all three of you to think about, but we, as Senators—Democrats and Republicans—are looking at, whether it be the CHIPS Act and how we divide our money up and this and that. I don't want to reinvent the wheel. Okay? And I don't want to split the baby. The bottom line is, you do what you do, and NSF should do what they do. And for some reason, whoever has what in their state—I would like to make sure that we are not making that mistake and going down a path where you don't have the ability to make up the differences where we are lagging behind right now.

So if you can—and this isn't disparaging anything in NSF. They have so much expertise in certain areas, but in the CHIPS Act, you know, what we have done there, you already have that computing expertise, you already have the investment in the supercomputers and quantum computing and all that. Why would we basically try to reinvent the baby again—you know, the wheel, if you will? So would you all speak in comparison of what you think each one of you all do with our labs versus NSF and how we can direct more of our attention to make sure that both of you can meet your full potential?

You want to start, Ms. Fu?

Ms. FU. Sure, I am happy to speak on this because there has been a lot of discussion on the AI policy.

The CHAIRMAN. Does it make sense, what I am asking you?

Ms. FU. Of course, yes. NSF obviously plays an extremely important role in the nation's ecosystem. It is focused on workforce development. It is focused on training. It is focused on providing grants to research institutions all across the country. And that is incredibly important and we need that. DOE's focus is as a capability organization. We are a mission-driven R&D agency that is focused on science at scale to solve complex challenges that only can be done by big-team science. And so, we also work very closely with universities across the country, but we are focused on specific problem sets that we are trying to address.

And so, I think that the roles of NSF and DOE are actually quite complementary because the NSF funds researchers that then become part of the AI ecosystem that can become part of the workforce that is going to help drive the frontier. But ultimately, we do play very, very different roles in the AI ecosystem and the innovation ecosystem.

The CHAIRMAN. Not to put you on the spot, but did we direct, through the CHIPS Act, investments toward NSF that are trying to recreate what you are already doing?

Ms. FU. Well, they are certainly working on the national AI research resource. And I will say, on that, because we recognize the importance of access to compute, I will say this: DOE's supercomputers have been open to the research community. We leaned in and extended the life of Summit supercomputer at Oak Ridge National Lab and also provided access to testbeds through the NAIRR pilot. So we are working very closely with NSF in this endeavor.

The CHAIRMAN. You don't feel that competition that one is taking away? We can do even more if it was directed to what we do and what our expertise is versus trying to duplicate that.

Ms. FU. I will say, we are playing our part in the ecosystem. And I firmly believe they are very, very complementary.

The CHAIRMAN. Dr. Gleason, do you want to comment on this? It's not the easiest. I am putting you in a spot, I know that, but what we are trying to do—I think all of us are trying to make sure that we have used our taxpayer dollars in the most efficient and effective way possible, and have NSF do what they do best and let you do what you do best, but not trying to overlap each other.

Dr. GLEASON. So this is a very good question. I would echo a lot of what Helena said about complementary roles and responsibilities. Maybe saying the same thing just a little bit differently, from my perspective as a leader of scientists at Oak Ridge National Laboratory, is that NSF is about access to software infrastructure tools for the masses—for universities, students, et cetera, to have access to artificial intelligence and computational power to try out new methods, new algorithms, evaluate new software and tools. Oak Ridge National Laboratory and the lab system really provide world-leading capabilities and world-leading science and technology input to that. So for example, we, as Helena mentioned, we provide the Summit supercomputer as part of the NAIRR effort. We have had lots of people sign up to use that, as part of the NAIRR program, and we help them achieve their science and technology objectives because we have subject matter expertise that we can put alongside them. How do you use a supercomputer? What is the scientific area that you are trying to make discoveries in? We have experts in those spaces that we can line up with them and help them achieve their science and technology objectives.

So that is a differential. And we rely heavily on NSF for workforce development, new students, training, that we can—hopefully, some of those will come to the national labs and contribute at some point.

The CHAIRMAN. Sounds like you all are doing better than we are at working together.

Dr. GLEASON. I agree.

The CHAIRMAN. And Dr. Kaushik, do you have a comment on it?

Dr. KAUSHIK. Yes, I agree with everything that they have said, but I would point out one other thing. I think NSF's focus is more on foundational research, on basic research where we do not have near-term applications or we do not know about exploring the unknown, where DOE, they are trying to supercharge the capabilities we have to get things out there to take an aim at moonshots. And I think that is very critical for our national security enterprise, and the critical role—one of the differentiators between DOE and NSF is the role DOE labs play in furthering our national security—all the NNSA labs—in furthering our national security work, as compared to the more fundamental science that NSF tries to invest in.

The CHAIRMAN. Thank you all.

We will go for seven minutes, okay, to give you a little bit more time since other Senators are at so many different committee meetings. My main thing is on power, too, because I know it's going to take an awful lot of power to generate this. I am concerned. We have seen over 90 gigawatts of coal power retired in the last decade. That is dispatchable, 24/7 power—gone. And we can see twice as much dispatchable capacity retire in the next decade on the

path that we have been heading down, historically. It can't be more clearly demonstrated than PJM's recent assessment that 40 gigawatts of existing generation are at risk of retirement by 2030, yet only 30 gigawatts of equivalent capacity are projected to be added. Take that in comparison, China is bringing on 90 gigawatts online every two years of dispatchable power, and we are, I mean, this whole environment, we are all responsible, but we have to understand what we are dealing with.

I don't know if any of you want to comment on that, and if you have raised the concern that we are not going to be able to energize these data centers to compete? Just as quickly as you can.

Ms. FU. This is a focus for the Department. We understand the implications of having enough power to power both manufacturing that is coming back to the United States, electrification of the grid, as well as the data centers and the AI that is going to be needed to train those models in the United States. The Secretary and the entire Department are very focused on this issue. We just recently issued a new website—a new hub—for folks who want to work with us on these issues.

I will say this: there are new technologies and new tools that we have available—grants, tax credits, loans, technical assistance—that we are bringing to bear on this particular issue. Our Lawrence Berkeley National Lab is also working on a study that is looking at energy efficiency in data centers. And then, I will also point to the work that we were able to do in the exascale computing project.

The CHAIRMAN. You are all on different grid zones. Are you concerned about the grid being able to be reliable, the grid that you are in?

Ms. FU. We absolutely need to make sure that the grid is resilient and that it's able to manage the load.

The CHAIRMAN. Are you all evaluating that and monitoring?

Ms. FU. Yes. We are focused on this issue, especially as it relates to data center energy growth.

The CHAIRMAN. How many of you are on PJM? Most of you are on PJM as far as dispatchable, you know, where our power is—the PJM system. I am just saying—I just think we are heading for a real calamity here.

Anybody else want to comment on that?

Dr. KAUSHIK. I am happy to, Senator. Just one of the things that we have to understand—the reality is, over the last six years, the computational needs of AI systems have grown a millionfold, like ChatGPT-1 to ChatGPT-4, the computational needs have grown a millionfold. The parameters have grown a millionfold. Now, since 2010, we have seen that the number of computations that we are putting toward AI models is doubling every six months. And there is no reason to believe that that is going to slow down any time soon.

I think there was a recent Bloomberg article stating that it is taking about seven years' delay for a completed data center that would require 100 megawatts or more of energy to be connected to the grid in Virginia. And I think those statistics should raise some alarm—and I think to what Helena pointed out, I think those tools are great, but we would need further action, probably something, you know, not just about how we are providing loans and financing

to data center companies or utility companies, but what are we doing in terms of energy-efficient AI? What are we doing in terms of making sure that data centers can come online, whether it's, you know, in the long term, where we are building those data centers in the United States, but in the near term, how can we make sure that those data centers are not going to countries which are using—infrastructure, but are using American hardware.

And so, I think those are important questions for us to address. And I think the action that this Committee has taken on permitting will have a big impact on that, but we need more.

The CHAIRMAN. Got you.

Senator Barrasso.

Senator BARRASSO. Thanks, Mr. Chairman.

Let me stick with you, if I could, Dr. Kaushik. You are an expert on China's science and technology policy. What unique threats does China pose to government-funded research and development of critical and emerging technologies?

Dr. KAUSHIK. I think, Senator, the answer is very clear. They have a targeted effort that we call the civil-military fusion, where even their universities have put out statements saying that all the basic foundational research that they do is toward military gain. Every IP theft case that we have seen, every espionage concern that we have seen, I think, all of that is ultimately feeding into their military complex. Now, that plus their legal situation with the National Intelligence Law or the National Cybersecurity Law and all those things are making it more complicated for Chinese researchers to be able to actually act in good faith because no matter what commitments they made to U.S. institutions, they are required by law to share all that information with the Chinese government. And I think when they are trying to go after our technology, as you mentioned with regards to a recent espionage case where a researcher was charged regarding data center plans, I think they are going after that cutting-edge technology. They want to—they cannot independently replicate it. And so, they want to steal our IP and build it there in the short term to be able to catch up.

These numbers are not just a mirror reflection of their investments in R&D. These are also a reflection of how they have exploited our open system.

Senator BARRASSO. Ms. Fu, he talked about the targeted researcher for military activities, and if you follow the long history of Chairman Mao, his efforts when he was on Stalin's payroll were to try to get the nuclear weapons, and they fast-forwarded the technology to him. When Stalin was attacked during World War II, his goal was then to try to work with the United States to get the nuclear weapons. I mean, all of the issues have been a militarization of China.

So you know, in 2020, the Hoover Institution released a 169-page report. I know you are familiar with it. It is titled "Global Engagement: Rethinking Risk in the Research Enterprise."

[The report referred to follows:]


Global Engagement
RETHINKING RISK IN THE RESEARCH ENTERPRISE
A PUBLICATION OF THE HOOVER INSTITUTION

81

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/QQ58XiznSlfTLYv5rARfjL.

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=MDUyOTFMcVpFYlBJUjh1WDFMdXhZUzdEaDFUM3FUcldNMUZyQ1VSN3FmWWVkcEZ5M2tXNy9MVkYyNkdMUzdGOVg=.

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/.

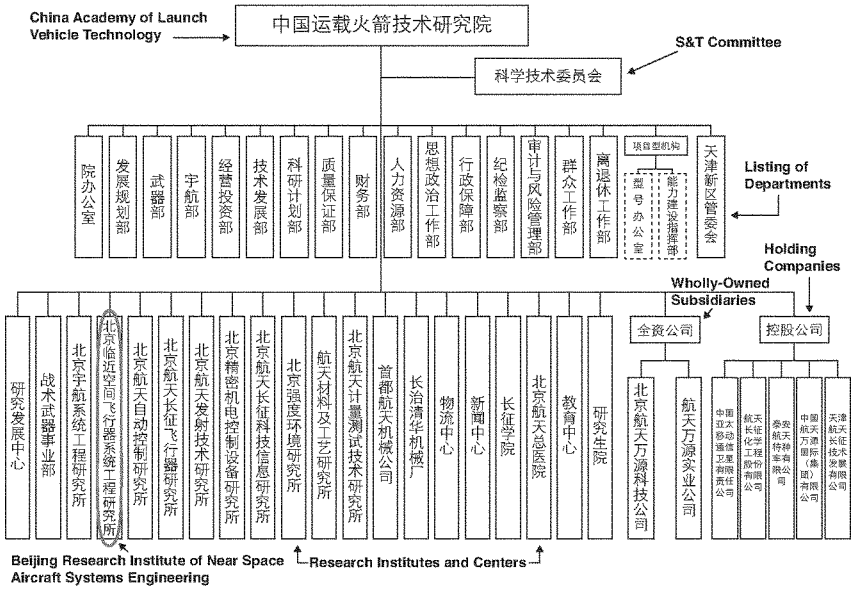


Figure 1. China Academy of Launch Vehicle Technology organizational structure (with added English annotations). *Source:* "组织机构, [Organizational Structure]" 中国运载火箭技术研究院 [China Academy of Launch Vehicle Technology], accessed June 14, 2020, http://www.calt.com/n481/n490/index.html.

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 H Atom Addition to 1,3-Butadiene and Related Reactions on the 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

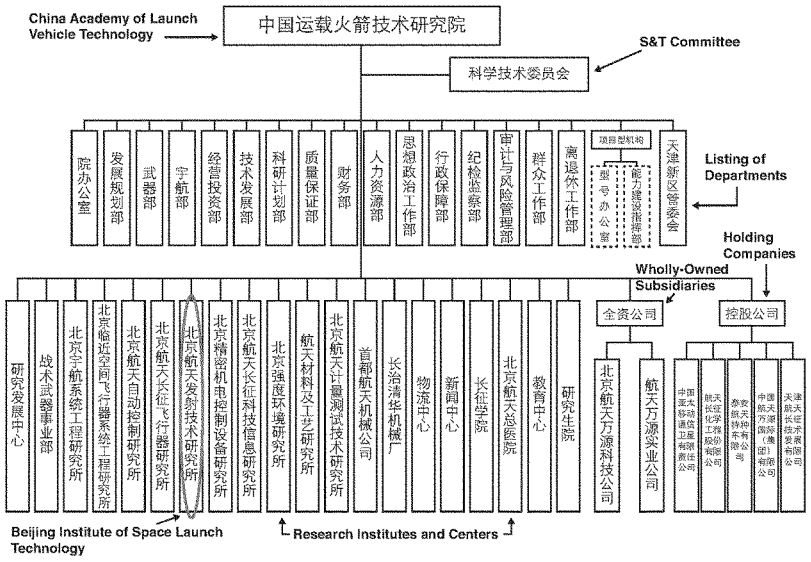


Figure 2. China Academy of Launch Vehicle Technology organizational structure (with added English annotations). *Source:* "组织机构, [Organizational Structure]" 中国运载火箭技术研究院 [China Academy of Launch Vehicle Technology].

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?

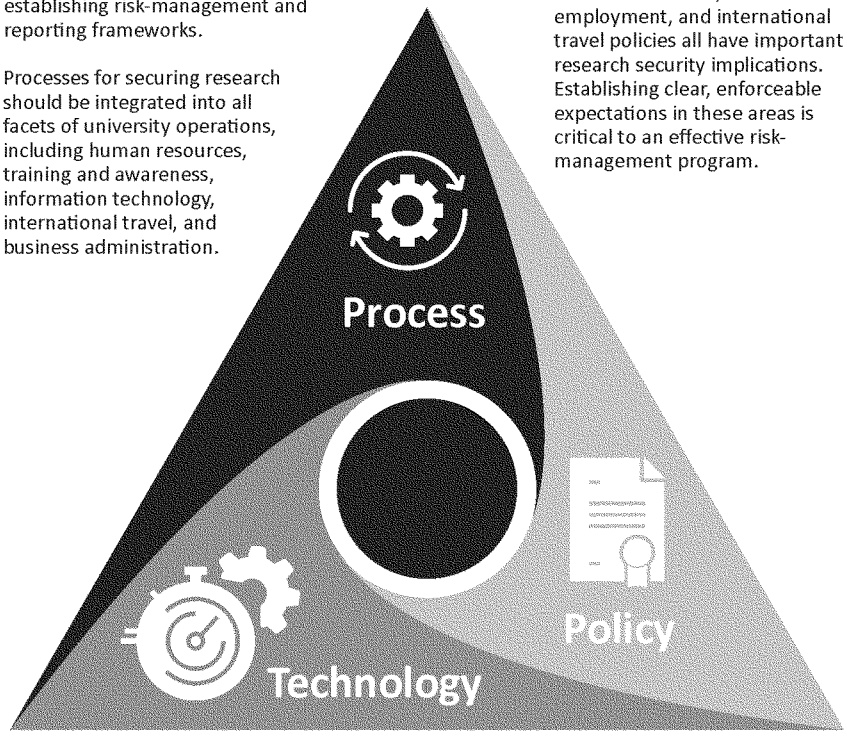
Process Solutions

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).

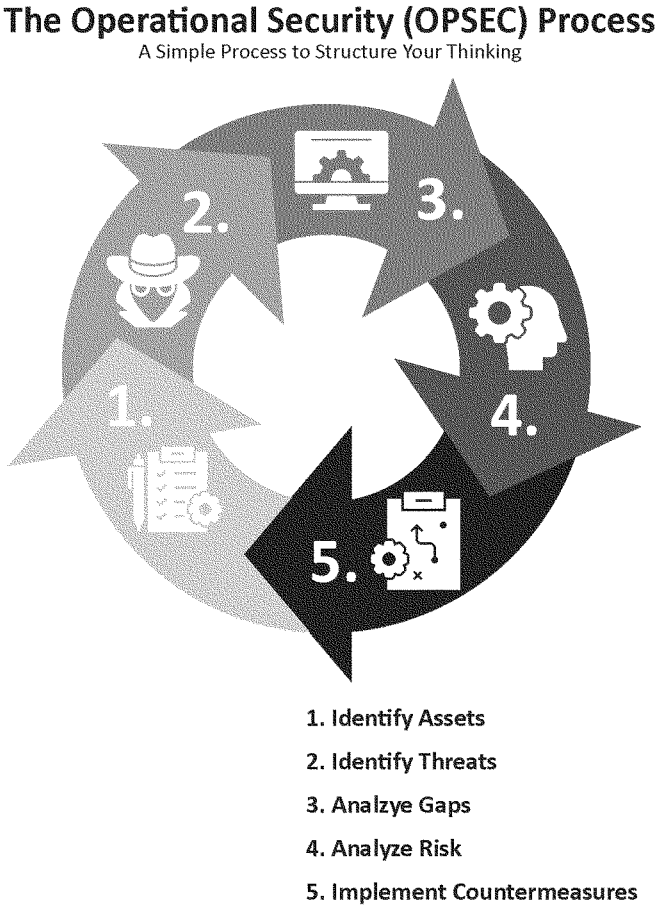


Figure 2. The OPSEC Process.

- *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.

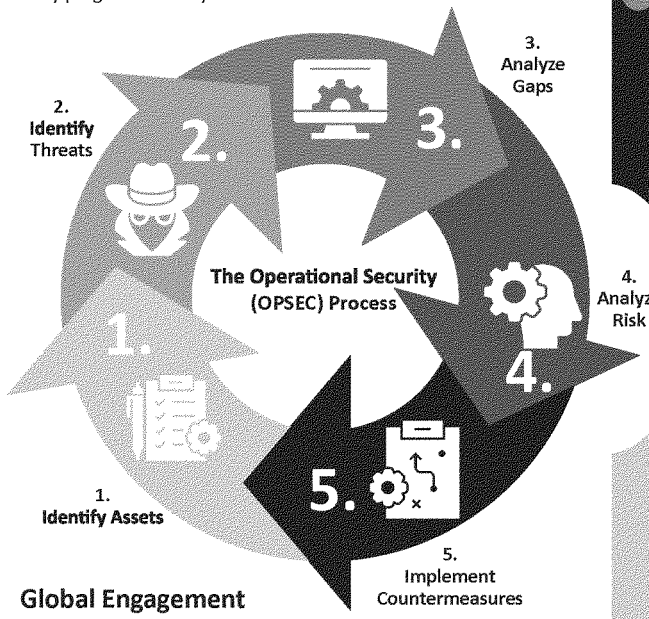
1. What is Global Engagement Maturity Modeling?

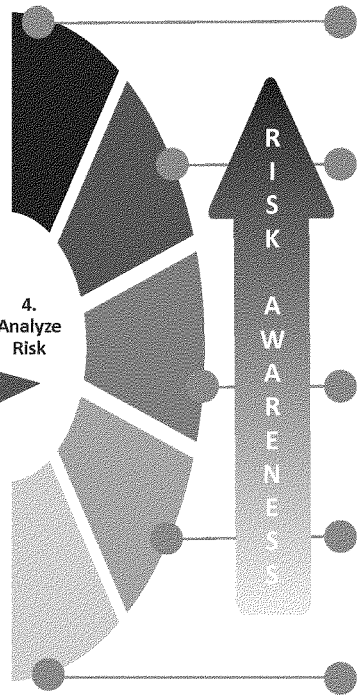
The GEMM provides a formal method for assessing the policies and processes in an institution's GERAMP and ensuring that they are effective, replicable, and continuously improved. Information technology provides one path for successfully automating and integrating those elements into the institution's 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.





Level 5: Integration
Organizations operating at Level 5 have processes that are automated, documented, and constantly analyzed **for optimization. Research security has** been integrated into all aspects of **organizational culture.**

Level 4: Managed
The organization begins to measure, refine, and adapt its security **processes to make them more effective and efficient based on the information** it receives from its program.

Level 3: Implementation
Processes have become formal, standardized, and defined. This process **maturation creates consistency across the organization.**

Level 2: Repeatable Processes
Some processes become repeatable at this stage of maturity. A formal program has begun, although discipline is lacking. Some processes have been established, defined, and documented.

Level 1: Implementation
At this level, organized processes are not yet in place. Ad hoc and informal **security processes are reactive and not** repeatable, measurable, or scalable.

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://nices.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.

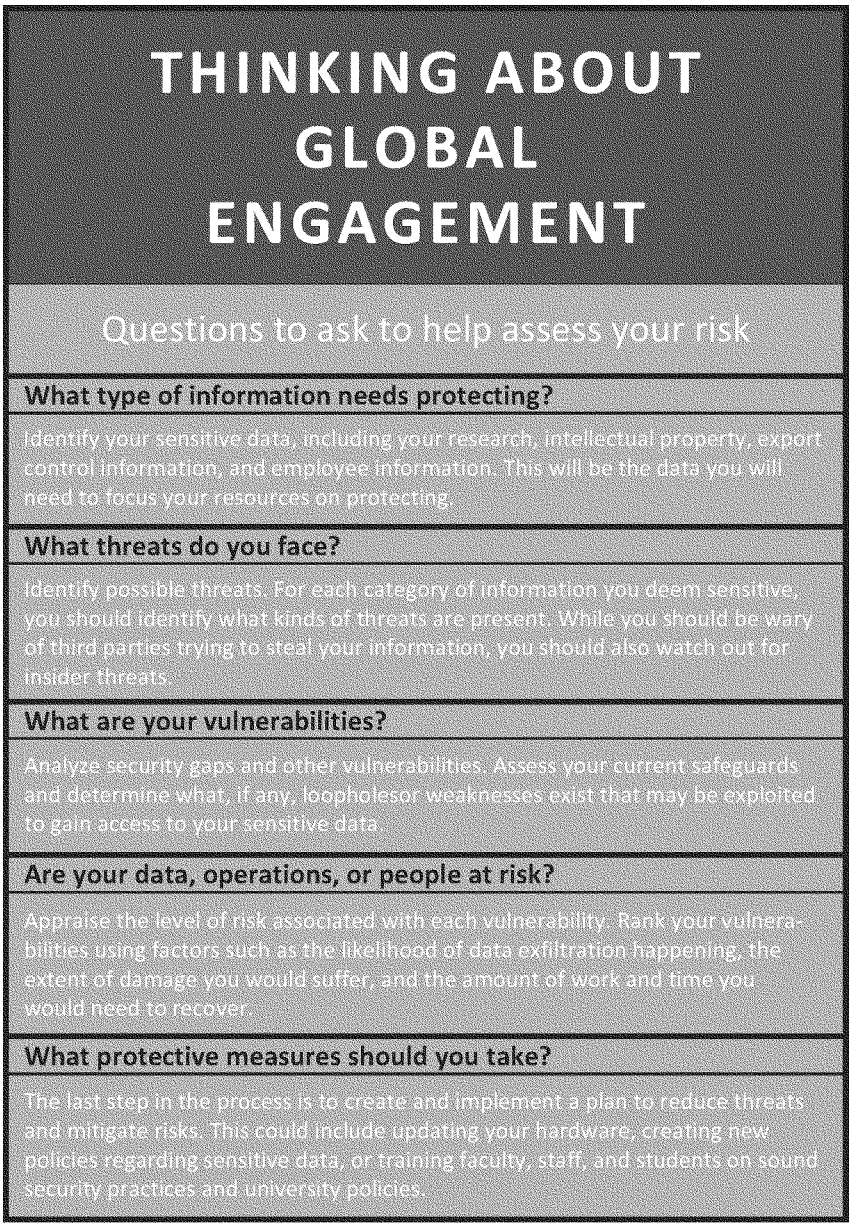


Figure 4. Thinking about Global Engagement.

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

Senator BARRASSO. The report states that a group of universities in China, known as the Seven Sons of National Defense, tying this into the military, operate as prime pathways for harvesting U.S. research and diverting it to military applications. Can you please explain why the Department still collaborates with researchers at the Seven Sons of National Defense?

Ms. FU. So I will say research security is an issue that I have long thought about and the Department has been extremely focused on since the Manhattan Project. I personally worked on research security policy in the last Administration at the Office of Science and Technology Policy. So this is an area that is critically important for our continued national competitiveness.

DOE, as a government agency—we do not have any bilateral, ongoing cooperation with Seven Sons institutions. We are aware and very clear-eyed about the risks of China's military-civil fusion policies. And that is why we have a managed research environment within the fence lines at the DOE National Labs when it comes to our science and technology risk matrix, the foreign national access screenings that we do, as well as our ban on foreign government-sponsored talent recruitment plan participation.

Senator BARRASSO. So, Dr. Kaushik, you mentioned the Seven Sons of National Defense in your testimony. What is your opinion? Should the Department just cut all ties along these lines, or is there further——

Dr. KAUSHIK. Certainly, I think no researcher being funded by any taxpayer dollars should be collaborating with any researcher at Sevens Sons of National Defense.

Senator BARRASSO. So what are several things that the Department of Energy could do better to protect advanced computing research?

Dr. KAUSHIK. I am so glad you asked that question because I think there are a lot of things that the DOE has been doing that are ahead of the curve compared to other agencies, and in fact, I have to give them credit for that—the recently released "Guidance for Implementing National Security Presidential Memorandum 33 (NSPM–33) by the OSTP. DOE is already implementing things that are ahead of that.

Now, what more can we be doing? And I think this doesn't just apply to DOE, but to the broader research ecosystem. I think we need to increase transparency here, right? We must be more forthright with the researchers about the concrete risks to our national security. Currently, we just often present warnings or hypothetical scenarios of illicit technological transfer, which is insufficient to convey the gravity of the situation. These are researchers and scientists. These are generally well-intentioned people who are analytical, who want to see more evidence to be able to see what the stakes are. An example I will give you is the MD Anderson case, which was about the NIH. They provided a clear example of a security breach, where an email explicitly directed the transfer of privileged information. And that letter was published openly. So I think such concrete examples are more persuasive than generalities.

The other thing I would say is, we need to clearly delineate basic research environments—our research environments more generally, right? We need to reassess the classification of basic research. We

need to establish clearer boundaries between open and secure environments. Now, for example, in the Air Force Research Lab in Rome, they have a facility outside the gate to interact with universities and others, whereas, everything behind the gate is doing secure research. Now, DOE does a lot of that at a lot of labs, but that needs to be the practice. That needs to be the norm.

It is not clear to me why NSF funded hypersonics research, for instance, which is considered basic research. I would be all for having basic research open if it was truly basic research, but that is not basic. And I think that is something that we need to clarify.

And then, I would say that very specific to DOE, we need to strengthen the protection of commercially relevant technologies. Now, a critical area that requires our attention is the protection of research that is conducted in partnership with commercial entities. National labs and universities frequently engage in projects with significant commercial value through mechanisms like strategic partnership opportunities or user facilities agreements. Now, current policies, whether it be the NSPM–33 or even the CHIPS Act, they do not adequately address the security concerns associated with these public-private partnerships. We need to develop more comprehensive guidelines and authorities to manage these partnerships effectively to ensure proper safeguards there. And I think this, again, extends beyond DOE facilities, but also the universities that are collaborating with major technology and pharmaceutical companies.

Senator BARRASSO. Thank you.

Mr. Chairman, my time is expired. I just wanted to comment on the last question you asked about the disposable power.

The CHAIRMAN. Right. Dispatchable.

Senator BARRASSO. And you know—I'm sorry, dispatchable power. The magazine, the Economist, says that, kind of, since the Paris Climate Accords, the U.S. has taken out about 150 gigawatts of coal-related power. China and India, 250 more gigawatts on. Why do they need it? Because of the technology, the AI, all of those things. The New York Times says five years from now the amount of energy that we are going to need in this country is equal to adding an entirely new California to the grid. Why? Because of this very reason. So we seem to be woefully behind in our ability to produce the power that we are going to need and are taking down, right now, power that can be used and needed because of the attacks from the environmental communities, but we need to be very clear-eyed about what is happening globally and what China is trying to do in terms of trying to become the military, the economic, and the technological superpower of the world. So thank you, Mr. Chairman.

The CHAIRMAN. Thank you, Senator.

Senator Hickenlooper.

Senator HICKENLOOPER. First, let me thank each of you for your service and being involved in this. Mr. Chair, I appreciate you for calling this meeting.

Let me start. Dr. Kaushik, AI obviously can improve efficiency and reliability of our electric grid in predicting and managing supply and demand. While we work toward that goal, however, the National Electric Reliability Cooperation, as well as the Bravo

Group, projected, as we have just been discussing, significant increases in demand on the grid in part from data centers that are training and running these AI systems. So Dr. Kaushik, how much do we know, and what more information do we need about what our benefit is here? In other words, how much more electricity will AI and these emerging technologies require, and how can we begin to estimate the benefits and the savings in energy that they will provide us?

Dr. KAUSHIK. Thank you, Senator. I think predicting this future demand is going to be challenging, one, because we don't have the insights into proprietary plans of companies for training new models, or sometimes they have speculative, unfulfilled requests for our new capabilities from data center vendors. But what we do know is that the International Energy Agency has predicted that the electricity demand for data centers will double by 2026—the global demand. And I think data, even if it does not double, even if it is just, you know, increasing by ten percent, we cannot take that risk. We need to be prepared for that. I think, as Dr. Gleason mentioned, that there are some reports that predict that 10 percent of global energy usage will be by AI data centers.

I think we have to reduce that uncertainty, and I believe DOE is already working on that as part of a mandate they have from the Energy Act of 2020, but I think overall, the facts of the matter on the ground are that in your home state, for instance, in Colorado, a hyperscaler recently invested in geothermal energy west of the Rockies. I think the private sector is seeing this, and they are like, we need to invest in the capabilities. Just this week, on Oracle's earnings call, they shared that they are willing to build a one-gigawatt data center and they have started the process on that. And these are things that companies are actually investing in, and I think that is a clear signal for why we need to be prepared.

Now, what needs to happen to reduce that uncertainty? I think AI can help there. We have all these earnings reports coming out. We have all these announcements from companies. We have the GIS data. We can use that to better reduce our uncertainty on how much power demand will be in particular regions. It may not be an issue nationally, but it's certainly creating strain on particular regions like Northern Virginia, for instance.

Senator HICKENLOOPER. A lot of regions, I agree completely.

Ms. Fu, the National Institute for Standards and Technology (NIST) has established the U.S. AI Safety Institute to work with government agencies and the private sector to develop metrics and benchmarks and tests that ensure AI systems are both safe and reliable. And as we have been hearing today, DOE is home to incredible technical expertise, a world-class computing infrastructure, valuable scientific data that positions the Department to be, really, a leader in all this AI research and development. Ms. Fu, could you describe how DOE collaborates with NIST and NSF and other agencies, but that collaboration to advance AI safety research which, I think, you know, we are getting the cart before the horse here a little bit.

Ms. FU. Thanks so much for that question. Certainly, AI safety and security is of key importance for DOE and for the country. This is something that the AI executive order speaks to. We have

been coordinating with commerce very closely. We are working on an MOU with the AI Safety Institute so that we can bring the expertise at DOE to bear on these questions of AI safety and security. One thing I will note is that our National Nuclear Security Administration has been focused on this issue, even before the issuance of the AI executive order because of how important it is to our mission, and they have been doing evaluations of open models and proprietary models for some time now. And we think that there is expertise that we have developed through that process that we hope to bring to bear in our cooperation with the AI Safety Institute.

With NSF, we have been working very closely to try and see where we can align some of our workforce efforts. We talked a little bit about that before, about how we can draw the line a little bit more closely between the workforce efforts they are doing at universities all across the country and the resources and training and capabilities we have at our national labs. We also are co-funding a research coordination network on privacy-enhancing technologies because we think that this is an incredibly important field of work that is important to coordinate on.

Senator HICKENLOOPER. Of course, absolutely.

And I figure there is an opportunity here for the White House Office of Science and Technology Policy to begin to help coordinate all these different efforts, because there does need to be some sort of, you know, the hive mentality has to be directed properly and coordinated.

Dr. Gleason, Colorado's Elevate Quantum recently received an award from the Department of Commerce to expand our—what we feel is the nation's leading quantum ecosystem, and Colorado companies, universities, and the workforce are determined and ready to build on this federal investment to create quantum-enabled technology that solves real-world problems in navigation, communications, computing, et cetera. Quantum computers and classical computers are most effective at solving different and distinct problems. So how will DOE bring together the different advanced computing technologies, including quantum and classical computers, to solve these, the most challenging science and technology questions?

Dr. GLEASON. So, very good question. It's a very important question. I think what I will start with is that it comes down to heterogeneity of computer systems. So what I mean by that is, bringing different computing technologies together to bear that can attack different parts of a problem where they are the most efficient technology to attack that piece of the overall challenge. And I will just use history as an example. So high-performance computing used to be CPU-focused only. Then, they became more heterogenous by adding GPUs.

Senator HICKENLOOPER. Right.

Dr. GLEASON. And GPUs are very good at AI training, et cetera. CPU is good at modeling and simulations. So there is an example of where heterogeneous computing can be used to attack different types of problems, different parts of a problem.

I think the future—one of the things that DOE and the national labs are very focused on are what are the next versions of heterogenous computing that are on the horizon. And you have already mentioned one. We talked a lot about quantum recently in this

hearing. Quantum computers are very good at solving optimization problems, for example. Logistics problems. They are very good at simulating molecular dynamics or chemistry because of the nature of the quantum mechanics that are used to drive the quantum computers. So integrating classical HPC with future quantum computers, I think, is a really important thing that the Department and the national labs need to look at, and that is a big challenge. How do you integrate these very different types of architectures that run with very different software stacks and software platforms? How do they connect together? How do they communicate? And how do you make a quantum co-processor, for example, that lives in a data center with a frontier supercomputer and takes on some of these challenging parts of the problem, probably in a more energy efficient way and probably faster? Other technologies—neuromorphic computing is another good example of another heterogeneous option. Neuromorphic co-processors can also tackle unique challenges.

And so, and then, I think there are computational architectures that we haven't even thought of yet, and the Department of Energy is exploring and the labs are exploring what those might be, but I think increasing the heterogeneity is one really strong path that DOE and the labs should follow.

Senator HICKENLOOPER. I think we are going to need several more hearings to really explore this thoroughly.

Senator KING [presiding]. On behalf of the Chairman, Senator Hawley.

Senator HAWLEY. Thank you very much, Senator King. Thanks to all the witnesses for being here.

Dr. Gleason, if I could just start with you. I just want to start with a question about Oak Ridge National Lab, since you are here from that institution. You have worked there for more than 30 years, is that right? Thirty-four I think you said in your opening statement. Do you mind if I ask, do you happen to live in the area as well?

Dr. GLEASON. I do.

Senator HAWLEY. Here is why I am asking. You are probably familiar with the role of Oak Ridge in the Manhattan Project, I bet. Is that fair to say?

Dr. GLEASON. I am, yes.

Senator HAWLEY. Could you just give us, for the benefit of those who are watching the hearing, could you just give us a thumbnail sketch of what Oak Ridge did for the country, to the extent that you know it? It doesn't need to be detailed, but just give us a synopsis of what Oak Ridge did for the country during the Manhattan Project?

Dr. GLEASON. Yes, I mean, Oak Ridge, you know, was stood up in the early 40s to try to help build the nuclear material that would power the bomb. So we built the world's first continuously operating nuclear reactor, called the Graphite Reactor, which is part of that process. The Graphite Reactor is no longer operational but you can go look at it. It is a wonderful tour stop when you come to Oak Ridge, but we are very proud of our roots in the Manhattan Project and it continues to inform our national security mission, part of what we do. We do Office of Science work. We do national

security work. But our roots in the Manhattan Project—one of the big areas that came out of that was our materials science strength. And we have a huge pillar and strength in materials science that's roots go back to that Manhattan Project and Oak Ridge's contributions.

Senator HAWLEY. Very good, thank you for that.

I asked because Oak Ridge was such a critical part of the Manhattan Project, as you say, and the Oppenheimer movie of this last year, I think, raised awareness about what that project looked like and how it got started and the importance of Los Alamos, but really at Oak Ridge, you know, the government produced plutonium and then there were other uranium processing sites around the country, including in my home State of Missouri, in St. Louis. And as you probably know, in both Oak Ridge and St. Louis, despite the fantastic vital contributions of those processing plants, facilities, and labs to our national security, the nuclear waste was not properly disposed of in either place, and in Oak Ridge, the effects on the community have been severe. And I just want to quote from another one of your fellow residents there in the Oak Ridge area—Tanvi Kardile is her name. She is the coordinator for the Oak Ridge Environmental Peace Alliance, who has said that, "It is time that people in Oak Ridge receive compensation for being exposed to radiation from nuclear waste." And now, Oak Ridge, as we speak, is a Superfund site, and that is good. It is well long overdue that it be cleaned up, but not only should it be cleaned up, those folks, your neighbors in the area who have been exposed to nuclear radiation over the years, ought to be compensated for it, just like in the city and region of St. Louis.

And I bring all of this up because this body, to its credit, passed legislation that would compensate the good folks of Oak Ridge and the St. Louis area and other similar nuclear sites and other folks who were exposed to downwind testing during the Manhattan era and the Cold War era. We passed that legislation by 69 votes. And I look across the aisle, Senator King voted for that. I appreciate that, Senator. And many—most of my colleagues, it was a huge vote. It's now in the House of Representatives. And I just, having you here from Oak Ridge, considering everything Oak Ridge and the entire region there that you work at has done for this country, I couldn't let the opportunity pass to thank the good people of Oak Ridge, to thank the scientists that you work with, to thank that community, and also to call on my colleagues in the House to pass this legislation. Compensate these good Americans, who bore the brunt of our effort in the Second World War and the Cold War, which we won because of the effort of people at Oak Ridge and in St. Louis, and the residents who weren't themselves scientists but lived in the area and have suffered the effects of the nuclear radiation—they are proud to be Americans and to have served in this effort. They deserve compensation, however, just as they deserve to have their communities cleaned up.

So thank you, Dr. Gleason, for testifying about the significance of that.

Dr. Kaushik, if I could just come to you in my remaining moments here, just about the dangers posed by China and AI. You highlighted in your opening statement—your written statement—

the 2017 National Intelligence Law in the PRC requiring Chinese citizens and organizations to share information with state intelligence. Can you just speak to the dangers of American AI companies doing business with China, investing in Chinese AI, partnering with the Chinese businesses, whether overtly state-controlled or not? Can you speak to that a little bit?

Dr. KAUSHIK. Senator, thank you for that question. I think it hits right at the heart of the argument on economic security and national security. I think American businesses doing business in the PRC—at one point, our government promoted them to do it, and that is okay, like, that was our understanding of the PRC back then. Things have changed. And today, if a company goes and invests in China, what they are doing is inherently supporting their economy, inherently supporting an authoritarian regime. They don't know whether what they are investing in is also fueling slave labor in Xinjiang. I think that is an important consideration for any American company who wants to invest in other countries—they have to take that into account.

We have to be realistic about what is happening. We cannot live in a dreamland of the China we want to operate with. We don't control that. We control what is the China that we are operating with.

Senator HAWLEY. I am so glad to hear that from you, and I hope that every corporate CEO will listen and take to heart the words you just said. I asked partly because I just had the opportunity to talk with an Intel executive who was testifying at a different committee. Intel, of course, is investing billions in China, and in Chinese AI, in particular. And this executive argued to me—this was just 48 hours ago—argued to me that this is of great benefit to the United States. There are no security concerns with it at all. It's really good for America. But the telling thing was, you mentioned the Uyghurs—Xinjiang Province. He would not condemn the persecution of the Uyghurs. He said, "you know, well, I just—I can't speak to that. It's unclear if there really is any forced labor in China." This, I think, is, frankly, the moral hazard that our companies face if they do business in China. If they find themselves compromised by the PRC, they are effectively—they run the risk of supporting slave labor, of helping the Chinese AI program in a way that is materially to our detriment, but is also, frankly, just morally wrong.

So thank you for your clarity on that. And I just think these companies, these so-called American companies, it's time that they actually did something for the values that we cherish as Americans, and ending slave labor ought to be at the very top of that list. And I, frankly, am sick of these companies taking billions—Intel is getting billions—$8.5 billion—just approved to go to Intel under recent laws that this body has passed. And yet, they are turning around and spending billions in China, and won't condemn slave labor—in fact, they may be benefiting from it. And I just think that's wrong.

I see my time is expired. I have a couple more questions for you, Dr. Kaushik, just about safeguarding our national labs. So I will give those to you as written questions.

Thank you, Mr. Chair.

The CHAIRMAN [presiding]. We might have a second round too, if you can stay, okay?

Senator Cortez Masto.

Senator CORTEZ MASTO. Thank you. I want to thank the Chairman and Ranking Member for this conversation. I love this chart, by the way, thank you.

I understand one of my colleagues talked about it, but I am just going to put a finer point on this because I understand that this conversation just highlights the fact that a rapid increase in projected electricity demand is happening because of AI and because of data centers. And I know this in Nevada because we actually have both happening here, and we are a major hub for data centers. You just had conversations with Switch in my state on this very topic. So I am very interested in how we address that demand. And I think it is everybody's responsibility to figure this out if we want to lead in this country in emerging technology, right? So if you have any additional information, I would love to hear it, on how we address and be a part of the solution here to address that emerging demand as well.

Ms. Fu.

Ms. FU. Yes, this is something, as I mentioned earlier, something that the Department is laser-focused on. And I think it is due to our role in leadership in advanced computing, understanding what the energy needs of AI will be, but also in our role with the energy part of our name. We see an enormous opportunity here. It is true that energy demand is growing. It is doubling. Energy demand from data centers is doubling from a very low base. However, it is a local issue that we need to really get our heads around. We think that DOE has a really unique role here in helping to convene stakeholders. This is something that the Secretary has been thinking through. She has charged her Secretary of Energy Advisory Board to look at this issue and they recently came out with recommendations. We would be happy to share them. We are starting to implement and look through those recommendations to see what we can do. We will be convening stakeholders around the country in areas of high load-growth. This is going to be an effort over the next several months.

We do think that there are things that we can do now. And I think part of the challenge with AI load-growth is that it's both a very large load and the expectations are very fast, you know, this large load is going to come online in the next—now, through the next few years. And so, we have many different kinds of technologies that we are looking at that are going out to 2030. We are doing everything that we can to look at what we can unlock now.

Permitting, of course, is one piece of that. We actually have an AI and permitting pilot that we have already launched to see how we can use AI to expedite and streamline the permitting process. And one of the things that we have been able to do is to take the entire corpus of NEPA documents, which normally go in a huge binder and they get put on the shelf, and make them AI-ready, digitize them, and make them available to the entire scientific community and to industry to develop new tools to help with this process.

But we know that there are near-term needs, mid-term needs, and longer-term needs, and DOE is focused on all of those.

Senator CORTEZ MASTO. And I know you are, because of your footprint in Nevada, by the way. And so, thank you. My only ask is, and you talked a little bit about it, you invite industry in to have them as part of the solution. I talk with the CEO of Switch regularly, and I just talked to him about this issue. They have ideas.

Ms. FU. Yes.

Senator CORTEZ MASTO. Right. And so, they should be part of this discussion.

Ms. FU. Absolutely.

Senator CORTEZ MASTO. Nevada is a perfect place to have this discussion because of DOE's footprint, but also there is this nexus between energy and water and the challenges we have there. There is also, in Nevada, a large footprint just of the Federal Government that should be partnering with the state and private sector in figuring this out. And for that reason, I am hoping DOE is also partnering with the Department of Interior. You talked a little bit about permitting, but it's Department of Interior that has/owns a lot of the land, right? So I am hoping that—and can you talk about that? Is there that partnership that is happening with other federal agencies, including the Department of Interior?

Ms. FU. Yes, there is a lot of focus on this. We are working through the CEQ that is convening the interagency body. I will say the AI and permitting pilot, we are working with the 13 agencies in the permitting council on this issue. And we recently, through Savannah River National Lab, issued an RFI that looks at potentially siting data centers, even on federal land.

Senator CORTEZ MASTO. Okay.

Ms. FU. So we are looking at all of these issues, looking at all of these options. We understand the urgency of the issue.

Senator CORTEZ MASTO. Okay.

And the only other stakeholder that must—must be at the table is our state and local folks, right, because we manage our economic development, our population growth, our needs with the Federal Government because the Federal Government owns most of the land in the state. So I am hoping that you pull our folks in as well in this conversation. It is crucial. Thank you.

You talked a little bit about the workforce that we need for the future. What else should we be aware of here in Congress that we have to focus on, particularly for that workforce of the future that is going to kind of lead and be a part of these emerging technologies? Anything that we didn't talk about that I need to know, or we need to know?

Dr. KAUSHIK. Happy to take that on. I think, Senator, that is an incredibly important question that is at the heart of this conversation. The population of the PRC is four times ours.

Senator CORTEZ MASTO. Right.

Dr. KAUSHIK. They are producing four times as many bachelor's degree holders in STEM, twice as many master's and twice as many Ph.D.s. This is not a competition that we faced in the Cold War. The population of the Soviet Union was nearly as much as ours. The economy was far below, and here the population is much

higher, much more talent to tap into, and they have these sophisticated programs and they are trying to bring more talent into their country. I will give you an example. They have this national innovation-driven development strategy, which aims for the PRC to become a key hub for global high-end talent by 2050. Now, they have changed their visa and permanent residency programs. They have established a "thousand foreign talents" program, alongside the Thousand Talents Program, to recruit foreign nationals to China. And I think we need to have a talent strategy here.

What does our talent strategy look like? DOE has some fellowships for U.S. nationals. I think NSF has their own fellowships. Agencies have their work cut out here, but at the same time, there is a big chokehold that only this body can solve, and that is—I will quote the Singaporean leader, Lee Kuan Yew, who said when he was asked whether he thought China would overtake the United States in the 21st century, he said, "No, because the United States has long attracted the world's best and brightest." He said that the United States fosters a diverse culture of creativity, and China will struggle to do so. Despite having 1.3 billion people to tap into, the United States has seven billion to tap into because we can assemble a rest-of-the-world team. But I think you see that in AI today. Sixty-five percent of the top AI startups have at least one person as a founder or co-founder who came here through legal immigration means. I think that has to be an important part of the conversation on workforce.

So we need an all-of-the-above approach here to be able to match the numbers that they are putting out in STEM Ph.D.s and STEM master's and bachelor's.

Senator CORTEZ MASTO. And then finally, and I agree, but that can be done, Dr. Kaushik, with what your caution was before of how do we secure it? How do we ensure that we are securing the technology, right, for our use in our labs? There is a way to balance it and you believe that can be done?

Dr. KAUSHIK. Absolutely. There are, you know, the guardrails I talk about, most of them are objectively laid out in what we call the National Security Decision Directive 189, which was issued during the Reagan Administration during the Cold War, about protecting American technological advantage. The National Academies also did a report in 2022 at the direction of this body on protecting U.S. technological advantage, and they said that it is possible. Now, what do we need to do to actually get there? I think we have to recognize the competition is a bit different. You know, we cannot continue funding hypersonics research as basic research and saying that we will make that openly accessible, right? We have to classify the research when it needs to be classified. We have to have that conversation.

A risk matrix cannot be a silver bullet. We have to have a prior conversation on what is okay to be made openly accessible and what needs to be behind closed doors, who should have access to certain research and who should not. And I think we need to be very careful about whether it is even people from our partner and allied countries to be able to have access to those, you know, those technologies that we are researching that are of a sensitive nature. It's not just about preventing PRC access to those technologies.

Sometimes we just don't want the fact that we are developing those technologies disclosed. I think there is a way we can balance that, and I think NSPM–33 does a really good job at it. It was produced by the Trump Administration as an all-of-government approach. The Biden Administration, to its credit, has continued working on it. Despite OSTP's massive delays in releasing implementation guidance, it is the right approach. The Trump Administration also issued the Presidential Proclamation 10043, which bars the entry of certain Chinese graduate and postgraduate students who have ties to military-civil fusion institutions. And I think that is taking a scalpel rather than a sledgehammer to this and that is the right way to go about it.

Senator CORTEZ MASTO. Okay, thank you.

The CHAIRMAN. Senator King.

Senator KING. Thank you, Mr. Chairman.

As we have been sitting here, a few minutes ago, I asked a question of ChatGPT-4, and the prompt was "give me a poem in the style of Robert W. Service about the U.S. Senate Committee on Energy and Natural Resources." Okay, Robert W. Service is my favorite poet. He wrote about the Gold Rush, and wrote "The Cremation of Sam McGee" and "The Shooting of Dan McGrew." Anyway, that was what I asked. In three seconds, this is what I got back:

"In the hallowed halls of Congress where the mighty stand so tall, there is a group that tends the nation's needs, its energy and all. The Senate committee gathers round with purpose in their eyes, for the fires of coal and sun and wind they seek to harmonize. Old Service might have marveled, for their work is just as bold as the gold rush tales he spun so well of lands both harsh and cold. They wrestle with the power lines, the drilling, and the frack, the forests and the oceans deep and what they give us back. Oh, the Senator from Texas . . ." and by the way, this proves AI isn't always right, there is no senator from Texas on this committee, ". . . with a mind on oil's flow, speaks of wealth beneath the earth and profits yet to grow . . ." listen to this: ". . . but across the room a voice rings clear from Maine's wild rocky shore, there is wind upon the sea my friend, we must demand much more. The coal fields of Wyoming, the pipelines out of sight, they spar with solar panels shining clean and bright, and as they hash their quarrels out with power in debate, the future of the nation's grid they strive to navigate."

Isn't this amazing? This was three seconds. It continues: ". . . yet all the while the rivers run, the mountain stands so high, the forests whisper ancient tales beneath the open sky, and those who sit and legislate with duty on their chest know nature's gift is fleeting and they must do their best. So let them weigh the costs and gain. Let compromise be found, for in the hands of those who lead the nation's fate is bound. And like the miner seeking gold and Service's rugged lore, the Senate digs for answers deep on nature's precious shore."

That is what AI can do, which I think is absolutely astounding, but the fact that it made a mistake, I think, is also a cautionary tale.

Okay, Senator Barrasso was talking about the electricity issue and the coming problems, and that is one of the reasons we are

supporting—I don't know if you know, but two weeks ago we reported out a comprehensive permitting bill in order to unleash the power, particularly of renewables, because without transmission we are not going to have those resources.

Okay, one question on quantum computing and advanced computing, and I don't want to pursue this too deeply, but I want to be sure, Ms. Fu, that we are not duplicating. There are other people in the U.S. Government working on this problem and I just want to be sure that there is coordination, and you don't have to go into any detail, but assure me that you know what is going on in other agencies and that we are doing this, because this is an expensive proposition, that we are not duplicating and overlapping because of competing jurisdictions.

Ms. FU. We are not duplicating. We are working closely with the White House National Quantum Coordination Office, and working closely with other agencies on this issue. And I think what we talked about earlier around AI, you know, and where DOE plays a role is around developing the capability. And so, the foundries that we are developing, the testbeds, the different kinds of user access programs, these are things that only DOE can do. We work with other agencies to build up the broader ecosystem, but the large-scale science and the facility side of this issue is something that is a DOE strength.

Senator KING. Well, please keep an eye on that issue.

Ms. FU. Absolutely.

Senator KING. And in the context of this Committee, are there ways that AI can assist us in the more efficient allocation of power, the more efficient running of the grid? There is a lot of inefficiency on the grid today, and we are developing what are called GETs—grid-enhancing technologies. I think that a complex system like the grid, and by the way, we need to distinguish between power and the grid, between capacity and the wires. But can AI be helpful to us in more efficiently managing the grid?

Ms. FU. It can, and I think just taking it back to the poem that you wrote with ChatGPT earlier, I think that is a really good example. ChatGPT and all of the commercial large language models were trained on human-generated information off the entirety of the internet. And the kinds of things that we are talking about in our FASST proposal are not training on the internet. It's not training human-generated data. It is training on scientific data where we can trust the provenance of that data and it can follow the laws of math or biology or physics. And so, when we look at the grid and we look at the things that we are going to need, and that is a very, very high-consequence use-case, this is lights on or lights off. We need to 100 percent have trust in where the data is coming from to train this and what——

Senator KING. I am assuming it's trustworthy data, my point is, analyzing massive data about how the grid is operating will enable us to operate it more efficiently. Is that correct?

Ms. FU. Yes, we think that there is a huge use-case on using AI to look at how we control massive systems like the electric grid.

Senator KING. Thank you.

Final point, and we have touched on this—we just did. Dr. Kaushik, how much talent are we losing because of our not-very-

functional immigration system and, you know, the quote from Lee, Kuan Yew, who is a genius, is very appropriate, but my sense is it used to be a lot of foreign students would come to the U.S., they would get a graduate degree from Stanford or Notre Dame or NYU and they would stay. Now they are leaving. Now we are making it harder for them to stay. How do we open up this system safely? I understand there are security concerns, but my sense is we are losing a lot of talent.

Dr. KAUSHIK. Certainly, Senator. I think there was a recent study that was done which found that over 50 percent of AI Ph.D. graduates who leave the country cite that as the reason why they are leaving the country.

Senator KING. Because of the immigration laws?

Dr. KAUSHIK. Yes.

Senator KING. So there is a pile of talent who we are chasing away?

Dr. KAUSHIK. Correct. And many of them are from nations which we consider as partners and allies. I think that is something that we have to recognize, that there is——

Senator KING. So we are doing this not only to Chinese people, or Russian people, but we are doing it to Australians or people from France or Germany.

Dr. KAUSHIK. Correct, yes, Senator.

Senator KING. That is just crazy.

Dr. KAUSHIK. That is totally the case. In fact, the CCP recognizes this, and I am going to give you some quotes directly from them where commenting on the U.S. retention of Chinese STEM students, I will just say, the head of CCP's Central Talent Work Coordination Group complained that the number of talents lost in China ranks first in the world. But now, if you look at their data—granted all the issues in their data—the fraction of the Chinese students who are returning home is increasing despite long-term stay rates. If you look at students from the PRC who graduated from U.S. universities in 2015, over 90 percent of them are still in the United States, but that number is declining overall, especially at the undergraduate level, it's declining a lot.

A state-run consulting firm wrote in an AI policy white paper in China that U.S. restrictions on immigration have provided China opportunities to bolster its ranks of high-end talent.

Senator KING. Brilliant.

Dr. KAUSHIK. These are direct quotes from the Chinese Communist Party.

Senator KING. Shouldn't we—assuming sufficient security analysis—shouldn't we just staple a green card to diplomas?

Dr. KAUSHIK. I think, Senator, that is a worthy consideration. I would say that we do need security provisions attached, like some of the provisions that were under consideration here in the CHIPS and Science Act, for instance, of applying sanctions to people who are found guilty of economic or industrial espionage or academic espionage. I think that is something that we should be——

Senator KING. We can deal with that and that is a small percentage.

Dr. KAUSHIK. Correct.

Senator KING. In terms of gaining a huge amount of talent that will drive this country into the future.

Dr. KAUSHIK. I think what you are saying is absolutely right, and this is what Bill Evanina, who was a former counterintelligence chief in the previous administration, also said that we bring about 350,000 Chinese students here every year. We have very liberal student visa policies for them. About one in a thousand of them are bad-faith actors, and so we need that scalpel-based approach to remove that one out of a thousand rather than shutting the door on all 350,000. And I think that is the right approach that the Trump Administration took with its Presidential Proclamation 10043 and NSPM–33 and the likes. I think there are obviously still a lot of issues that we need to deal with and that can be done. At the same time, we—I think it was Senator Cantwell who said during the CHIPS and Science Act that either we recognize this problem today or we will wake up in ten years and China will be ahead in everything and we will have no time to work on it.

Senator KING. Thank you.

Thank you, Mr. Chairman.

The CHAIRMAN. Thank you.

Senator Murkowski.

Senator MURKOWSKI. Thank you, Mr. Chairman and thank you to those of you who have been part of the conversation here this morning.

Mr. Chairman, I want to thank you for your leadership and inviting me to join you with the Department of Energy AI Act that we are working to advance to make sure that DOE has the tools that are necessary to really leverage some of the benefits here of AI. I look forward to being able to advance that and also to be supportive of the measure that Senator Daines is introducing, the DOE Quantum Leadership Act of 2024, I think all good measures that just add to the toolbox here.

Senator King, I sit in just amazement of what you shared. Although, I will say that the "The Shooting of Dan McGrew" was still one of Robert Service's finer pieces of work, and I think he would have been offended by the——

Senator KING. "A bunch of the boys were . . ."

Senator MURKOWSKI. ". . . whooping it up in the Malamute Saloon." Yeah, we could go on, and I will regale you with my Robert Service. It's one of my favorites, so you made me smile here this morning.

I want to ask a little bit more about application of these technologies. There has been a lot of focus in the Committee here on national defense, competitiveness issues, power grid resilience, and as Senator King mentioned, efficiencies. Talk to me a little bit about how we can utilize these technologies in other fields, whether it's resource exploration, disaster prediction, climate resilience, adaptation planning. Let me share with you—I had a meeting just yesterday with some scientists from Woodwell, focused on what they call the Permafrost Pathways. And it's essentially utilizing available mapping to understand and determine where we have greater vulnerabilities, whether it is with releases of carbon, as we are seeing the permafrost melt or just the application in whether or not you would even think to put a community or a structure

there, and a lot of discussion about where the data is. As scientists, are they able to access the public repositories? You know, BLM does certain analysis, or a service in Alaska does analysis. What is available to them and how would their work be facilitated in other ways? And I think exactly about some of what we are talking about here.

The other thing that I will ask you to think about and help me with, we had a deadly landslide in my hometown of Ketchikan just a few weeks ago. This is an area in a neighborhood where my family grew up, had the same house for 60 years, and not in an area that is prone to landslide, and yet, as we are seeing more intense weather, we are seeing these impacts in our communities that are really quite frightening. And so, we are asking what mapping have we done? What monitoring is going on in terms of precipitation?

And we are told that, well, at the place that we were at the day of the landslide, the rainfall was somewhere between six and eight inches that day, whereas the weather monitoring station, which is right across—maybe a half a mile away, is less than two inches. Still a rainy day. And so, we are talking about—we have these tools that are out here, but who is able to communicate with who? And I am giving you a rambling open-ended question, but I have a lot of problems that we are looking to solve on the disaster side, or just preparedness awareness, but also with being able to utilize some of the public data that is out there as we are trying to assess is there greater potential for a critical mineral in this area, and do we need to do the actual drilling or can we extrapolate from these tools and these technologies?

Have at it.

Ms. FU. Thank you so much. And these are all super-important questions and real application spaces for AI. And I will just give a few examples of where this might be useful. Climate modeling and environmental research—you mentioned earlier the ability to look at vast datasets from the Arctic region, including sensor and satellite data to understand permafrost thaw and changes in the ecosystem. This is work that PNNL and Oak Ridge are already engaged in.

AI for energy resilience—this is an area where we look at how we can optimize energy systems for remote communities. And we know that NREL is doing quite a lot of work in that space where we can look at energy demand, plan out where storage should be and reduce dependence on costly diesel fuel. These are things that I think can be very impactful for everyday people.

There is also, obviously, AI for infrastructure monitoring, and this is work that Sandia has underway, looking at AI to monitor critical infrastructure, like pipelines and transportation, especially in remote areas where it will be hard for people to go to regularly.

So to your point around data, this is an incredibly important issue. We talked a little bit about what we are doing on AI and permitting data, especially NEPA data, making it AI-ready. I think it was millions and millions of pages that we were able to make AI-ready so that it could be used more broadly for tools and application development. I think there is an opportunity to do this across this entire spectrum, from climate data, energy data, the whole grid—the grid questions here—and knit them together. And that is

part of what we are thinking about through FASST. How do we get all of the different stores of data—data we collect, as well as public data—and make them actually useful, because I think poems are great, and these tools that we have commercially available today are really great for efficiencies and they are really great for language, but the kinds of problems that we have are going to be hard scientific problems that will then need to be applied to real-world situations.

Senator MURKOWSKI. Well, I appreciate that, and I am thinking about the application to the Department of Defense. Right now, on Alaska's coastline, we have some older military assets that are greatly threatened by what we are seeing with coastal erosion. And you have to make decisions, expensive decisions about do we stay there, do we relocate, and you want to make sure that the decisions that you are making are going to be in place for more than just the next decade. It has to be more long-term, so, the tools that we have to put in place.

Dr. Kaushik, you wanted to——

Dr. KAUSHIK. Sure, Senator, I think that is exactly the kind of work we should be doing at the Federal Government level where it's not necessarily like the private sector has incentives to build those kinds of tools. They don't have the data. They don't have the sensitive data. I think, for instance, NOAA collects about a terabyte of data every day that nobody ever gets to see. I think that is something that we can be doing, but at the same time, there are some private-sector actors who are working on this, like NVIDIA developed a digital twin of the Earth, right? And what that allows them to do is conduct millions of simulations of extreme weather events, compared to what we can today do, which is like just about thousands of simulations to see, to better predict the weather.

Another area where I think we need to think about what the national labs could be doing is, like the Pacific Northwest National Laboratory is working on this idea called Cloud Labs, right? We have changed dramatically how we work in every sector since the industrial revolution, but science has still stayed the same. You go into a lab, you prep your chemicals, you do it how you do it. A cloud lab allows you to automate how to do scientific discovery. You can run experiments at scale. They are more applicable. They can be run faster, with more precision. And I think the same goes with how we explore critical minerals. It's a very CapEx-heavy stage at the exploration level. And I think USGS has a program on that where you are using AI along with radar data to understand better what kinds of materials may be underneath the Earth.

And I think all of those things, not necessarily—the private sector has near-term incentives to invest in or develop. And I think those are the kinds of things that generally people look to the Federal Government for.

Senator MURKOWSKI. Dr. Gleason.

Dr. GLEASON. I just wanted to touch on something Helena mentioned, which is the data problem, and you touched on it as well. Making sure that data is AI-ready is a huge undertaking. A lot of people underestimate the challenge. You know, you could have a lot of data, but it's not valuable until it is made AI-ready. It has to

be organized. It has to be labeled in some cases, sometimes not, but it has to be ready to train an AI system. So there is a huge part of FASST which is to make data AI-ready, and public data, scientific data from the national labs, a very important challenge that's not the most exciting piece of the work, but it's really the most important because data is the fuel for the AI engine.

The other thing I just wanted to mention, just as an example, is something we are doing in disaster response and disaster recovery is, Oak Ridge is stitching together satellite images from across the entire world and then mapping the actual building infrastructure from those images, in fact, to the point where we are predicting some of the materials that those buildings may be made of from the spectral reflections and the information in the satellite image. The cool thing about that is, now you can, if you see a disaster, predicted disaster, from a climate model or even a military situation, you can understand what the affects might be, and after it happens you can do a before and after comparison and decide where do I need to direct my emergency resources most effectively, most quickly, to save the most people, restore function, et cetera. So AI is a huge tool to help those kinds of things that are connected to some of the things you mentioned earlier.

Senator MURKOWSKI. Fascinating.

Senator KING [presiding]. On behalf of the Chairman, the distinguished former Governor and current Senator from the State of North Dakota.

Senator HOEVEN. Thanks, Governor, appreciate it.

Thanks to all the witnesses for being here. And my question for all of you is, you know, there are probably a lot of metrics we use to measure AI. What are the most relevant metrics? For example, if we are saying, okay, how do we compare it to China or someone else in terms of where we are with AI, what are the metrics that we use to measure who is ahead and why it matters?

And then my second question is going to be how do we really manage the security, not only for ourselves, but you know, how do we address the security issues for others that are developing AI, be it China or anyone else? And you know, you have this great workforce and you get them, you know, all trained up on this stuff and they develop it, and I am guessing there are a lot of folks in a lot of other countries that decide they want to hire them and are offering some pretty big wages and so forth to have them come over and it may be for malign purposes.

So first, the metrics, how you measure them, why it's important, and then the security aspects, both for us here and for our adversaries and particularly regarding the workforce that you are developing and training.

Ms. FU. Thank you so much for that question. These are all things that we are thinking very deeply about at the Department of Energy. On metrics, the AI executive order refers to how much power is used to train the model, or FLOPS. So in the AI executive order it refers to 10 to the 26th as the amount of power that is used to train some of the most powerful models that are here today. Now, is power or the amount of money that you spend to train a model a good metric for capability?

Senator HOEVEN. It's just an input.

Ms. FU. It's imperfect. It's imperfect, and we recognize that. And I think what we are doing at the Department and across the interagency as well is thinking about what other ways of identifying model capability there are. I mean, one way to look at it is the data that is used to train the models. It's not always the size that counts, it's how useful that model is. And I will point to work that is underway across many of the national labs, but work that we are doing on red-teaming of open-source as well as proprietary models through our National Nuclear Security Administration. This is an area of intense work where we are pairing our data scientists with our experts in radiological and nuclear expertise to really understand how capable some of these models are relative to each other. And that is work that we hope to bring to the work of the AI Safety Institute to help inform that effort.

More broadly, around the workforce issues, I think this is incredibly important. We have a managed research environment within the DOE national labs to look at risk across a continuum. Of course, for classified work, we have extreme restrictions on that. We have a science and technology risk matrix that looks across different areas of critical and emerging technology and we use that to help guide who works on what kinds of projects. We also screen foreign nationals who come into the labs.

Now, to your point of, well, once they are in the labs and what if they leave, what if they take that knowledge, the training and go somewhere else, to industry or elsewhere? And I think that is part of the U.S. open ecosystem. We can't control where people go. We can take measures while they are in our system. And I think it calls for why the capabilities that we have at DOE attract talent from all over the world, because they are unique facilities. We have people at the labs who come to the United States because of that facility, because of that supercomputer, or because of that neutron source. And the investments that we are making at DOE and our national labs continue to keep that center of gravity for talent here in the United States.

Senator HOEVEN. Yes, I mean, I would argue that, you know, China or somebody else could actually want to develop people that come here and train under you, learn everything you have got, all your advanced technologies, and go back home and make sure that they have access to all that information and everything else and that capability.

Ms. FU. So I would say we are extremely clear-eyed about those threats, and that is why we have a managed research environment. That is why we work very closely with our Office of Intelligence and Counter Intelligence. We have our eyes wide open to those things and that is why we focus on where people have access to, even when they come to the lab, the kind of research that they are focused on, the kind of access that they have at the national lab. It's not a free-for-all once they come through. We have ongoing efforts underway. We have training. People understand what those risks are and there is an ecosystem around our labs to make sure that we are managing those risks properly.

Senator HOEVEN. Are you seeing people leave and go to other countries?

Ms. FU. I mean, we are seeing people leave and go to other companies. There is really a competition for talent in these areas of critical and emerging technology. If you speak to companies, they will say they can't hire enough people to do that. And I think if you talk to our national labs, they will say the same. I think the things that attract people to DOE are mission and the access to the kinds of resources that we have. But that leadership is not assured. That leadership is not assured, and people—other companies—are paying quite a lot more than what DOE national labs are paying, but people come to us because of the mission, the work that we do.

Senator HOEVEN. Right.

Dr. GLEASON. Just as a leader of a few organizations where I have tried to hire and retain talent across these emerging technologies, it is a big challenge. You know, recruiting—we need to increase our domestic workforce, the supply. In terms of retention, my personal experience is we have lost less to other countries, I can't even think of specific examples, but we lose a lot to industry. And I would rather lose to industry in the U.S. that is, you know, creating new AI technology that will advance the cause of the United States, but it is a challenge. And as Helena said, the ones that stay at the national lab for the long haul are the ones that are motivated by the mission. They love the lab mission and they love to work at a place where they can explore science and technology objectively without a profit motivation, which is a good motivation, but that's not why you come to the national lab.

So I just wanted to echo what she said our challenge is, which is recruiting domestic talent with, you know, U.S. citizenship in the STEM fields. So one thing Oak Ridge is doing a lot, and other labs are doing this as well, is engaging in middle school, in high school. By the time they get to college, you are almost too late, right, because they have already decided their path. But having our scientists go mentor at local schools to try to encourage young men and women to enter STEM fields because we have such a huge shortage of that. So I think that is a big thing we need to focus on.

Dr. KAUSHIK. I will just add to that, Senator. On metrics, I think no metric will give you a perfect picture. Every metric is targeting a different conversation, like, when you look at papers, you are asking about who is ahead in more basic research. When you are looking at commercialization, how many users are using iFLYTEK AI in the PRC actually outpaces how many people are using AI in the United States. But at the same time, nobody can dispute that the capabilities of our frontier AI model providers, whether it's Open AI, Anthropic, Meta and all those, are undisputedly in the lead. That said, their development of DeepSeek, which used to be, by the way, a financial firm in China, which the Chinese government said you have to work on AI now. And now they are churning out such amazing models—they actually publish all their results, and we can see that their results are actually very competitive to our models. You look at Huawei's new AI chip, which outperforms NVIDIA's A100 on several metrics. So there is an aggregate of statistics that we probably need to be looking at here, an aggregate of metrics.

I think on the talent side, like, I think the labs are really great at recruiting mission-driven, focused people. At the same time, like, you can put, you know, you can have all the fancy knives in a restaurant, but if you don't have the Michelin-star chefs, you are not going to make a good meal. And I think that is the challenge the labs have to deal with.

Senator HOEVEN. Thank you, all three of you.

The CHAIRMAN [presiding]. Thank you, Senator.

Senator Daines.

Senator DAINES. Chairman Manchin, thank you, and thanks for holding this hearing on my bipartisan Department of Energy Quantum Leadership Act, which will reauthorize and strengthen DOE's programs under the National Quantum Initiative.

In 2018, this Committee and Congress passed the National Quantum Initiative Act in order to focus research, development, and encourage commercialization of the next generation of high-powered computing. That bill has been very effective in spurring quantum research in the United States and in Montana. Since passage, Montana has seen a surge of economic development in jobs surrounding the quantum supply chain. The smartest people want to find the best places to also live and work, and Montana fits that bill. In fact, Montana now boasts over 50 companies and 1,200 employees focused solely on quantum and photonics. Montana State University is home to the MonArk Quantum Foundry, which focuses on quantum materials research. Through the CHIPS and Science Act, Montana hosts the Headwaters Technology Hub, focused on smart photonics, which is a key component in the future of quantum technology. Simply put, and you may not be aware of this, in Montana right now, we are helping lead the world in quantum and photonics, which is why I am proud to say we have strong support from Montana and other national leaders to reauthorize the DOE Quantum Initiative, including the Montana Photonics and Quantum Alliance, Montana State University, the Montana Chamber of Commerce, the Energy Sciences Coalition, the Quantum Industry Coalition, the Quantum Economic Development Consortium, and in fact, many more.

Chairman Manchin, I ask unanimous consent to enter into the record the many letters of support I have received for the DOE Quantum Leadership Act.

The CHAIRMAN. You want an answer on that?

Senator DAINES. I need a yes.

The CHAIRMAN. Yes.

Senator DAINES. Thank you.

[Laughter.]

[Letters of support for the DOE Quantum Leadership Act follow:]

"Advancing the Photonics Frontier"

MONTANA
PHOTONICS & QUANTUM

August 26, 2024

The Honorable Steve Daines
United States Senate
503 Hart Office Building
Washington, DC 20515

Re: Support for the Department of Energy Quantum Leadership Act of 2024

Dear Senator Daines,

The Montana Photonics & Quantum Alliance (MPQA) actively supports the advancement of photonics and quantum technology through our workforce and professional development activities, industry networking events, business development support, and business attraction efforts. Accordingly, the MPQA fully supports the Department of Energy Quantum Leadership Act of 2024 that you and Senator Durbin have proposed. This legislation is critical to continuing the work begun under the National Quantum Initiative Act of 2018 ensuring American supremacy in quantum technologies.

The MPQA was established in 2013 and comprises of over 50 member companies. Montana has a well-established photonics industry with a history of over 40 years and currently employs more than 1200 people in the Gallatin Valley alone. The MPQA is committed to driving technological innovation, advancing photonics, and promoting the commercialization of quantum technology. Many members of MPQA are actively involved in commercializing quantum technology in cryogenics, quantum materials, and quantum communications. Additionally, the MPQA has a leading role in the EDA Headwaters Technology Hub and is heading the largest component project to develop an Integrated Photonics Ecosystem (IPE) in Montana. The IPE project will receive over $14 million in funding to boost Montana's global leadership in photonics technology to establish the groundwork for future quantum technology advancements. As the nation's sole EDA-designated photonics-related technology hub, we are committed to fostering a supportive ecosystem that promotes economic growth and positions Montana at the forefront of developing innovative photonics, quantum technologies, and solutions for the benefit of our state and the nation.

The MPQA is a sub-awardee of the MSU flagship quantum project, the Applied Quantum Core, which received more than $27 million in funding last fiscal year from the Air Force Research Lab in Rome, New York. This program establishes a test bed facility on the MSU Innovation Campus to conduct fundamental and applied research on quantum technologies, support workforce development, and improve quantum literacy for the non-scientific community.

The Department of Energy National Quantum Leadership Act of 2024 and similar efforts will be essential to our economic and national security for decades to come. We wholeheartedly support this initiative and others like it to ensure our economic and national security for the future.

Sincerely,

Jason Yager
EXECUTIVE DIRECTOR, Montana Photonics & Quantum Alliance

406.223.6894
director@mpqa.org
JASON YAGER

MONTANA CHAMBER OF COMMERCE
WE MEAN BUSINESS

August 15, 2024

The Honorable Steve Daines
United State Senate
320 Hart Senate Office Building
Washington, DC, 20510

RE: Montana Chamber Supports S.4932, Department of Energy Quantum Leadership Act of 2024

Dear Senator Daines,

The Montana Chamber of Commerce represents businesses of all sizes from Montana's many industries. We are guided by the four pillars of our Envision2026 Strategic Plan: business climate, workforce readiness, infrastructure, and entrepreneurship. With the limitless applications of quantum technologies and the opportunities the industry presents, the Montana Chamber of Commerce wholeheartedly supports the *Department of Energy Quantum Leadership Act of 2024*.

From farmers using high-tech equipment to researchers in our universities finding innovative ways to use these technologies, advancements in quantum allows businesses in all fields to thrive. We must continue to support our quantum industry to ensure American businesses and leaders remain on top.

The *Department of Energy Quantum Leadership Act* is well-structured to support the whole system of quantum technologies, including addressing research needs, developing a workforce, and tackling supply chain issues. We anticipate that quantum innovation will continue to expand across Montana and this legislation, building off the *National Quantum Initiative Act of 2018,* will allow our state to take all these innovations in stride.

"With the widespread impacts of quantum technology across industries, this investment is essential to further quantum research, solidify American quantum companies as world leaders, and tackle complex workforce and commercialization issues within the quantum industry. The bill's focus on public-private partnerships and emphasis on small to medium quantum businesses will allow all states, including Montana, to benefit from this investment and will build on the good work we're doing here with the Headwaters Tech Hub."

We appreciate your support of this important piece of bipartisan legislation to continue the leadership of American quantum technologies for the benefit of all.

Sincerely,

Todd O'Hair

Todd O'Hair
President & CEO
Montana Chamber of Commerce

MONTANA STATE UNIVERSITY

August 12, 2024

The Honorable Steve Daines
United States Senate
503 Hart Office Building
Washington, DC 20515

Dear Senator Daines,

Montana State University has always supported efforts to advance technology through our education, research, and service missions. Thus, it is without reservation that we offer our full support to the *Department of Energy Quantum Leadership Act of 2024* that you and Senator Durbin have proposed. This legislation is critical to continuing the work begun under the *National Quantum Initiative Act of 2018* to ensure American supremacy in quantum technologies.

Montana State University is leading the way in both fundamental and applied research in the quantum field. Our flagship quantum project, the Applied Quantum Core, with the Air Force Research Lab in Rome, New York, was awarded more than $27 million for the. This program is creating a test bed facility on the MSU Innovation Campus to perform fundamental and applied research on quantum technologies, support workforce development, improve quantum literacy for the non-scientific community, and move forward projects in quantum communications at Spectrum Labs. Further, Montana State has partnered with the University of Arkansas to create a 2D material quantum foundry (MonArk) through a $22.6 million National Science Foundation grant. Research at MonArk is improving scientific understanding of what materials will shape the future of quantum.

The *Department of Energy Quantum Leadership Act of 2024* would expand on the work already happening at Montana State University and deploy necessary resources to support future projects. Additionally, it creates pathways for our graduates to turn their research into careers right here in Montana. Further, we see opportunities in this legislation to contribute to the quantum supply chain conversation especially if we receive the full funding for our National Science Foundation Quantum Supply Chain Engine proposal. The possibilities for collaboration under these programs are only limited by our collective imagination.

Losing the race to establish quantum supremacy is not an option. Legislation such as the *Department of Energy National Quantum Leadership Act of 2024* is critical to ensuring American dominance in this field and giving quantum research a much-needed boost. We strongly support this effort and so many like it to ensure our economic and national security for decades to come.

Sincerely,

DocuSigned by:
Alison Harmon

Alison Harmon
Vice President for Research and Economic Development

Office of Research & Economic Development
221 Montana Hall
P.O. Box 172460
Bozeman, MT 59717
montana.edu/research

Tel 406-994-2891

Mountains & Minds

ENERGY SCIENCES COALITION

Department of Energy Quantum Leadership Act of 2024 Support Letter

August 8, 2024

On behalf of over 100 member organizations that make up the Energy Sciences Coalition (ESC), we are writing to express strong support for the bipartisan *Department of Energy (DOE) Quantum Leadership Act of 2024*. As the bill moves forward in the legislative process, we urge Congress to reconcile differences between the DOE provisions in the Senate *DOE Quantum Leadership Act* and the House *National Quantum Initiative Reauthorization Act* (H.R. 6213) and pass legislation as soon as possible to ensure continued U.S. leadership in quantum science and technology.

In particular, ESC supports the *DOE Quantum Leadership Act* because the legislation maintains and further expands the DOE Office of Science's leadership role in advancing quantum science and technology for U.S. competitiveness, leverages the unique expertise and world-leading research facilities at DOE national laboratories and DOE-funded research universities, helps train the next-generation workforce, and expands public-private partnerships to accelerate innovation and future adoption. Similar to the DOE provisions in the *National Quantum Initiative Reauthorization Act*, ESC supports key provisions in the *DOE Quantum Leadership Act*, including:

- maintaining a foundational research program in quantum information science (QIS);
- expanding the foundational QIS research program to include first use cases and application development;
- renewing and increasing funding authorization for the 5 DOE National Quantum Information Science Research Centers;
- consolidating quantum networking and quantum user program provisions from the *CHIPS and Science Act* to ensure a comprehensive QIS program;
- expanding quantum computing, networking, and communications initiatives;
- creating a new quantum science and technology instrumentation and infrastructure program, and

- strengthening coordination between DOE STEM and workforce development activities at the DOE quantum centers and national laboratories with the new proposed National Science Foundation Education and Workforce Hub.

ESC also supports additional or modified provisions included in the Senate legislation:

- an early-state quantum high performance computing research and development program to fund testbeds and prototypes to help inform the 10-year Quantum High Performance Computing Strategic Plan;
- a dedicated quantum traineeship program to build the quantum workforce. This type of program has been successful in other science and technology areas and provides needed classroom training and research opportunities to undergraduate and graduate students working toward bachelor's, master's or Ph.D. degrees. Research projects would partner students with DOE national labs to help students develop hands-on research and training experiences and build quantum curricula at research universities;
- higher authorized funding levels for the new quantum instrumentation and quantum foundry program needed to design, build, and deploy unique instrumentation, equipment, national lab infrastructure and manufacturing capabilities for quantum materials, devices, and other relevant quantum technologies; and
- a quantum supply chain study to identify critical quantum science, engineering, and technology supply chain needs to develop and maintain a robust domestic manufacturing base.

Collectively, these provisions will help the U.S. maintain a quantum advantage and start to explore early applications of this nascent technology that could have broad impacts in national security, telecommunications, health, finance, and energy. Thank you for advancing this critically important legislation.

Sincerely,

Leland Cogliani
Co-chair
202-289-7475
leland@lewis-burke.com

Sarah Walter
Co-chair
202-434-8003
swalter@msu.edu

ESC Membership

American Association of Physicists in Medicine
American Association of Physics Teachers
American Astronomical Society
American Chemical Society
American Crystallographic Association
American Geophysical Union
American Geosciences Institute
American Institute of Physics
American Mathematical Society
American Nuclear Society
American Physical Society
American Society for Engineering Education
American Society of Agronomy
Acoustical Society of America (ASA)
American Society of Mechanical Engineers
American Society for Microbiology
American Society of Plant Biologists
American Vacuum Society
Arizona State University
Association of Public and Land-grant Universities
AVS – The Society for Science and Technology of Materials, Interfaces, and Processing
Battelle
Binghamton University
Biophysical Society
Boston University
Case Western Reserve University
City College of CUNY
Clemson University
Coalition for Academic Scientific Computation (CASC)
Consortium for Ocean Leadership
Columbia University
Computing Research Association
Council of Scientific Society Presidents
Cornell University
Cray Inc.
Crop Science Society of America
Duke University
The Ecological Society of America
Florida State University
Fusion Power Associates
Geological Society of America
George Mason University
Georgia Institute of Technology
Harvard University
Health Physics Society
IBM
IEEE-USA
Iowa State University
Jefferson Science Associates, LLC
Krell Institute
Lehigh University
Long Island University
Massachusetts Institute of Technology
Materials Research Society
Miami University of Ohio
Michigan State University
Michigan Technological University
New York University
Northeastern University
Northern Illinois University
Northwestern University
Oak Ridge Associated Universities (ORAU)
Optica (formerly OSA)
Pace University
Penn State University
Princeton University
Purdue University
Rensselaer Polytechnic Institute
Rochester Institute of Technology
Rutgers, The State University of New Jersey
Society for Industrial and Applied Mathematics
Soil Science Society of America
South Dakota School of Mines
Southeastern Universities Research Association
SPIE
Stanford University
Stony Brook University
Tech-X Corporation
The Ohio State University
University of California System
University of Chicago
University of Colorado Boulder
University of Delaware
University Fusion Association
University of Hawaii
University of Illinois System
University of Iowa
University of Maryland, College Park
University of Michigan
University of Missouri System
University of Nebraska
University of North Texas
University of Oklahoma
University of Pennsylvania
University of Rochester
University of Southern California
University of Tennessee
University of Texas at Austin
University of Virginia
University of Wisconsin-Madison
Universities Research Association
Washington State University
West Virginia University
Yale University

Quantum Industry Coalition

August 28, 2024

The Honorable Richard Durbin
711 Hart Senate Office Building
Washington DC 20510

The Honorable Steven Daines
320 Hart Senate Office Building
Washington DC 20510

Dear Senators Durbin and Daines:

The Quantum Industry Coalition (QIC) is a group of companies dedicated to maintaining the United States' leadership in the development and commercialization of quantum technologies. Our members range from start-ups to Fortune 100 companies focusing on a variety of aspects of quantum technology, including hardware, software, and application development. We write to thank you for introducing the Department of Energy (DOE) Quantum Leadership Act, and to endorse this important legislation.

Quantum technologies, including computing, networking, sensors, and cryptography, have the potential to bring transformative economic, scientific, and national security impacts. It is imperative that the United States lead in the global quantum race. The National Quantum Initiative (NQI) is key to enabling US leadership. Your legislation updating the NQI's DOE provisions to account for six years of US quantum progress is vitally important.

QIC particularly appreciates that the DOE Quantum Leadership Act broadens the scope of DOE's quantum programs beyond fundamental research. It is time for DOE to help move quantum technologies beyond the lab and into general use, and for the Department not just to do research *on* quantum technologies, but also to do research *with* quantum technologies. We look forward to working with you and the Committee to identify other opportunities to expand DOE's scope of quantum activity, including working with industry to develop quantum hardware, software, and near-term applications. QIC also applauds the bill's expansions of the Quantum Network Infrastructure Research and Development program and the Quantum User Expansion for Science and Technology Program.

Again, thank you for introducing the DOE Quantum Leadership Act. The Quantum Industry Coalition endorses this bill and urges its passage as part of the NQI reauthorization process in the 118th Congress.

Sincerely,

Paul Stimers
Executive Director
Quantum Industry Coalition

www.quantumindustrycoalition.com

CHICAGO
QUANTUM
EXCHANGE

August 28, 2024

The Honorable Richard Durbin
U.S. Senate
711 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Durbin:

The Chicago Quantum Exchange (CQE) connects top universities, national labs, and industry partners to advance the science and engineering of quantum information, train the future quantum workforce, and drive the quantum economy. Home to some of the world's top experts in the field, the Midwest-based CQE community is a central driver of US leadership in quantum technologies.

The *Department of Energy Quantum Leadership Act* will advance the research mission and workforce activities of the CQE. The bipartisan legislation maintains and further expands the DOE Office of Science's leadership role in advancing quantum science and technology for U.S. competitiveness, leverages the unique expertise and world-leading research facilities at DOE national laboratories and DOE-funded research universities, helps train the next-generation workforce, and expands public-private partnerships to accelerate innovation and future adoption.

Your leadership in advancing innovation in the state of Illinois and the Midwest region is much appreciated.

Yours sincerely,

David Awschalom
Director
Chicago Quantum Exchange

THE UNIVERSITY OF CHICAGO | OFFICE OF THE PRESIDENT

A. Paul Alivisatos
President
T 773.702.8800

August 30, 2024

The Honorable Richard Durbin
U.S. Senate
711 Hart Senate Office Building
Washington, D.C. 20510

Dear Senator Durbin,

As I know you are aware, the University of Chicago has assembled a world-class group of scientists and engineers who are leading the quantum revolution. In addition to our cutting-edge faculty in physics, engineering and chemistry, we offer one of the nation's first doctoral programs in quantum science and engineering. Buttressed by your ongoing effective advocacy for our national labs, the University also works in close partnerships with two Department of Energy (DOE) National Quantum Information Science (QIS) Research Centers at Argonne and Fermilab.

The DOE Quantum Leadership Act of 2024 will continue to advance and expand the research, education and training in quantum science occurring both on campus and at our national labs. The bill's focus on expanding R&D activities, building upon the foundational work of the QIS Research Centers, reducing barriers to commercialization, increasing interagency coordination and establishing new programs to support workforce demands will further serve to advance the Chicago region's national leadership as an innovation hub for promoting quantum science and technology.

I want to thank you for co-sponsoring this bipartisan bill. Your tireless commitment to promoting research and innovation continues to yield many tangible benefits to the University of Chicago, the national labs, the State of Illinois, and the nation.

Thank you and best regards,

A. Paul Alivisatos
President, University of Chicago

The University of Chicago
Edward H. Levi Hall, 5801 South Ellis Avenue, Suite 501, Chicago, Illinois 60637 uchicago.edu

September 6, 2024

As part of the national quantum community comprising industry, academia and nonprofit stakeholders, we are writing to express our support for advancing U.S. quantum information science and technology (QIST) through the Department of Energy (DOE) Quantum Leadership Act of 2024, which authorizes $2.5 billion in QIST R&D project funding over the next five years. This act builds upon the investments made in the National Quantum Initiative Act (NQIA) of 2018 to ensure continued U.S. leadership in QIST.

In 2018, the NQIA established national quantum research centers through the DOE and National Science Foundation (NSF), launched a quantum education network, increased research at the National Institute of Standards and Technology, and coordinated quantum activities across federal agencies to strengthen American leadership in this important emerging technology area. To date, U.S. investments in QIST have already created new industries, jobs, and markets; have bolstered our national security; and improved our global leadership.

QIST has the potential to revolutionize many sectors, including computing, finance, communications, sensing, cryptography, pharmaceuticals, and materials. Meanwhile, competition between the U.S. and other countries continues to grow. This bill is a necessary piece in the US strategy to be at forefront of this critical technology.

We were very encouraged of the many aspects of the DOE Quantum Leadership Act of 2024 that fulfills NQIA's mandate by:

- reauthorizing and expanding R&D activities across DOE through 2029
- building on the foundational work of DOE's five National Research Centers
- directing DOE to study and address quantum supply chain challenges and reducing barriers to commercialization
- increasing interagency and industry coordination
- establishing new programs to support the workforce demands of the growing quantum R&D and commercial industry.

The DOE Quantum Leadership Act of 2024 helps place U.S. research and industry out in front of the competition. We appreciate your leadership on this issue in Congress. We stand ready to work with your offices to provide any information or assistance you may need. Thank you for your consideration of this important matter.

(Signature Page Follows)

SIGNED BY:

ColdQuanta, Inc., DBA Infleqtion
Duke University
EPB Chattanooga
IBM
Montana Photonics & Quantum Alliance
NY CREATES
Quantinuum
Quantum Economic Development Consortium (QED-c)
Rigetti
SPIE
TOPTICA
University of Colorado Boulder
University of Rochester
Vexlum
Yale University

Senator DAINES. It's who you know in this business, isn't it, Joe?

Thank you, Joe, I appreciate it—Senator Manchin—Chairman Manchin.

Anyway, thank you.

The CHAIRMAN. Still Joe.

Senator DAINES. And it's still Joe and I am still Steve, too.

The CHAIRMAN. I know.

Senator DAINES. We must continue to focus our energy on developing the best technology and leading the world in quantum research, and this starts with passing my bipartisan bill. So I want to thank Chairman Manchin for entering those letters into the record and his partnership and support of this as well, and I yield back my time to the Chairman.

The CHAIRMAN. Thank you, Senator.

First of all, before I adjourn, and thank you all for a great job and it was really wonderful, you know, just so much to do here. I want to make a clarification on—I know I put you all on the spot. I wasn't asking you to basically disparage on our sister NSF. What I was asking is, for the record, we wanted to avoid duplication. When we did the CHIPS and Science Act at the highest of DOE and the labs and intended to do the same with AI and other emerging technology, we were trying to avoid that duplication, and DOE, the labs, we were working on their behalf. I want to make sure that we have that balanced approach and we are not robbing Peter to pay Paul and trying to reproduce the same thing again, dual application. We just, I don't think any Democrats or Republicans want that to happen.

So with your assurances that's not happening, and that you have the resources and you are working with the NSF to try and have a balanced approach with what they do and can do best for you to support what you are doing and vice versa is what we are trying to make sure happens. We just don't want you to think you have to be muffled on this. If you want to speak out, this is the place to do it.

But with that being said, I believe that this hearing demonstrated consensus that we need to continue investing in and leading these emerging technologies in a way that leverages DOE's assets to avoid reinventing the wheel, as we have said, or duplicating between agencies. We worked to avoid duplication in the CHIPS and Science Act, and at the behest of DOE and labs, intend to do the same here in AI. We also agree on the need to secure the research from foreign espionage, and I believe that Senator Barrasso and I prepared a solid bipartisan compromise with the Intelligence Committee to do just that in the NDAA, which will complement our efforts on this Committee. It's a scalpel approach that protects our critical research while continuing our labs to leverage the best scientific minds in the world. We are concerned about not only the espionage that goes on, but also people that are working within, and we are training them to use it against us, but we understand the delicate thing that you have to work with in the freedom-loving country that we are and the democracy that we rule ourselves under.

So members will have until close of business tomorrow to submit additional questions for the record.

And the Committee stands adjourned.

[Whereupon, at 11:57 a.m., the hearing was adjourned.]

APPENDIX MATERIAL SUBMITTED

U.S. Senate Committee on Energy and Natural Resources

September 12, 2024 Hearing: *The Department of Energy's Role in Advanced Computing Research, Application, and Security*

Questions for the Record Submitted to Ms. Helena Fu

QUESTIONS FROM SENATOR MANCHIN

Q1a. How will the bipartisan AI and quantum computing bills that I discussed in my opening statement help us stay competitive with China?

A1a. Thank you for your leadership on this key topic. DOE's national labs are at the forefront of AI and quantum research, which has significant implications in our intense strategic competition with the PRC.

The DOE AI bill would support the Department and our 17 national laboratories as we continue to harness safe, secure, and trustworthy AI for good. We aim to leverage DOE's capabilities, infrastructure, and partnerships to build the world's most powerful integrated scientific AI systems for science, energy, and national security. In particular, DOE's Frontiers in Artificial Intelligence for Science, Security and Technology (FASST) is an ambitious AI initiative that would provide frontier-scale science-based AI systems to solve critical challenges in science, energy, and national security. This kind of public capability is critical to extend the United States' competitive edge in scientific innovation, to develop effective rights-respecting AI governance and safety measures, and train an AI-ready workforce. DOE is positioned to address the AI challenge from beginning to end, starting with data and ending with the development and implementation of AI applications for the critical challenges we face as a nation. We look forward to working with the sponsors of the legislation as it moves through the legislative process.

The DOE Quantum Leadership Act would allow the Department to further its innovative research and development efforts in quantum information science and explore applications in computing, sensing, imaging, simulation, and networking. This would leverage the successes of the National Quantum Initiative Act of 2018, which called upon the DOE to establish the National Quantum Information Science Research Centers. These Centers have established quantum foundries for advanced device fabrication, built

underground facilities for characterizing quantum devices, developed highly successful open-source control-software, advanced innovative superconducting devices to improving the precision of critical atomic clocks, and more. The Centers have also contributed to building the U.S. quantum workforce with 300 new hires and over 600 students and postdocs engaging with the Centers. The DOE Quantum Leadership Act would further advance quantum information science and position us as a leader in developing this new technology.

The Department, and our National Labs in particular, are at the frontier of both AI and quantum information science, and the whole of the DOE stands ready to ensure that we rise to the challenges posed by today's competitive landscape.

Q1b. What is at stake if China and our other adversaries take the lead in artificial intelligence and other emerging technologies?

A1b. If the PRC or our other strategic competitors take the lead in these technologies – and we know they intend to – they will dominate the global emerging technologies policy environment, writing the rules of the road and shaping global standards. In the long run, they could dominate global data flows and create technological dependencies.

DOE is focused on AI's role in responsible innovation and helping to maintain U.S. scientific, energy, and national security leadership. And three things are clear: Whoever leads the world in AI for science will lead the world in scientific discovery and will have a lead in translating those scientific discoveries into competitive economic growth and market innovation. Whoever leads the world in AI for energy will lead the world in developing and deploying next generation energy technologies. And whoever leads the world in understanding and mitigating the risks of AI and the use of AI to improve

national and global security will determine the landscape in which we and our allies and partners work for the future.

Other emerging technologies surface analogous scenarios. For example, the PRC has indicated biotechnology and biomanufacturing are a top national priority, starting with the 13th Five-Year Plan and continuing into the 14th Five-Year Plan, including one devoted specifically to the bioeconomy. The U.S. bioeconomy is valued at close to $1 trillion. DOE contributes to U.S. leadership in biotechnology and biomanufacturing by generating and working with substantial amounts of high-quality biological data, developing and attracting a world-class workforce, informing standards, and bolstering the U.S. innovation ecosystem so that impactful goods and services are produced. Similarly, technologies like quantum computing hold the potential to drive innovations across the U.S. economy but adversarial use of quantum computers also poses significant risks to the economic and national security of the United States. DOE's work in quantum information science is focused on maintaining and advancing U.S. leadership in this critical technology.

Much is at stake in the competition for leadership in critical and emerging technologies, and DOE is working every day to maintain and extend the U.S. technological leadership.

U.S. Senate Committee on Energy and Natural Resources

September 12, 2024 Hearing: *The Department of Energy's Role in Advanced Computing Research, Application, and Security*

Questions for the Record Submitted to Ms. Helena Fu

QUESTIONS FROM SENATOR JAMES RISCH

Q1. We have seen transformational evolution of artificial intelligence the last couple of years. What are some groundbreaking practical examples of AI that you think could accelerate applied energy for the nation?

A1. The Department of Energy is optimistic about using AI to accelerate applied energy throughout the energy ecosystem. We believe that AI can speed the planning and permitting process, unlock new efficiency gains in both fossil energy and renewables, accelerate the recovery of critical minerals, and contribute to a reliable and resilient grid. DOE published a report on AI for Energy in April 2024 that details many near-term potential AI uses in applied energy. This report contains examples of how AI can optimize four key areas of grid management: planning, permitting, operations and reliability, and resilience, and how AI can enable the characterization of subsurface to support geological storage for hydrogen and CO_2, characterization of critical minerals, and locating orphan wells. In addition, the report includes examples of how AI can accelerate progress across the energy economy, including the transportation, agricultural, industrial, and building sectors, and in cross-sectoral applications including characterizing the subsurface. A handful of these examples are described below.

AI for permitting has practical potential uses that are in development now. DOE announced the VoltAIc initiative to use AI to help expedite and improve siting and permitting at the Federal, state, and local level. As part of that initiative, DOE is building AI-powered tools to improve siting and permitting of clean energy infrastructure. For example, we are developing PolicyAI, a policy-specific large language model test bed that will be used to develop software to augment NEPA and related reviews. PolicyAI can help utilize AI to support drafting documents, permits, and other text for Federal reviewers, which can support more timely decisions for critical infrastructure projects. Additionally, advances in large language models (LLMs) can support more efficient

handling of public comments for critical infrastructure projects, allowing agency staff to focus on comment analysis and developing solutions to community concerns.

Through the National Reactor Innovation Center, Idaho National Lab (INL) is developing semi-autonomous design AI tools for advanced nuclear energy technologies. These tools allow for simple textual input to be automatically converted to plant computer aided design (CAD) files and then, with minimal human effort, semi-autonomously converted for analysis using high performance analysis codes. Through DOE's Frontiers in Artificial Intelligence for Science, Security and Technology (FASST) initiative, INL seeks to deliver an ecosystem of tools for semi-autonomous power plant design and licensing document generation. Early studies estimate this could reduce the probability of schedule delays by roughly 20% for advanced nuclear power plants, which is a significant AI-driven opportunity across a projected 200GW of new nuclear power. In addition, INL, in partnership with other national laboratories, has developed the Multiphysics Object Oriented Simulation Environment (MOOSE) ecosystem of multi-physics tools and integrated these tools with advanced AI technologies. MOOSE, digital engineering, AI, and the laboratory's one-of-a-kind nuclear facilities can be combined under FASST to bring semi-automation (with appropriate human decision-making 'in the loop') to advanced nuclear experimentation, unlocking new fuels, materials, and other nuclear technologies faster to maintain U.S. leadership in nuclear energy.

Scientists at the National Renewable Energy Laboratory (NREL) in Golden, Colorado, are using generative AI to accelerate community-centric clean energy transitions to a more sustainable and resilient future. We can develop community-specific representations of built infrastructure, resulting in more accurate predictive models, and we can assess the impacts of extreme weather events on communities and the built

environment under various climate scenarios to inform risk mitigation strategies for a more resilient energy infrastructure.

Office of Electricity-funded researchers are investigating Artificial Intelligence and Machine Learning (AI/ML) use for enhanced online and real-time microgrid installation visibility and monitoring. This effort will synchronize, harmonize, and combine microgrid system data at different timescales and from multiple sensors as well as develop and train ML models to facilitate microgrid health and condition monitoring, detect anomalies, and predict potential constraint violations. These solutions will enhance situational awareness and accelerate intelligent reporting for proactive risk mitigation and faster response times, which will further improve the reliability of the electric power system.

Finally, AI can help us identify potential alternatives for critical minerals and find more critical minerals where they exist in unconventional sources, such as mine waste and coal ash. The success at Pacific Northwest National Laboratory (PNNL) in identifying novel battery materials is an excellent example of how we are using AI to address critical mineral challenges. In addition, DOE's National Energy Technology Laboratory (NETL) has published the world's first peer-reviewed, AI multi-modeling of unconventional rare-earth elements and critical minerals resource assessment model. It uses AI/ML applied to data from sedimentary core samples, the geologic history, and so on to create a predictive model. This effort resulted in the discovery of the U.S.'s largest unconventional accumulation of rare earth elements in Wyoming's Powder River Basin.

DOE's work using safe, secure, and trustworthy AI to accelerate applied energy is starting to have an impact, and we hope to increase our investment in AI R&D to build a stronger, more efficient, and resilient energy ecosystem.

U.S. Senate Committee on Energy and Natural Resources

September 12, 2024 Hearing: *The Department of Energy's Role in Advanced Computing Research, Application, and Security*

Questions for the Record Submitted to Ms. Helena Fu

Q2a. In your testimony you talk about enhancing DOE's Science, Energy, and Security Mission. When you reference Energy, does that include applied energy?

A2a. Yes, it includes applied energy.

Q2b. And, if so, what are some practical examples of applied AI applications that can further this mission?

A2b. DOE published a report on AI for Energy that details near-term AI uses in applied energy. See response to A1 for select examples.

In addition, DOE National Laboratories are already developing foundation models and partnerships for applications in applied energy, with examples including medium-range weather forecasting for wind and solar energy; enabling technologies for nuclear plant modernization and applications of digital twins; using automated labs to develop useful new materials for clean energy technologies; developing improved sensor design for hydrogen production; enabling combustion efficiency for gas turbines; and identifying unconventional rare-earth and critical minerals.

U.S. Senate Committee on Energy and Natural Resources
September 12, 2024 Hearing: *The Department of Energy's Role in Advanced Computing Research, Application, and Security*
Questions for the Record Submitted to Dr. Shaun Gleason

Question from Chairman Joe Manchin III

Question 1 (part 1): How will the bipartisan AI and quantum computing bills that I discussed in my opening statement help us stay competitive with China?

Government investment in the research and development of emerging technologies such as AI and quantum is essential to ensure the U.S. maintains its leadership position relative to China and other nations. As a historical example of government investments propelling the US into a world leadership role, consider DOE's investments into high-performance computing over the last two decades. This investment has propelled the U.S. in the lead with the fastest open science computers in the world—the most recent example being Frontier, the nation's first exascale supercomputer, deployed at Oak Ridge National Laboratory. Because it and other leadership class systems at the national laboratories were designed and built in partnership with the private sector, this government investment catalyzed U.S. companies (e.g., NVIDIA, HPE, AMD, IBM, and others) to develop the world's most sophisticated HPC hardware and software.

The private investment by U.S. industry in both AI and quantum is strong and vibrant and is an essential innovation and application driver for both fields. Complementing this private investment is government investment in AI and quantum research and development, tools and testbeds, and workforce development. At the DOE national laboratories, this government investment supports the construction and operation of world-class research facilities, tools, and testbeds for the nation's scientists (e.g. leadership computing for AI and state-of-the-art quantum computing laboratories), enables revolutionary AI and quantum discoveries, employs such discoveries to overcome critical national challenges in science, energy, and security, and, through the process, educates the future scientific and technical workforce in these fields. Additionally, the national laboratories' science and technology discoveries are made available to industry through technology transfer programs so they can be commercialized, help U.S. industry compete in global markets, and have a positive impact on the U.S. economy. Government investment in university R&D that educates the next generation of AI and quantum scientists and engineers will provide the essential foundation of future U.S. leadership. When all three pillars of the U.S. innovation ecosystem—national laboratories, industry, and academia—have the resources they need and are given the tools and direction to collaborate, the U.S. will excel and lead the world in AI and quantum.

Continued federal investment is even more important today to maintain U.S. leadership in these fields. Public investment by China appears to be greater than the U.S. in quantum, and the government backed investment organization, China International Capital Corporation, announced this month (September 2024) plans to invest $1.4 trillion in AI development over the next 6 years. The U.S. industry is recognized to be stronger than China's in both AI and quantum, but China is still acknowledged to be a world leader, along with the U.S., in both areas. Regarding quantum investments, the Information Technology and Innovation Foundation recently argued that the U.S. will "will need more government investment to maintain its lead over China." Their published research on the AI development race between the U.S. and China states that for the U.S. to maintain leadership, "It is critical for Congress and the White House to

U.S. Senate Committee on Energy and Natural Resources
September 12, 2024 Hearing: *The Department of Energy's Role in Advanced Computing Research, Application, and Security*
Questions for the Record Submitted to Dr. Shaun Gleason

craft and fund a comprehensive national AI strategy that addresses the dual goals of increasing AI development and adoption." U.S. national laboratories, industry, and academia each play critical and complementary roles in advancing AI and quantum science and innovation, and healthy government investment will keep the U.S. not only competitive in these emerging technologies but can propel the U.S. well ahead of China.

Question 1 (part 2): What is at stake if China and our other adversaries take the lead in artificial intelligence and other emerging technologies?

AI and quantum are two emerging technologies that are uniquely poised to revolutionize many aspects of our lives and have the potential for unprecedented impact on our economic, energy, and national security. How we share and secure information, transport people/goods/services, generate and dispatch distributed energy sources, manufacture goods, discover new materials, and defend our nation, just to name a few, will all be impacted in significant ways with the maturation and application of AI and quantum technologies. The impact of AI is already being felt in business, art, education, and science, for example, but we are seeing only the tip of the iceberg. The country that advances these enabling technologies most rapidly to realize real-world impact will be positioned to outpace the world in many other areas of science and technology. As an example, AI is on a trajectory to become powerful enough to enable new and rapid scientific discoveries in many fields including medicine, materials science, energy, and national security. Also, there are other cascading effects of AI leadership on critical technology areas such as microelectronics and alternative computing architectures (e.g. quantum co-processors for AI). As such, AI can be viewed as the "rocket fuel" for the innovation engine, and whoever refines that fuel first will have the ability to accelerate discovery on many science and technology fronts and quickly leave other countries behind.

As a scenario where we must maintain leadership in all aspects of AI, consider the security of deployed AI systems. As we deploy AI systems in every domain, including our critical infrastructure (electric grid, water treatment, transportation systems, financial systems, national defense systems, etc.), we must be able to secure those systems against clear PRC objectives and advanced capabilities to infiltrate and control those AI systems for their own advantage. To prevent this cyber threat scenario, we need a focused and comprehensive investment into the field of AI security. Another compelling reason for government investment into AI science and technology is to address the ethical implications of AI leadership, including the reduction of AI system bias and the development of robust guardrails in AI systems to prevent misuse and/or abuse.

There is still uncertainty in the timing and level of impact that AI and quantum will have, but we cannot afford to take a "wait-and-see" approach—the stakes are too high. The U.S. cannot afford to fall behind China and other nations in these critically important fields because our economic and national security will be at extreme risk.

U.S. Senate Committee on Energy and Natural Resources
September 12, 2024 Hearing: *The Department of Energy's Role in Advanced Computing Research, Application, and Security*
Questions for the Record Submitted to Dr. Divyansh Kaushik

Questions from Chairman Joe Manchin III

Question 1: How will the bipartisan AI and quantum computing bills that I discussed in my opening statement help us stay competitive with China? What is at stake if China and our other adversaries take the lead in artificial intelligence and other emerging technologies?

Q1: The Department of Energy's role in advancing artificial intelligence and quantum computing is crucial for maintaining America's technological leadership. DOE's network of national laboratories, with their world-class facilities and expertise, are uniquely positioned to drive innovation in these fields.

As you highlighted in your opening statement, DOE has a long legacy in computational science dating back to the Manhattan Project. Today, this legacy continues with DOE operating the two fastest supercomputers in the world. This computational power, combined with the multidisciplinary expertise at our national labs, provides an unparalleled foundation for pushing the boundaries of AI and quantum computing research.

In the field of AI, DOE's role is particularly important for addressing complex societal challenges where there isn't yet an established commercial market. Areas like advanced manufacturing, nuclear security, and genomics require the kind of long-term, fundamental research that DOE excels at. The national labs can develop foundational AI models, create testbeds for new AI platforms, and establish rigorous safety and security protocols that are essential for responsible AI development.

Quantum computing represents another frontier where DOE's capabilities are critical. The potential of quantum computers to solve complex problems far beyond the reach of classical computers could revolutionize fields from cryptography to materials science. DOE's expertise in both the theoretical and practical aspects of quantum science positions it to make significant contributions to this rapidly evolving field.

Moreover, DOE's role extends beyond just research and development. As you mentioned, cybersecurity is a crucial concern in this new era of emerging technologies. DOE's work in developing secure AI systems and quantum-resistant cryptography is vital for protecting our critical infrastructure and national security interests.

The stakes in this technological race are incredibly high. As your opening statement pointed out, whoever leads in the development of these technologies will likely secure an unequivocal lead in scientific and technological innovation broadly. This leadership has profound implications for our economic prosperity and national security.

If China or other adversaries were to take the lead in AI and quantum computing, it could impact our ability to defend against cyber threats, compromise our critical infrastructure, and potentially shift the balance of global economic and military power. Moreover, it could allow other nations

U.S. Senate Committee on Energy and Natural Resources
September 12, 2024 Hearing: *The Department of Energy's Role in Advanced Computing Research, Application, and Security*
Questions for the Record Submitted to Dr. Divyansh Kaushik

to set the standards and norms for how these powerful technologies are used, potentially in ways that do not align with our values of privacy, individual liberty, and human rights.

By leveraging the expertise and infrastructure of our national laboratories, we can accelerate our efforts in a cost-effective manner, building upon the resources and capabilities we've already developed. This approach not only advances our technological capabilities but also helps safeguard taxpayer dollars by maximizing the return on our existing investments.

In conclusion, DOE's role in advancing AI and quantum computing is not just beneficial – it's imperative for maintaining our global leadership, ensuring our national security, and driving economic prosperity in the 21st century. The department's unique capabilities and expertise make it an essential player in our nation's efforts to stay competitive in these critical technological domains.

Questions from Senator Josh Hawley

Question 1: What are the risks associated with allowing Chinese nationals to study artificial intelligence in the United States?

Q1: While there are potential risks associated with Chinese nationals studying artificial intelligence in the United States, it's crucial to approach this issue with nuance. As mentioned in my testimony, the vast majority of Chinese students come to the U.S. legitimately and contribute positively to our research and innovation ecosystem. In a letter to the Select Committee on the CCP (attached), former national security leaders from every previous administration going back to President Ford emphasized that U.S. leadership in technology rests largely on our ability to leverage domestic and international talent. While we must be vigilant about potential technology transfer or intellectual property theft that could benefit China's military-civil fusion strategy, it's important to remember that these risks apply to a very small minority of students. The focus should be on implementing targeted security measures rather than broad restrictions that could harm our competitive advantage in attracting global talent.

Question 2: Sen. Waner, who chairs the Senate Select Committee on Intelligence, has introduced the "Intelligence Authorization Act for FY 2025," which includes a provision prohibiting "covered foreign nationals" from working at our national labs. S. 4443, §436. This includes nationals of China, Russia, Iran, and North Korea. In your view, should the United States ban Chinese nationals from studying artificial intelligence at our research institutions? Why or why not?

Q2: The United States should absolutely not implement a blanket ban on Chinese nationals studying artificial intelligence at our research institutions. As my testimony highlights, such a move would be counterproductive to our national interests. Instead, we should focus on enhancing our ability to attract and retain global STEM talent, which is a key competitive advantage over the Chinese Communist Party. The national security leaders' letter I referenced

earlier rightly points out that nearly two in three graduate students in U.S. AI and semiconductor-related programs were born abroad. Implementing targeted security measures, such as those initiated under NSPM-33, can protect sensitive research while maintaining our open and collaborative research environment. The goal should be to strike a balance between security and openness, ensuring that the U.S. remains the most attractive destination for the world's brightest minds in AI and other critical fields. TSMC founder Morris Chang fled China during its civil war, moving to the United States to pursue studies at Harvard, then MIT. He later spent 25 years at Texas Instruments, rising to lead the company's global semiconductor division. In the latter years of the Cold War, a new era of international talent recruitment emerged as Soviet mathematicians and scholars sought opportunities beyond the Iron Curtain, similar to how many Chinese scientists seek today in democratic nations. American universities found themselves in an advantageous position, able to select from the cream of Soviet scientific talent, engaging in competitive bids for the most distinguished figures. A 1990 New York Times article captured this sentiment, quoting an American mathematician who noted that these Soviet academics were "replenishing the mathematical juices of the United States." Another Soviet émigré echoed this sentiment, reporting almost daily inquiries from fellow scholars eager to relocate to the United States. Proposals even surfaced to subsidize employers of these scientists, aiming to assimilate them as quickly as possible.

Strategic recruitment of international science and technology talent proved a major boon to American science. Between 1901 and 1933, Americans won only three of thirty Nobel Prizes in physics. From 1934 to 2020, Americans won a piece of two-thirds of all such awards, in large part thanks to either first or second-generation immigrants.

Given this history, it should be no surprise that China views the competition for top talent within and outside the Chinese diaspora as a major economic and national security threat. In key areas like AI, the CCP is offering Western-trained returnees enormous cash bonuses in the hundreds of thousands of dollars. Unfortunately, early evidence suggests such generous subsidies might be working. China's global share of top AI researchers and the share of those returning to China are growing. We must double down on our advantage and recruit the best and brightest---with appropriate security measures in place.

Question 3: Should the United States allow Chinese nationals to be employed by our National Laboratories? Why or why not?

Q3: The United States should continue to allow carefully vetted Chinese nationals to be employed by our National Laboratories for **unclassified** research, with extensive security measures in place. As my testimony emphasizes, the DOE's National Laboratories have long been a beacon for scientists and researchers worldwide, embodying the pinnacle of scientific pursuit and technological innovation. This global appeal is not just a point of pride; it's a cornerstone of our technological leadership. The national security leaders' letter corroborates this, noting that efforts to onshore critical supply chains may not succeed unless we also onshore the talent necessary to compete. By implementing robust security protocols and focusing on

retaining top talent, we can maximize the benefits of international collaboration while mitigating potential risks.

Question 4: Should the United States ban Chinese nationals from accessing DOE national laboratories or our cutting-edge AI technologies?

Q4: Rather than implementing a blanket ban on Chinese nationals accessing DOE national laboratories or cutting-edge AI technologies, the United States should adopt a more strategic and nuanced approach. As I shared in my testimony, we should focus on precision tools for identifying specific threats rather than broad, nationality-based restrictions. This aligns with the national security leaders' recommendation to pair talent attraction policies with measures that protect government-supported research and development. We should implement tiered access levels based on security clearances and research sensitivity, enhance vetting procedures, and strengthen counterintelligence efforts. Crucially, as both your testimony and the letter emphasize, we must focus on retaining top AI talent in the U.S. through immigration reforms. The letter rightly points out that bottlenecks in the U.S. immigration system endanger our national advantage by driving international science and engineering talent elsewhere. By addressing these bottlenecks and investing in both international and domestic STEM talent, we can maintain our position as a global leader in science and technology while safeguarding national security interests.

Question 5: What steps can the United States take to protect our artificial intelligence intellectual property from the People's Republic of China?

Q5: To protect our artificial intelligence intellectual property from the People's Republic of China, the United States can take several strategic steps while maintaining our competitive edge in attracting global talent. As emphasized in my testimony, it's crucial to strike a balance between security measures and preserving the openness that makes our research ecosystem so robust and attractive to international talent.

First, we should fully implement and continuously update research security measures like those initiated under NSPM-33. This approach, as mentioned in my testimony, allows us to protect sensitive research while maintaining an open and collaborative environment for unclassified, fundamental research. It's about using a scalpel rather than a sledgehammer in our security approach.

Second, we need to enhance our vetting procedures for individuals working on sensitive AI projects, particularly in our National Laboratories and critical research institutions. This doesn't mean implementing blanket bans based on nationality, which would be counterproductive. Instead, as I stressed in my testimony, we should develop more precise tools for identifying specific threats.

U.S. Senate Committee on Energy and Natural Resources
September 12, 2024 Hearing: *The Department of Energy's Role in Advanced Computing Research, Application, and Security*
Questions for the Record Submitted to Dr. Divyansh Kaushik

Third, we must strengthen our counterintelligence efforts to identify and mitigate specific risks of intellectual property theft. This includes better coordination between academic institutions, industry, and government agencies to share information about potential threats.

Fourth, and critically important, we need to address the bottlenecks in our immigration system that currently drive away international STEM talent. As the national security leaders' letter points out, our ability to attract and retain global talent is a key competitive advantage. By streamlining pathways for top AI researchers and engineers to stay in the U.S. after their studies, we can prevent the transfer of knowledge and expertise back to China.

Fifth, we should invest heavily in domestic STEM education and workforce development to reduce long-term reliance on foreign expertise. However, as I mentioned in my testimony, this should complement, not replace, our efforts to attract international talent.

Sixth, we need to foster stronger public-private partnerships in AI research and development. By combining the long-term vision and resources of government agencies like the DOE with the agility and market-driven focus of American industry, we can create a more robust ecosystem for AI innovation that's more resilient to foreign interference.

Lastly, we should work with our allies to establish common standards and protocols for AI research security. This international cooperation can help create a united front against intellectual property theft while maintaining the global flow of ideas that drives innovation.

In implementing these measures, it's crucial to remember that our open research system is a key strength, not a weakness. As I emphasized in my testimony, the vast majority of international researchers, including those from China, contribute positively to our innovation ecosystem. Our goal should be to address specific security concerns without undermining the collaborative, international nature of scientific progress that has been key to America's technological leadership.

Question 6: Do you think China is ahead of the United States when it comes to supercomputing?

Q6: The answer is a bit nuanced. They are ahead of us in the basic research that is being conducted today. They are producing 30.6% of the top papers in high performance computing today compared to the U.S.'s share of 23.7% in high performance computing. The thing with basic research investments is that they don't usually have immediate applications but may have those applications in a few decades from now. Like how when U.S. researchers discovered laser, there was no application for it. But today, it powers our weapons systems. However, when it comes to today's applied research, the U.S. is ahead but PRC is catching up really fast. The U.S. plans to limit access to high tech chips and chipmaking equipment has scuttled China's applied research ecosystem for now. But they have been investing in their domestic capabilities to catch up to the U.S.

U.S. Senate Committee on Energy and Natural Resources
September 12, 2024 Hearing: *The Department of Energy's Role in Advanced Computing Research, Application, and Security*
Questions for the Record Submitted to Dr. Divyansh Kaushik

Question 7: What steps can the United States take to ensure we remain ahead of China in key technologies such as supercomputers and artificial intelligence?

Q7: To ensure the United States remains ahead of China in key technologies such as supercomputers and artificial intelligence, we must adopt a multifaceted approach that leverages our strengths while addressing our vulnerabilities. As I emphasized in my testimony, our ability to attract and retain global talent is a critical advantage that we must protect and enhance. First and foremost, we need to double down on our investment in research and development. As I mentioned in my testimony, the Department of Energy's network of 17 National Laboratories and 35 user facilities are our technological vanguard. We should significantly increase funding for these institutions, particularly in areas like AI, quantum computing, and advanced energy systems. This investment should extend to both basic research and applied technologies to ensure a robust pipeline of innovation.

Second, we must address the talent bottleneck that threatens our technological leadership. As the national security leaders' letter points out, nearly two in three graduate students in U.S. AI and semiconductor-related programs were born abroad. We need to streamline our immigration system to make it easier for these highly skilled individuals to stay and work in the U.S. after graduation. This could include measures like exempting those with advanced STEM degrees from green card caps, as suggested in the letter and endorsed by former President Trump recently.

Third, we should focus on fostering a more dynamic ecosystem for innovation. This means strengthening partnerships between our National Laboratories, universities, and private sector companies. By facilitating the flow of ideas and talent between these sectors, we can accelerate the development and commercialization of cutting-edge technologies.

Fourth, we need to enhance our efforts to protect intellectual property and sensitive research. As I stressed in my testimony, this doesn't mean closing our doors to international collaboration. Instead, we should implement more precise security measures that target specific risks without stifling innovation or driving away international talent.

Fifth, we must invest heavily in our domestic STEM education pipeline. While attracting international talent is crucial, we also need to cultivate our homegrown expertise. This includes initiatives to increase STEM education at all levels, from K-12 through post-graduate studies. Sixth, we should leverage our alliances and partnerships globally. By collaborating with like-minded nations on research and development, we can pool resources, share knowledge, and create a more robust bulwark against technological competition from China.

Seventh, we need to ensure sustained, predictable funding for long-term research projects. Breakthroughs in areas like quantum computing and advanced AI often require years of steady investment. We should create funding mechanisms that provide stability and allow for the kind of long-term planning necessary for groundbreaking research.

U.S. Senate Committee on Energy and Natural Resources
September 12, 2024 Hearing: *The Department of Energy's Role in Advanced Computing Research, Application, and Security*
Questions for the Record Submitted to Dr. Divyansh Kaushik

In conclusion, our strategy should focus on amplifying our strengths – our open society, our culture of innovation, our world-class institutions, and our ability to attract global talent – while addressing our vulnerabilities through targeted security measures and increased investment. By doing so, we can ensure that the United States remains at the forefront of technological innovation, maintaining our edge over China in critical areas like supercomputing and artificial intelligence.

May 15, 2023

The Honorable Mike Gallagher
Chairman, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party
U.S. House of Representatives
Washington, DC 20515

The Honorable Raja Krishnamoorthi
Ranking Member, Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party
U.S. House of Representatives
Washington, DC 20515

Cc: Members of the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party

Dear Chairman Gallagher, Ranking Member Krishnamoorthi, and Members of the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party:

U.S. leadership in technology rests in large part on our ability to leverage domestic and international talent. We are writing because you are in a position to influence whether Congress protects or forfeits this national asset in the face of unprecedented competition from China.

As national security leaders who have served in each of the past several administrations, we are united in calling on Congress to address the emerging gap in advanced STEM talent with China. From computing to aerospace, critical sectors of our defense-industrial base rely on attracting global STEM talent. For example, nearly two in three graduate students in the United States specializing in artificial intelligence and semiconductor-related programs were born abroad.[1]

As this committee explores a wide range of issues, it has a critical opportunity to highlight the self-inflicted drag that immigration bottlenecks impose on U.S. competitiveness. Previous legislative efforts have considered exempting those with advanced STEM degrees from green card caps to better compete with China. That policy adjustment would respond appropriately to this national security concern, especially if paired with policies that protect government-supported research and development, such as the full implementation of NSPM-33. We urge the committee to conduct a substantive hearing examining the U.S. talent bottleneck with knowledgeable witnesses and to issue a prescriptive report to committees with a jurisdictional mandate to take action.

[1] Will Hunt and Remco Zwetsloot, "The Chipmakers: U.S. Strengthes and Priorities for the High-End Semiconductor Workforce," Center for Security and Emerging Technology, 2020.

President Xi Jinping has said that "scientific and technological innovation has become the main battlefield of the international strategic game, and the competition around the commanding heights of science and technology is unprecedentedly fierce."[2] Despite significant investments by the Chinese Communist Party to attract international science and engineering talent through its Thousand Talents Plan and other means, the United States remains the most desirable destination for the world's best scientists and engineers[3]. The Chinese Communist Party recognizes this; Chinese sources have worried that expanded talent pipelines into the U.S. "would pose a huge challenge for China."[4]

Bottlenecks in the U.S. immigration system endanger our national advantage by driving international science and engineering talent elsewhere. Indian STEM graduates can expect to wait for decades before being issued a green card.[5] A recent study suggests about 80% of STEM master's graduates leave the United States, largely as a result of policy restrictions.[6] Inaction on resolving this bottleneck is already exacting a cost. In 2021, National Defense Industrial Association members identified the U.S. human capital gap as the single most vulnerable part of their supply chain.[7] Recent studies show half of advanced STEM workers in the defense-industrial base were born abroad.[8] These reports illustrate how efforts to onshore critical supply chains may not succeed unless we also onshore the talent necessary to compete.

China is aggressively growing its domestic STEM talent pipelines. It has doubled its higher education budget in less than a decade.[9] Chinese universities are rapidly climbing global rankings. While the United States began this century with a comfortable lead, China now has double the annual U.S. STEM masters' output and will double the number of U.S. STEM PhDs within the next three years.[10] Much of this talent will be working in Pentagon-identified critical technology areas—such as AI, biotechnology, hypersonics, and space. None of these trajectories show signs of slowing down.

---

[2] May 28, 2021 speech translated by Zichen Wang.
[3] Helen Toner, "Foreign STEM Talent is the Key to Future U.S. Competitiveness," Aspen Institute, 2022.
[4] Remco Zwetsloot, "Winning the Tech Talent Competition," Center for Strategic and International Studies, 2021.
[5] William A. Kandel, Jill H. Wilson, and Sarah A. Donovan, "U.S. Employment-Based Immigration Policy," Congressional Research Service, 2022.
[6] Michel Beine, Giovanni Peri, and Morgan Raux, "International College Students' Impact on the U.S. Skilled Labor Supply," NBER Working Paper Series, 2022.
[7] "Vital Signs 2022: The Health and Readiness of the Defense Industrial Base," National Defense Industrial Association, 2022.
[8] Jeremy Neufeld, "STEM Immigration is Critical to American National Security," Institute for Progress, 2022.
[9] Ryan Fedasiuk, Alan Omar Loera Martinez, and Anna Puglisi, "A Competitive Era for China's Universities," Center for Security and Emerging Technology, 2022.
[10] Zwetsloot, "Winning the Tech Talent Competition," Center for Security and Emerging Technology, 2021.

Fixing the U.S. talent bottleneck goes hand in hand with ensuring that U.S. research is secure from theft or espionage. Drawing on the world's best and brightest allows us to accelerate scientific and technological advancement. Strengthening security standards ensures that sensitive information and intellectual property remain secure. The United States is fully capable of advancing both objectives.

We believe a security-conscious approach to strengthening our advanced STEM talent will help address the national security and global competition issues addressed in this letter. As the National Security Commission on Artificial Intelligence put it, such targeted STEM talent reforms are "a national security imperative."[11]

Preserving our ability to attract international STEM talent transcends political partisanship. The House G.O.P. China Task Force Report noted the U.S. "needs to continue to attract the best and brightest STEM talent from around the world, or risk falling behind in the global race for talent and losing its competitive advantage in innovation."[12] Similarly, the Biden administration has argued "one of America's greatest strengths is our ability to attract global talent to strengthen our economy and technological competitiveness."[13] A recent study of the National Security Innovation Base by the Reagan Institute found that current talent pipelines pose "ongoing major vulnerabilities."[14] The Future of Defense Task Force, a bipartisan initiative of the House Armed Services Committee, identified STEM immigrants' contributions to U.S. leadership as "staggering" but concluded that "immigration policy hinders the U.S.'s ability to attract and retain foreign STEM talent that instead flows to other countries, including competitors." The Task Force called for "aggressively expanding visas for STEM talent."[15] Such measures, along with vital security screening provisions, fit squarely within the spirit of this bipartisan committee's purview as key levers that will determine the outcome of strategic competition with China.

China is the most significant technological and geopolitical competitor our country has faced in recent times. With the world's best STEM talent on our side, it will be very hard for the United States to lose. Without it, it will be very hard for us to win.

Sincerely,

---

[11] "Final Report," National Security Commission on Artificial Intelligence, 2021.
[12] "China Task Force Report," 2020.
[13] "Biden-Harris Administration Actions to Attract STEM Talent and Strengthen our Economy and Competitiveness," 2022.
[14] "National Security Innovation Base Report Card," Ronald Reagan Institute, 2023.
[15] "Future of Defense Task Force Report 2020," House Armed Services Committee, 2020.

Elliott Abrams
Former Special Representative for Iran and Venezuela, Department of State
Former Deputy National Security Advisor

Ross Ashley
Former Assistant Administrator, FEMA, Department of Homeland Security

Norm Augustine
Former CEO and Chairman, Lockheed Martin
Former Chairman, Defense Science Board

Douglas Baker
Former Special Assistant to the President and Senior Director for Border and Transportation Security Policy, Homeland Security Council

Craig Barrett
Former CEO and Chairman, Intel Corporation

Kari Bingen
Former Deputy Under Secretary of Defense for Intelligence and Security

Joseph Bosco
Former China Country Director, Office of the Secretary of Defense

Scott Boylan
Former Senior Advisor to the Secretary, Department of Homeland Security

Dan Brown
Former Deputy Associate General Counsel for Immigration, Department of Homeland Security

Michael Brown
Former Director, Defense Innovation Unit, Department of Defense

Carter Burwell
Former Counselor to the Secretary for Terrorism and Finance Intelligence, Department of the Treasury

Steve Chu
Former Secretary of Energy

Rita Colwell
Former Director, National Science Foundation

Gus Coldebella
Former General Counsel, Department of Homeland Security

Barbara Comstock
Former Member, U.S. House of Representatives

France A. Córdova
Former Director, National Science Foundation

Madelyn Creedon
Former Deputy Director, National Nuclear Security Administration
Former Assistant Secretary of Defense for Global Strategic Affairs

Richard Danzig
Former Secretary of the Navy

Dana Deasy
Former Chief Information Officer, Department of Defense

Elaine Dezenski
Former Deputy and Acting Assistant Secretary for Policy Development

Lisa Disbrow
Former Under Secretary of the Air Force

Elaine Duke
Former Deputy Secretary, Department of Homeland Security

Doug Fears
Rear Admiral U.S. Coast Guard (Ret.)
Former Homeland Security and Counterterrorism Advisor to the President

Carrie Filipetti
Executive Director, The Vandenberg Coalition
Former Deputy Special Representative for Venezuela, Department of State

Michele Flournoy
Former Under Secretary of Defense for Policy

Richard Fontaine
Chief Executive Officer, Center for a New American Security
Former Foreign Policy Advisor, Senator John McCain

Marc Frey
Former Director of the Visa Waiver Program, Department of Homeland Security

John Grunsfeld
Former Associate Administrator, NASA Science Mission Directorate

John Hamre
Former Deputy Secretary of Defense

Rachel Hoff
Policy Director, Ronald Reagan Presidential Library and Institute
Former Policy Advisor, Senate Armed Services Committee

John Holdren
Former Assistant to the President for Science and Technology

Chad Holliday
Chairman Emeritus, U.S. Council on Competitiveness
Former CEO and Director, DuPont

Jamil Jaffer
Founder and Executive Director of the National Security Institute
Former Chief Counsel, Senate Foreign Relations Committee

Neal Lane
Former Assistant to the President for Science and Technology

Mark Lewis
Former Acting Deputy Under Secretary of Defense for Research and Engineering

Joe Lieberman
Former U.S. Senator from Connecticut
Former Chairman, Senate Homeland Security and Governmental Affairs Committee

Mary Beth Long
Former Assistant Secretary of Defense for International Security Affairs

Ellen Lord
Former Under Secretary of Defense for Acquisition and Sustainment

Arunava Majumdar
Inaugural Director, Advanced Research Projects Agency-Energy

Anja Manuel
Former Special Assistant to the Under Secretary for Political Affairs, Department of State

Lynden Melmed
Former Chief Counsel, USCIS, Department of Homeland Security

John Mitnick
Former General Counsel, Department of Homeland Security

Robert Mocny
Former Deputy Assistant Secretary, Department of Homeland Security

Brian Murphy
Former Chief of Operations, Center for Cyber Intelligence, Central Intelligence Agency

Henry Nau
Former White House Sherpa for G-7
Former Senior Official, National Security Council

Michael H. Neifach
Former Principal Legal Advisor, Immigration and Customs Enforcement (ICE), Department of Homeland Security Former Director for Immigration and Visa Security Policy, Homeland Security Council

David Norquist
Former Deputy Secretary of Defense

Richard Outzen
Former Senior Advisor to the Secretary of State

DJ Patil
Former U.S. Chief Data Scientist

Michael Petrucelli
Former Deputy Director, U.S. Citizenship and Immigration Services, Department of Homeland Security

Brian Roehrkasse
Former Director of Public Affairs, Department of Justice

Paul Rosenzweig
Former Deputy Assistant Secretary, Department of Homeland Security

Randall Schriver
Former Assistant Secretary for Indo-Pacific Security Affairs, Department of Defense

Al Shaffer
Former Deputy Under Secretary of Defense for Acquisition and Sustainment

John (Jack) N.T. Shanahan
Lieutenant General U.S. Air Force (Ret.)
Inaugural Director of Project Maven and the Department of Defense Joint Artificial Intelligence Center

David Shedd
Former Director, Defense Intelligence Agency

Patrick Shen
Former Special Counsel for Immigration-Related Unfair Employment Practices, Department of Justice

Gary Shiffman
Former Chief of Staff, Customs and Border Protection, Department of Homeland Security

Valerie Smith Boyd
Former Assistant Secretary for International Affairs, Department of Homeland Security

Alan Stern
Former Associate Administrator, NASA Science Mission Directorate

Daniel Twining
President, International Republican Institute
Former Foreign Policy Advisor, Senator John McCain

Stewart Verdery
Former Assistant Secretary, Department of Homeland Security

Joseph L. Votel
General, U.S. Army (Ret.)
President and CEO, Business Executives for National Security

Dave West
Former Foreign Policy Advisor to the Secretary, Department of Homeland Security

Joe Whitley
Former General Counsel, Department of Homeland Security

Jim Williams
Former Director, US-VISIT Program, Department of Homeland Security

Deborah Wince-Smith
President and CEO, U.S. Council on Competitiveness, Former Assistant Secretary, Department of Commerce

Robert Wilkie
Former Secretary of Veterans Affairs

Julie Myers Wood
Former Assistant Secretary and Head of Immigration and Customs Enforcement (ICE), Department of Homeland Security
Former Assistant Secretary, Department of Commerce

Thomas Zurbuchen
Former Associate Administrator, NASA Science Mission Directorate

ENERGY SCIENCES COALITION

Statement in Support of the Department of Energy Artificial Intelligence Act

July 30, 2024

The Energy Sciences Coalition (ESC) strongly supports and urges swift passage of the bipartisan Department of Energy (DOE) Artificial Intelligence (AI) Act. Consistent with prior ESC recommendations, the legislation gives DOE a central role in AI research and development, including unique applications in science, energy, and national security to advance DOE missions, while also mitigating risks associated with this new sector of innovation. New and expanded programs at DOE would fully leverage the agency's unique high performance computing infrastructure, existing investments in AI and machine learning, and expertise and vast amounts of data from DOE's 17 national laboratories and 35 user facilities, to drive AI innovation and address societal grand challenges.

In particular, ESC supports the four key pillars of the DOE AI Act:

- **Frontiers in Artificial Intelligence for Science, Security, and Technology (FASST) program.** This cross-cutting, whole-of-DOE effort would bring together the world's leading scientists and engineers from all 17 DOE national labs, research universities, and other research organizations to drive AI innovation for unique science, energy, and national security missions and more broadly maintain U.S. leadership in AI. This program would support fundamental math and computer science, the development and deployment of safe and trustworthy AI models and systems, early-stage engineering and prototyping of AI hardware and software technologies, and development of next-generation computing platforms and infrastructure. This program is needed to accelerate the pace of scientific discovery and technological innovation in a responsible and secure manner.
- **AI Research and Development Centers.** Consistent with prior ESC recommendations, the legislation would authorize the creation of at least 8 AI innovation centers focused on advancing unique AI applications for DOE science, energy, and national security missions. These teams of DOE national labs, universities, industry, and other research organizations would bring together unique DOE research expertise, infrastructure, and STEM education and workforce training to have significant impact. DOE has successfully used these large-

scale centers to integrate, test, and deploy new technologies and complements the innovative work advanced by individual researchers and small research groups.

- **AI Risk Evaluation and Mitigation program.** ESC supports a risk evaluation and mitigation program which would require DOE to identify and find solutions to mitigate safety and security risks related to the use of AI. This is particularly important for DOE's nuclear and other national security missions, protection of critical energy infrastructure, assessing capabilities of adversaries, and overall general understanding of potential consequences of deploying AI tools.
- **STEM Education and Workforce Development.** ESC supports allocating at least 10 percent, or about $240 million per year, of AI research and development funding to support DOE STEM education and workforce development programs in AI. This targeted investment in training programs, research opportunities, and support for new degree and certificate programs in AI-related disciplines at research universities and community colleges is needed to meet growing demand for a highly skilled and AI-literate workforce. ESC also supports efforts to expand the number of AI researchers from underrepresented groups interested in pursuing and attaining AI-relevant skills.

The legislation authorizes bold investments—$12 billion over five years—and bold new programs needed by DOE to fully develop and utilize AI for unique science, energy, and national security missions. An ESC-sponsored congressional event in July highlighted some of the early applications of AI using high performance computing capabilities. These include, to name a few: grid resilience and security; designing advanced materials that can resist very high temperatures and extremely hot plasmas for fusion reactors; safe and reliable long-term carbon dioxide storage, geothermal energy, nuclear waste isolation, and petroleum extraction; improved climate modeling prediction based on better understanding of cloud behavior and associated droughts and floods; and, in partnership with the National Institutes of Health, automating complex data analysis for new insights into cancer and developing improved treatment options, just to name a few. This important piece of legislation would help unlock DOE's potential to tackle and help solve major challenges for the nation.

We look forward to working with Congress to advance this legislation.

Sincerely,

Leland Cogliani
Co-chair
202-289-7475
leland@lewis-burke.com

Sarah Walter
Co-chair
202-434-8003
swalter@msu.edu

ESC Membership

American Association of Physicists in Medicine
American Association of Physics Teachers
American Astronomical Society
American Chemical Society
American Crystallographic Association
American Geophysical Union
American Geosciences Institute
American Institute of Physics
American Mathematical Society
American Nuclear Society
American Physical Society
American Society for Engineering Education
American Society of Agronomy
Acoustical Society of America (ASA)
American Society of Mechanical Engineers
American Society for Microbiology
American Society of Plant Biologists
American Vacuum Society
Arizona State University
AVS – The Society for Science and Technology of Materials, Interfaces, and Processing
Battelle
Binghamton University
Biophysical Society
Boston University
Case Western Reserve University
City College of CUNY
Clemson University
Coalition for Academic Scientific Computation (CASC)
Consortium for Ocean Leadership
Columbia University
Council of Scientific Society Presidents
Cornell University
Cray Inc.
Crop Science Society of America
Duke University
The Ecological Society of America
Florida State University
Fusion Power Associates
General Atomics
Geological Society of America
George Mason University
Georgia Institute of Technology
Harvard University
Health Physics Society
IBM
IEEE-USA
Iowa State University
Jefferson Science Associates, LLC
Krell Institute
Lehigh University
Long Island University
Massachusetts Institute of Technology
Materials Research Society
Miami University of Ohio
Michigan State University
Michigan Technological University
New York University
Northeastern University
Northern Illinois University
Northwestern University
Oak Ridge Associated Universities (ORAU)
Pace University
Penn State University
Princeton University
Purdue University
Rensselaer Polytechnic Institute
Rochester Institute of Technology
Rutgers, The State University of New Jersey
Society for Industrial and Applied Mathematics
Soil Science Society of America
South Dakota School of Mines
Southeastern Universities Research Association
SPIE
Stanford University
Stony Brook University
Tech-X Corporation
Tufts University
The Ohio State University
University of California System
University of Chicago
University of Colorado Boulder
University of Delaware
University Fusion Association
University of Hawaii
University of Illinois System
University of Iowa
University of Maryland, College Park
University of Michigan
University of Missouri System
University of Nebraska
University of North Texas
University of Oklahoma
University of Pennsylvania
University of Rochester
University of Southern California
University of Tennessee
University of Texas at Austin
University of Virginia
University of Wisconsin-Madison
Universities Research Association
Vanderbilt University
Washington State University
West Virginia University
Yale University