"Reassessing Threats to US Innovation Posed by China and Implications for Safeguarding Future Supply Chains"

Testimony Before the U.S.- China Economic and Security Review Commission

Hearing on "U.S.-China Competition in Global Supply Chains"

June 9, 2022

Jeffrey Stoff
Founder, Redcliff Enterprises

Table of Contents

Hearing Co-Chairs Borochoff and Goodwin, distinguished Commissioners and staff, thank you for the opportunity to participate in today's hearing. Much of what I will discuss in this testimony comes from my knowledge and experience working in the US government on China issues for nearly two decades, and in particular the last 10 years that was dedicated to examining China's technology transfer apparatus. That said, all statements of fact, opinion, or analysis provided in this testimony are my own and do not reflect the official policy or position of the Department of Defense or other federal agencies.

Introduction

My testimony will focus on US vulnerabilities, challenges and the long-term implications with respect to China regarding future supply chains. Specifically, I am referring to the R&D and human capital inputs that make up our innovation ecosystem. As this hearing discusses how to secure defense-critical supply chains, it is important that we frame our R&D and innovation ecosystem as a critical supply chain input and a national asset. *Yet this is an area that is the least protected and the most vulnerable to China's predations.*

Protecting the earlier stages of our innovation ecosystem will become even more important in the near future as the pace of technology development accelerates; in many areas timelines will likely shorten between fundamental research and the development of commercially viable or weaponizable applications.

It is also important that we have candid conversations on the challenges and shortcomings that affect our ability to protect our research and innovation. We must objectively examine our deficiencies to overcome them. To oversimplify complex issues, these deficiencies are rooted in several inter-related areas, which include:

- Underutilized US government policies and tools to address supply chain risks and related threats posed by China, such as export controls, Treasury sanctions, other trade restrictions, CFIUS, and law enforcement and counterintelligence operations. These levers are inherently tactical or transactional; they are whack-a-mole efforts by their nature and their lack of sufficient resources leaves little room to examine the strategic aspects or interconnectedness of China's predations.
- A fundamental lack of understanding of the magnitude and complexity of China's state-supported technology acquisition and transfer apparatus. This has led to misconceptions over the nature and scope of the threats China poses to our innovation ecosystem, especially at earlier stages of R&D.
- An over-reliance on law enforcement as a means of threat mitigation.
- The minimal use of publicly available information within the government, and in particular the Intelligence Community, due to structural impediments and a dearth of Mandarin language and subject matter expertise.

This testimony will describe key entities, methods, and programs the PRC party-state deploys to acquire technology and knowhow from the United States and the corresponding vulnerabilities, knowledge gaps, and impediments to mitigating threats to our R&D and innovation ecosystem. This survey is not exhaustive; rather, the examples I provide are used to dispel misconceptions of China's predations and inform the recommended solutions.

Other China and international trade experts have called for revisions to existing policies and new legislation for good reason. As such, my recommendations will focus on capacity building - bolstering the supporting infrastructure needed to allow the existing arsenal of tools, policies, and enforcement mechanisms to realize their full potential. However, this capacity building

requires new paradigms that specifically address structural impediments that have prevented the government from adequately exploiting publicly available information.

Rethinking Prevailing Concepts

The lack of understanding of the magnitude and complexity of China's technology transfer apparatus has resulted in misperceptions, some of which downplay or understate the threats posed by China and/or overestimate the United States' ability to maintain technological and military superiority. For instance, our views of risks and threats posed by China are too often placed in simplistic, binary terms. The most common of these binary constructs are legal vs. illicit activity, international research collaboration vs. shutting ourselves off, and openly shared (and published) vs. classified research.

The White House Office of Science & Technology Policy (OSTP) recently stated that "the research security challenges we face are real and serious: some foreign governments, including China's government, are working hard to illicitly acquire our most advanced technologies. This is unacceptable."[1] While OSTP rightly draws attention to research security challenges posed by China, it also typifies the US government's myopic focus on "illicit" acquisition of US technology. Indeed, US government attention and responses are often limited to fighting lawbreakers. To be fair, this is partly by design, as democracies place constraints on government power and policing. A consequence of this limitation, though noble in intent, is that *the scale and scope of national and economic security threats posed by the PRC's technology transfer apparatus have outpaced the government's abilities or priorities to detect, deter, or neutralize the PRC's efforts.* Most of the threats I describe in this testimony are neither criminal in nature nor involve espionage, at least not how our legal system defines it.

The US government's focus on pursuing criminal prosecutions through efforts like the China Initiative led by the Department of Justice (DOJ) does little to resolve or neutralize research security threats. A series of dropped cases and unsuccessful prosecutions are perhaps a reason the DOJ decided to end the China Initiative (at least in its current form). But dropping criminal charges due to difficulties in proving criminal intent does not necessarily equate to an absence of concerning activity. These cases often involved individuals employed and tasked by the PRC government and Communist Party (CPC) to facilitate knowhow transfers that can undermine the security and integrity of federally sponsored research.

The other oft-used binary arguments relate to research collaboration and partnerships (particularly in STEM fields) with PRC institutions. For example, many within the academic community reject or downplay collaboration concerns by emphasizing that the pursuit of knowledge and advancement of science are critically dependent on global scientific collaboration and the US has benefitted tremendously from it. But the importance and value of international collaboration is not in dispute. The reality is there are certain risks when dealing with authoritarian nations, especially China, which require more robust scrutiny and nuanced approaches, and this fact cannot be overlooked through zero sum or all or nothing arguments with respect to international collaboration.

In a similar vein, some within academia frequently argue that fundamental research is meant to be openly shared through publication. This was also codified in the still-in-effect National

[1] Statement by Dr. Eric Lander, "Guidance for U.S. Scientific Research Security That Preserves International Collaboration," January 4, 2022, https://www.whitehouse.gov/ostp/news-updates/2022/01/04/guidance-for-u-s-scientific-research-security-that-preserves-international-collaboration/.

Security Decision Directive 189 (NSDD-189), a policy stipulating that there should be no restrictions on the sharing of fundamental research, except in special circumstances where national security concerns necessitate making such information classified. The argument is that given that the research is openly published, there is nothing to steal or cause national security concerns.

Here too, we need to lay to rest this argument. It overlooks the issue of who or what is using the research and for what specific purpose, and bypasses the fact that the hands-on, unpublished input, knowledge, and experience that goes into conducting research in collaborative environments is not easily replicable through passive reviews of published literature. Raw data and knowhow exist and may be transferred in ways that lie outside of the published result. Why would China devote so much effort and resources -- such as through its hundreds of talent programs that recruit individuals who had placement and access to US research -- if they can just read the published literature at home and "use" it themselves?

These knowledge transfers within the research enterprise often do not involve criminal acts or espionage, but just like the intent of our export control regime, end-users matter. An obvious example is fundamental research (such as materials science and metallurgical fields) that can enhance a nation's capabilities in designing and manufacturing nuclear weapons. Would it be wise to invite PRC, North Korean, and Iranian nuclear weapons scientists to the U.S. to study advanced methods in these fields, even if some of that research is fundamental and published? "End-user" entities within China's research enterprise matter, and real national security concerns can arise from the open collaboration they enjoy with US institutions.

Lastly, many have argued that the US government's response is an overreaction or overreach. Academia has justifiably asked the US government what the scale and scope of the research security threats posed by China looks like, as the government has shared only limited information on a small number of cases that are typically the results of completed investigations. There is a great deal of unknowns and a lack of empirical evidence that have important, unaddressed, or unrecognized implications. Consequently, we need to empirically examine the issues, such as viewing research security as a research discipline itself and develop systematic ways to understand the scale and scope of what is taking place. A key challenge is that no single agency owns this problem. This requires an unprecedented level of collective action, which gets to the heart of my recommendations I will describe at the end of this testimony.

PRC Exploitation of US R&D

This section offers four case studies that show how the PRC is exploiting the open nature of our research ecosystem that have serious national security implications and may affect future defense supply chains. Specifically, these examples show how China's defense and mass surveillance R&D and industrial bases are benefiting from largely unrestricted research collaboration with the U.S.

Example 1: US Research Collaboration with China's 'Seven Sons of National Defense'

In 2020, I coauthored a study that examined collaboration between US research institutions and a group of civilian universities in China that serve its defense R&D and industrial base, known as the "Seven Sons of National Defense" (国防七子). The report surveyed published scientific and engineering literature and examined coauthor networks and funding sources and discussed findings from supplemental due diligence performed on the PRC entities involved. These seven

universities have a primary mission to support defense R&D and industry development and promote state-directed military-civil fusion efforts. Most partner with defense state-owned conglomerates and serve as a training ground for future military leaders and technicians working on weapons systems and defense programs.[2] The seven PRC universities examined are:

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)

The report surveyed six years of scientific publications (2013-2019) that name coauthors from US academic institutions or government-funded laboratories[3] and the 'Seven Sons' schools. The survey identified 254 articles naming coauthors from 115 US research institutions. It is important to note that our findings understate the level of collaboration as the collected corpus of S&T literature was limited to exploitation of a domestic PRC publication aggregator; it did not examine English-language publications from international sources. Nevertheless, our research showed that many of the PRC partners directly supported People's Liberation Army (PLA) programs, classified weapons R&D projects, and PRC state-owned defense conglomerates.

In addition to the 'Seven Sons' schools, some of the surveyed publications named other China-based collaborators who work at nuclear weapons R&D facilities, missile design and fabrication centers, and/or conduct classified weapons research projects. For instance, the Harbin Institute of Technology (HIT) partners with two state-owned defense conglomerates - China Aerospace Science & Technology Corporation and China Aerospace Science and Industry Corporation. HIT also collaborates with the PLA Equipment Development Department (formerly known as the General Armament Department) and the PLA Rocket Force, which manages the PRC's strategic and nuclear missile arsenal.[4]

We presumed in this study that all collaboration involved fundamental research and no illicit activity had occurred. None of this research was subject to regulatory oversight (such as export controls), and some US academic institutions were unaware that such collaboration was taking place. Consequently, we judged that:

- A binary test of (il)legality is not a sufficient basis for assessing risks to national and economic security regarding research collaboration with foreign entities.
- 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 China.
- Fundamental scientific research should not default to meaning that research institutions and federal funding agencies have no control over, and thus no responsibility over research partnerships and the collaborators.

[2] Tiffert, Stoff, Gamache, "Global Engagement: Rethinking Risk in the Research Enterprise," *Hoover Institution Press*, 2020, https://www.hoover.org/global-engagement-rethinking-risk-research-enterprise.
[3] Examples of US government-funded facilities included Department of Energy national laboratories, Department of Defense laboratories, and National Institutes of Health research facilities.
[4] See pages 30-31 of the Hoover report for details.

Example 2: DoD-Commissioned Studies on Research Collaboration

While I worked at the Department of Defense (DoD), I oversaw several projects that also surveyed published scientific literature - in this case to catalog research collaboration of potential concern between entities receiving DoD research funding and PRC institutions or programs. This effort was methodologically similar to the Hoover Institution study on US collaboration with China's "Seven Sons" universities. The DoD studies were also limited in scope in terms of collected data. Most of the data were derived from domestic PRC publication aggregators, supplemented with limited exploitation of international publication sources and due diligence research. These studies served as initial proofs of concept; not as exhaustive risk assessments associated with US-China research collaboration.

The collected corpus of bibliographic data of scientific publications all credited DoD funding sources (though they varied in level of detail[5]) and named coauthors affiliated with PRC institutions and/or credited a PRC funding source. Key findings from these studies include:

- Some publications list coauthors affiliated with entities subordinate to the PLA (including a key hypersonics research and testing facility), China's nuclear weapons R&D complex, national defense laboratories, and civilian research institutes with extensive ties to defense research and industry.
- In one study, 97 out of 188 identified articles credited PRC government funding sources in addition to DoD grant(s).
- Multiple studies found that some coauthors maintained concurrent positions at both US and PRC institutions. Supplemental due diligence on a few cases revealed that the US-based coauthor did not disclose his/her dual affiliation with a PRC entity on CVs or faculty pages of their US employing institutions. In other cases, some coauthors claiming dual affiliations were PhD students and/or visiting scholars that spent a portion of their time in both nations.

Further investigation is needed to identify individuals who have (or had) full or part-time employment in both countries, and whether such joint appointments were reported to their US employers, created conflicts of interest or commitment, or ran afoul of other grant compliance issues.

Challenges remain, partly because the published literature surveyed in these studies were assumed to be designated fundamental in nature, which in accordance with NSDD-189, do not require restrictions on the publication of research findings or are subject to export controls. While the level of national security risks associated with collaboration with PRC entities vary depending on the mission of the PRC organization or specific research area, there is nevertheless a real risk that China's defense R&D and industrial base is benefitting from DoD-funded research programs.

Example 3: PRC Gifts or Contracts to US Institutions

In the previous two examples, it is unclear whether the collaborations involved direct resource sharing, personnel exchanges, or other formal agreements. This raises similar questions regarding the scope of PRC funding support to US research institutions writ large in the form of grants, gifts, or contracts. Being transparent and accountable on foreign monies coming in and reported to the government and made available to the public is important, particularly for higher

[5] For instance, some publications listed full details such as the DoD component and grant number/codes while other sources just stated that the research was supported by a particular DoD component. Additionally, not all publications identify which author received the DoD funding.

education institutions that receive federal funding. Public disclosures are not just important for national security reasons and to identify potential foreign influence, but also for ethical reasons. Human Rights Watch proposed a code of conduct encouraging universities to publicly disclose annually all direct and indirect PRC government funding and a list of projects and exchanges with PRC government counterparts.[6]

There is a formal process for such disclosures. Section 117 of the Higher Education Act of 1965 (20 U.S.C. 1011f) requires US colleges and universities to report the foreign gifts and contracts they receive to the Department of Education twice each year. This requirement is for all foreign gifts and contracts valued at $250,000 or more (alone or in combination with other gifts or contracts with a foreign source). I examined this disclosure data, which is accessible on the Department of Education's website,[7] and discussed below are two areas of concern.

Between 2014 and 2019, two U.S. universities reported 16 contracts totaling roughly $4.2 million from an entity listed as "Beijing Inst of Aeronautical Materia." This is a truncated or incomplete title, referring to the Beijing Institute of Aeronautical Materials (also known as the Beijing Aeronautical Materials Technology Research Institute, or BAMTRI), a subdivision of the PRC state-owned defense conglomerate Aviation Industry Corporation of China (AVIC). BAMTRI and its parent firm AVIC develop engines, cruise missiles, and defense aircraft for the PLA and is named on the Department of Commerce / Bureau of Industry and Security (BIS) Entity List for export control purposes. Thus, a major PRC defense aerospace firm was contracting with US universities to perform research on their behalf. If that research was designated fundamental, such contracts likely did not violate US export control rules.[8] Even if such arrangements are legal, is it really in the national interest to have US institutions perform contracted research for China's defense industrial base?

In late 2020, the Department of Education issued a report that showed significant non-compliance by US colleges and universities with respect to disclosing foreign gifts and contracts mandated by the Section 117 law.[9] This trend continues unabated: an examination of newer disclosures of foreign gifts or contracts from mid-2020 (when the department revamped its reporting system) to October 2021 show a trend of failure to name specific sources. There were 4,479 records that name China as a funding source; yet only 129 of those records list the specific entity. Additionally, 4,202 records state "N/A or No" on the question of whether the source is from a foreign government. Yet nearly all universities and research institutes in China are state-run; there is a real risk that many US universities may be falsely reporting (intentional or not) information to the Department of Education.

This lack of transparency by universities on foreign revenue sources also means the government cannot assess risks or advise universities on such risks when partnering with organizations that may threaten national security or undermine US interests. Consequently, it is impossible to

[6] "Resisting Chinese Government Efforts to Undermine Academic Freedom Abroad – A Code of Conduct for Colleges, Universities, and Academic Institutions Worldwide," Human Rights Watch, March 21, 2019, https://www.hrw.org/sites/default/files/media_2020/09/190321_china_academic_freedom_coc.pdf.

[7] Both current and historical data on foreign gifts and contracts can be found here: https://sites.ed.gov/foreigngifts/.

[8] Firms listed on the BIS Entity List does not equate to a ban; it simply indicates a license is required to export certain items to that entity.

[9] "Report on Institutional Compliance with Section 117 of the Higher Education Act of 1965," US Department of Education Office of the General Counsel, October 2020, https://www2.ed.gov/policy/highered/leg/institutional-compliance-section-117.pdf.

determine to what extent PRC defense-affiliated research entities or enterprises are funding US academic research.

Example 4: US Research Collaboration with China's Mass Surveillance Apparatus

US-China research collaborations of national security concern are not limited to China's defense R&D and industrial base. Equally troubling is academic and private sector cooperation with PRC entities that are part of or support China's mass surveillance and public security apparatuses that engage in human rights abuses. This is another area that receives insufficient scrutiny. Within academia, ethical risks to research collaboration with the PRC and other authoritarian nations are rarely considered if the research does not directly involve human subjects.

I coauthored a second study with the Hoover Institution that serves as a case study on ethical risks to research collaboration and demonstrates the critical importance of conducting robust due diligence on PRC partners. The report examined the domestic and international activities and partnerships of a major AI research institution in China: the Chinese Academy of Sciences Institute of Automation (CASIA).[10] CASIA exemplifies the challenges and complexities of collaboration with PRC institutions. CASIA has a dual identity: it conducts cutting edge research in AI and neuroscience fields and collaborates extensively with institutions throughout the developed world. Domestically, CASIA partners with public security organs and develops and commercializes mass surveillance technologies that enable the PRC's documented human rights abuses.[11] Figure 1 (in the Appendix) shows CASIA's diversion of nominally benign or beneficial research areas it conducts to ethically troubling applications.

The report found that CASIA collaborates extensively with US research institutions as well as major technology firms that sponsor research. And US entities are not just supporting or enhancing CASIA's fundamental research. CASIA is already commercializing and weaponizing its R&D. There are five companies CASIA owns major stakes in whose mass surveillance products and services -- including video surveillance and gait, iris, and facial recognition -- were born directly out of CASIA laboratories and research centers. These five companies contract with PRC public security organs, and at least two of them explicitly state they deploy their capabilities in the Xinjiang region where the party-state has engaged in genocide, mass incarceration, and other documented human rights abuses against the ethnic Uyghur and other Muslim minorities. These firms also partner with defense conglomerates and other companies known to support China's mass surveillance apparatus, such as Huawei and Hikvision.[12] Several of these commercial spinoffs claim to partner with or procure equipment from major US semiconductor firms. CASIA also owns equity stakes in at least 30 other companies, though further research is needed to determine the types of technologies those companies develop.

At the time of this testimony, neither CASIA nor its commercial operations are on the BIS Entity List. However, Tan Tieniu, one of CASIA's senior leaders and an expert in computer vision and surveillance technologies, concurrently serves as Deputy Director of the PRC government's Hong Kong office. He was placed on the US Treasury Department's "specially designated nationals list" as part of the US government's sanctions on Hong Kong officials for their

[10] Stoff, Tiffert, "Eyes Wide Open: Ethical Risks in Research Collaboration with China," *Hoover Institution Press*, 2021, https://www.hoover.org/sites/default/files/research/docs/stoff-tiffert_eyeswideopen_web_revised.pdf.
[11] Ibid.
[12] Ibid.

responsibility for a human rights crackdown in the city.[13] Yet Tan has played a central role in facilitating international cooperation agreements with both academic institutions and private companies from the U.S. and its allies.

Knowledge Gaps with Respect to China's Defense R&D and Industrial Base

China's exploitation of our research enterprise that may affect future supply chains described in the previous section is a complex problem. Securing or restricting existing US supply chains, both inbound and outbound, is at least conceptually a more straightforward problem. Much of the focus has been on identifying our vulnerabilities and choke points, such as over-reliance on China and/or a small number of suppliers of a particular input (e.g., pharmaceutical ingredients, rare earth metals, etc.). Equally important, however, is that the U.S. must have a clear picture of what China's defense research and industrial base looks like that may be in our critical technology supply chains. The previous example on CASIA identified unknown elements to China's mass surveillance R&D and supply chains. Similar efforts must be made to address the yawning knowledge gaps in this area.

Our knowledge gaps can substantially be attributed to a) the US government's inadequate use of and arguably its devaluation of publicly available information as a source of intelligence; and b) China's lack of transparency over corporate structures and ownership, minimal use of English (Chinese language serves as a form of encryption), and deliberate obfuscation of the nature or missions of key entities. I offer two examples that are illustrative of this problem.

Case Study: China Electronics Technology Group Corporation

Many of China's centrally managed state-owned enterprises (SOEs) are large conglomerates that can have hundreds or even thousands of subsidiaries or investments. Their ownership stakes can include other SOEs, publicly traded companies, privately held firms, and joint ventures with foreign businesses. China's state-owned defense conglomerates are no exception, and the China Electronics Technology Group Corporation (CETC) is an illustrative example.

CETC specializes in all aspects of electronics, microelectronics, and electronic information for the PLA as well as for civilian purposes such as public security, intelligent transportation, and new energy. It reportedly conducts business internationally in more than 110 countries and regions.[14] According to a 2021 securities filing, CETC had more than 200,000 employees, and encompassed more than 700 subordinate companies and public institutions. The latter includes 47 research institutes, 16 publicly traded companies, and 35 state key laboratories, research centers, and innovation centers.[15]

However, the BIS Entity List only names about two dozen CETC subsidiaries and research institutes. I am not aware of any efforts by the US government to survey all of CETC's subordinate entities and determine whether they are involved in US supply chains (import products to the U.S.), whether US firms have partnerships (such as joint ventures) or export

[13] "Publication of Hong Kong Business Advisory; Hong Kong-related Designations," US Department of the Treasury, July 16, 2021, https://home.treasury.gov/system/files/126/20210716hongkongadvisory.pdf.
[14] "China Electronics Technology Group Corporation," website of China Services Info, April 19, 2019, http://govt.chinadaily.com.cn/a/201904/19/WS5cb99627498e079e6801e9bc.html.
[15] "Issuance of Public Securities for CETC - Prospectus, November 17, 2021, file.finance.sina.com.cn/211.154.219.97:9494/MRGG/BOND/2021/2021-11/2021-11-17/16545564.PDF

hardware components or software to CETC entities, or whether there are US outbound investments in CETC affiliates.

This issue is particularly relevant within the context of semiconductors and microelectronics, given the criticality of the industry to our defense supply chains and increased calls to reduce our reliance on China via the CHIPS for America Act[16] and related legislation. A nascent survey of CETC-owned firms demonstrates the need for bolstering our due diligence efforts in this space. Table 1 (in the Appendix) lists five semiconductor or microelectronics firms in which CETC holds majority stakes in. It is notable that "CETC" or its name variants are excluded from these firms' names and none of them appear on the BIS Entity List. Table 1 is a mere sampling and should not be construed as a comprehensive inventory of CETC affiliates involved in semiconductor or related industries.

University-Industry Partnerships

China has a well-developed system of university and industry partnerships, such as dedicated S&T and industrial parks attached to or co-managed by major universities and innovation and technology transfer centers that seek to commercialize R&D conducted in academia. Some universities, including the "Seven Sons of National Defense" schools and other major scientific and engineering institutions like Tsinghua University, have commercial spinoffs and holding companies that make commercial investments both domestically and internationally. Jason Arterburn has conducted research in this area and shared some of his findings in previous testimony to this Commission. For example, Arterburn examined corporate records on the Harbin Institute of Technology (HIT, one of the 'Seven Sons' schools) and found that HIT has direct or indirect ownership interests in approximately 1,000 China-based companies and owns a 50-percent or greater ownership interest in approximately 50 entities.[17]

This offers a glimpse into the scale and scope of what may comprise China's defense industrial base outside the major SOEs. Needless to say, far more research needs to be done in this area to understand the supply chain implications.

Knowledge Gaps on PRC Universities Supporting Defense R&D

China's State Administration for Science & Technology Industry for National Defense (SASTIND) was established in March 2008 as the successor to the Commission for Science, Technology, and Industry for National Defense (COSTIND, 国防科学技术工业委员会) after a State Council reorganization that also created the Ministry of Industry and Information Technology, which oversees SASTIND.[18] SASTIND has joint development agreements with the Ministry of Education and provincial governments to promote defense-related research and education programs at over 50 PRC universities. These agreements have focused on recognizing and developing defense-related academic disciplines, key laboratories, and research groups at the universities, incentivizing researchers to apply for defense research funding, and promoting collaboration between university labs and defense industry firms and research institutes.[19]

---

[16] https://www.congress.gov/bill/116th-congress/house-bill/7178
[17] Jason Arterburn, "The Party-State in China's Military-Industrial Complex: Implications for U.S. National Security," Testimony to the US China Economic Security Review Commission, March 19, 2021.
[18] http://www.gov.cn/2008lh/content_921411.htm.
[19] https://www.sohu.com/a/255615361_396354

These universities that partner with SASTIND receive less scrutiny than the "Seven Sons of National Defense" in part because they do not have the same degree of involvement in defense-related research. SASTIND's support is typically limited to select departments, divisions, and labs within these universities. Thus, more robust due diligence research is needed to assess national security risks associated with collaborations with these PRC universities.

Compounding this challenge are deliberate efforts by the PRC to obfuscate information on entities supporting defense programs. An illustrative example is the University of Electronic Science and Technology of China (UESTC), one of the civilian universities co-managed by SASTIND. The English-language version of its website describing its organizational structure has a page entitled "Labs & Centers." This page lists only one entity it calls the "National Key Laboratory of Science and Technology on Communications."[20] Figure 2 (in Appendix) provides a screenshot of that English webpage.

In contrast, UESTC's Chinese-language website that corresponds to the English version lists nine entities, including one of the official names of the "communications laboratory" mentioned on the English page. Figure 3 (see Appendix) shows a screenshot of that Chinese webpage. A translation of the corresponding Chinese name is the National Technology Key Laboratory on Anti-Interference Communications, also referred to as the National Defense Technology Key Laboratory on Anti-Interference for Tactical Communications.[21] The pronounced difference between the English and Chinese versions suggests deliberate obfuscation to avoid international scrutiny. In addition, at least two of the other centers listed only on the Chinese page likely involve defense research, including a laboratory for "electromagnetic radiation control materials" and a laboratory for "extremely high frequency complex systems."[22]

Tapping into US Innovation

A key element of China's technology transfer apparatus are the tethers it has built to tap into the R&D and innovation occurring inside the U.S. In addition to benefitting from informal research collaboration and partnerships with US academic institutions described in the previous section, China's party-state deploys official and unofficial proxies; investment structures such as venture capital funds, incubators and innovation centers; start-up contests; talent programs and supporting recruitment networks; and partnerships with diaspora organizations, at least some of which are part of China's United Front apparatus commonly and myopically viewed in terms of political influence operations. A comprehensive examination of these areas exceeds the scope of this testimony and the topic of today's hearing. Instead, I offer a few examples of how this works and their implications.

A glimpse of China's evolving strategy to exploit US innovation can be gleaned from CPC policy documents and leadership speeches. In the book *China's Quest for Foreign Technology: Beyond Espionage,* contributing author Andrew Spear compiled excerpts of these policy

[20] https://en.uestc.edu.cn/Academics/Labs_Centers.htm
[21] The Chinese names are "战术通信抗干扰技术国防科技重点实验室," also known as "通信抗干扰技术国家级重点实验室." UESTC uses both of these Chinese name variants.
[22] The Chinese webpage listing these centers can be found here: https://www.uestc.edu.cn/211202a06493bf4a2a046d2b638cf5dd.html?n=8e7z368tn51.

documents.[23] A sampling of these statements along with the year in which they appeared include:

> "Fully exploit overseas talent resources and encourage overseas scholars to serve the motherland through various methods while that are studying or working overseas." (2009)
>
> "China must deepen international exchange and cooperation, fully use global innovation resources, [and thereby] advance indigenous innovation from a higher starting point, actively deploy and proactively use international innovation resources." (2013)
>
> "Adopt flexible and diverse methods to strengthen connections and communications with overseas-based Chinese student, scholar, and professional groups in order to provide them information, consultation, and 'matchmaking' services." (2014)
>
> China should "mobilize talents to engage in offshore innovation in foreign countries" or "attract 'migratory bird talent to engage in part-time innovation in China, while employed overseas." (2018)

Case Study: ZDG Group

A state-owned investment firm and technology incubator known as Zhongguancun Development Group Co., Ltd. (ZDG) and its US operations is a good example of how these policies have been put into practice.

In early 2017, at the "Beijing Silicon Valley High-level Talents Summit," eight American scientists were hired by the ZDG as the first batch of a newly created "Zhongguancun Overseas Strategic Scientists Program." The PRC Consul General San Francisco and the head of the Organization Department of the Beijing Municipal Party Committee unveiled the program, which seeks to recruit top scientists from prestigious US universities.[24] ZDG is a state-owned investment enterprise with operations in the US that seeks to invest in and/or acquire technologies and incentivize firms to set up operations in Beijing's technology district Zhongguancun.[25]

In a press interview, ZDG's Chief Operating Offer explained the reasoning behind the Zhongguancun Overseas Strategic Scientists program. He stated, "it is not always necessary for talents to return to their country. Rather, with the establishment of [this program], top scientists with outstanding achievements abroad can not only contribute to China's scientific research while in the United States, but also cultivate talent and continuously connect overseas talents with Chinese entrepreneurs and capital…This is a new option for those scientists who want to serve their country."[26]

In other words, a PRC state-owned entity, a PRC Consulate General, and a Communist Party official in charge of talent recruitment were involved in or supported establishing a program to hire US scientists to help the party-state with critical technology offshoring to China and talent recruitment efforts while remaining in the U.S. Supplemental research indicates that most of the

---

[23] See chapter 2 written by Andrew Spear of William Hannas and Didi Kirsten Tatlow, editors, *China's Quest for Foreign Technology: Beyond Espionage,* (Routledge, 2021). Note I authored three chapters of this volume.
[24] "中关村硅谷创新中心招才引智新方式: 引 '才'留 '人'", *People's Daily Online (Renminwang),* March 7, 2017, http://world.people.com.cn/n1/2017/0307/c1002-29129869.html.
[25] A discussion of Zhongguancun Development Group and its US strategy appeared in: "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, Office of the US Trade Representative, March 22, 2018, pages 145-147, https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF.
[26] "中关村硅谷创新中心招才引智新方式: 引 '才'留 '人'", *People's Daily Online (Renminwang),* March 7, 2017, http://world.people.com.cn/n1/2017/0307/c1002-29129869.html.

recruited scientists have worked on federally sponsored research throughout their academic careers, including from DoD.

PRC State-Sponsored Startup Contests

The PRC government sponsors many start-up or entrepreneurial contests that incentivize individuals to establish businesses in China. These start-up contests are often organized and controlled out of PRC diplomatic posts across the U.S. Overseas-based scholars, graduate students, and employees of technology companies pitch ideas for a start-up based on the research or technology they worked on in the U.S. These contests have grown in number over the last decade, and they now number at least several dozen that hold initial contest rounds in the U.S. (and other nations) to select finalists. Overseas finalists receive PRC government stipends to travel to China for the final rounds. Winners receive incentives to found businesses, such as low-cost financing, venture capital investment, housing, and free space in designated S&T and returnee parks.

PRC diplomatic missions and CPC organs have co-opted US-based professional associations to help host, organize, and serve as judges of the start-up contests. Many of these partnering entities are US nonprofit organizations that do not have to disclose donors and sources of revenue. Some of the co-opted diaspora groups also partner with China's United Front system. The United Front has traditionally been viewed as leading China's global political influence operations that co-opts organizations around the world to promote and project the CPC's interests. Less understood is that United Front operations include co-opting US-based entities to carry out technology transfer activities.[27] The start-up contests these organizations support also evade regulatory scrutiny such as export controls or the Committee on Foreign Investment in the United States (CFIUS) as no transactions occur on US soil.

Venture Capital Investments

Entities that enable PRC state-supported technology and knowhow transfers also support efforts to invest in or acquire technology firms and startups in the United States. Venture capital (VC) firms with close ties to or directly owned by PRC national or municipal government entities are active in major US technology hubs. The aforementioned ZDG is one example. Another is the PRC's flagship recruitment program, the Thousand Talents Program. This program has its own state-owned venture capital (VC) fund with a branch in Silicon Valley that provides "angel" or early round investments in technology startups and recruits talent from these firms to transfer the technology to China.[28]

According to an insider in the VC community I spoke with, some VC firms have shared sensitive startup company information obtained under the auspices of participating in an investment round, but subsequently provided that information to competitor firms (including PRC-based companies). It is unclear if VC firms with managing partners and staff from China conduct sufficient security vetting of those individuals (or are even incentivized to do so). There are risks that PRC nationals may be tasked, funded, or directed by PRC state entities to access business

[27] Alex Joske and Jeffey Stoff, "The United Front and Technology Transfer," Chapter 15, Hannas, Tatlow, eds., *China's Quest for Foreign Technology: Beyond Espionage*, Routledge, 2020.
[28] Additional examples of the investment activities and forums held in the U.S. by PRC-affiliated entities appear in Appendix 9 of: Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of US Innovation," *Defense Innovation Unit Experimental,* January 2018.

plans, deal flow, and influence seed investment decisions that may be diverted to China's benefit. Additionally, PRC state-backed investment entities are active in the US and partner with VC firms on investment rounds, some which obfuscate their PRC government backing which complicates risk assessment efforts by partnering VC firms or startups seeking capital. This can be particularly problematic for US startups that hope to contract with DoD in the future, as the PRC investors may create unacceptable foreign ownership, control, or influence risks to the DoD.

Tapping Into Talent Pipelines

China's state-sponsored talent recruitment programs are an important part of the overall technology acquisition strategy. They are run at national, provincial, municipal, and individual institution levels, and are woven into government and party organs, SOEs, research institutions, national laboratories, nominally private industry, domestic and overseas "NGOs," and global diaspora organizations. These programs have a singular purpose: to recruit experts of any nationality to transfer to China intellectual capital and property from overseas (agnostic to the legality of such activity) to bolster the PRC's economic, technological, and military competitiveness. Some of the national talent programs have been around long enough (some over two decades) such that many key leaders in critical technology fields in China were recruited from overseas through these programs. This is especially the case in areas where China is near-peer or perhaps overtaking the U.S., such as AI, hypersonics, and quantum communications.[29]

The US government has increased scrutiny over these talent programs given the national security implications and the fact that some selectees were tasked or incentivized to commit economic espionage or trade secret theft, and policymakers and members of this Commission are likely familiar with them given the significant media coverage and government messaging. My focus here is to highlight the persistent vulnerabilities and challenges to mitigating threats posed by these programs, and address misconceptions due to knowledge gaps.

The Australian Strategic Policy Institute, a government-funded think tank, has identified about 200 PRC state-sponsored talent programs.[30] However, US government efforts to date to identify and mitigate threats posed by these talent programs have focused primarily on the illegal activities of selectees of just a few of the nationally run programs. Consequently, the scale and scope of China's talent programs targeting US innovation (legally or not) are largely unknown.

Vulnerabilities to DoD-Funded R&D

While I worked for the Department of Defense (DoD), I led several projects that sought to identify and assess vulnerabilities to DoD investments in unclassified arenas. Both the Intelligence and Security and Research and Engineering divisions of the Office of the Secretary of Defense recognized the need to better understand the threats and challenges posed by the PRC in unclassified R&D domains. The studies identified potential instances where China was exploiting DoD investments for its benefit.

There has been a lack of oversight in this area largely because many of the identified threats posed by China are not illicit in nature. Nevertheless, the projects highlighted national security

[29] Jeffrey Stoff, "China's Talent Programs," Chapter 3 of *Beyond Espionage: China's Quest for Foreign Technology*.
[30] Alex Joske, "Hunting the Phoenix: The Chinese Communist Party's Global Search for Technology and Talent," *Australian Strategic Policy Institute,* 2020, https://www.aspi.org.au/index.php/report/hunting-phoenix.

concerns that can have serious implications with regards to future defense supply chains and warfighting capabilities. The projects sought to address these questions:

- What is the scale and scope of China's technology acquisition and transfer activities affecting unclassified DoD programs or investments?
- What does this threat landscape look like regarding research designated as fundamental that are not subject to export controls or other regulatory oversight?

The previous section of this testimony discussed research collaboration of national security concern that involved both DoD funding and PRC research institutions or programs. DoD-commissioned studies also examined PRC talent programs that recruited individuals involved in DoD-funded research.

In aggregate, these studies identified over 300 individuals who were recruited through a talent program that claimed to have supported DoD-funded research either as the Principal Investigators (PIs) or co-PIs (i.e., individuals that received DoD funding and oversaw the research projects), or the PhD students, postdoctoral researchers, or visiting scholars that helped conduct the research. Numerous programs run at national, provincial, and local levels had recruited these US-based individuals, although the nationally run programs such as the Thousand Talents and Changjiang Scholars Award Programs represented about half of all identified selectees.

It is important to note that further investigation would be required to determine if any individual engaged in illicit activity. However, based on engagement with the responsible DoD program and policy offices, we concluded that very few of the concerns raised in these studies likely involved criminal violations. Other key findings include:

- Some selectees were full-time US faculty members and PIs of DoD grants who are experts in their field with years of experience working on US government funded research. Many of those individuals did not disclose their China commitments or positions on DoD grant applications,[31] nor did they detail their (often extensive) China-based commitments, positions, or activities on their CVs or faculty pages on US institution websites.
- Roughly half of the identified PIs also supported other federal agency sponsored research, especially the National Science Foundation, Department of Energy, and National Aeronautics and Space Administration (NASA).
- Most of the US-based experts that served as PIs or co-PIs have trained PRC graduate students and postdoctoral researchers who subsequently return to China and engage in defense research programs.
- Roughly two-thirds of identified talent program selectees were graduate students, postdoctoral fellows, and visiting scholars - not the PIs themselves.
- Nearly all selectees have held appointments or affiliations with PRC entities that support defense research, or they collaborate with scientists associated with China's defense R&D and industrial base. These entities include China's nuclear weapons complex, PLA hypersonics facilities, state-owned defense conglomerates, and major civilian research institutions that conduct defense research.

In nominal terms, the affected DoD grants and PIs recruited by a PRC talent program represent a small fraction of the thousands of research grants and dollars awarded annually. Some may argue

[31] Some of these disclosures may not have been required at the time these studies were conducted. Changes in disclosure policies have been implemented since then, and National Security Presidential Memorandum-33 is establishing a set of government-wide standards on types of information required to be disclosed on federal grants.

that this indicates the risks to DoD are small and manageable. There are several problems with that argument. First, these studies were limited in scope and surveyed only a few of the DoD components that fund academic research. The number of identified talent program selectees (about 300) also constrained our ability to examine every individual to assess security or integrity risks. These projects represented an initial effort to identify areas of concern that warrant more systematic scrutiny across all DoD elements; they were not designed to be exhaustive threat assessments.

Secondly, some of the identified individuals who were PIs on DoD grants have overseen federally funded research for a decade or more and have trained multiple generations of graduate students and postdoctoral researchers who were subsequently recruited into talent programs and contribute to the PRC's defense R&D and industrial base. Some of the graduate students and postdoctoral researchers trained by PIs have no known association with talent programs, but now work on PRC defense research programs. Thus, the small number of identified PIs have influenced a much larger number of individuals of national security concern not reflected in the number of identified talent program selectees. Complicating this problem is that most DoD program offices do not have sufficient mechanisms to track and perform due diligence on key performers of research grants in academia other than the PIs.

Vulnerabilities to DoD's SBIR Programs

Another DoD commissioned study I oversaw sought to identify specific risks and vulnerabilities posed by China's tech transfer apparatus that affect DoD-funded Small Business Innovation Research (SBIR) programs. This was a small, pilot effort to document the nature of the identified risks and recommend solutions to address SBIR program vulnerabilities. That effort narrowly focused on case studies involving entities that directly or indirectly support China's defense R&D and industrial base. Limited resources constrained the number of cases and due diligence research performed. Nevertheless, the study found that China has benefited from DoD's SBIR programs and reveal vulnerabilities to potential future DoD supply chains. Some key findings include:

- DoD's SBIR program lacks standard, DoD-wide capabilities and resources to conduct adequate due diligence on funding recipients *pre- and post-award* of a contract to assess national security risks or monitor for compliance. The program primarily relies on self-certifications by offerors.
- Some key employees of US firms receiving SBIR funding were recruited via a PRC talent program and relocated to China, but they continued research collaboration with officers of the US companies where they were previously employed.
- US firms established PRC-based subsidiaries, and in some cases, later dissolved US operations and received PRC government investments.
- In one observed case, a recipient of multiple DoD SBIR contracts established another firm in China based on the same technologies and has reportedly worked on wheeled combat vehicles in partnership with a subsidiary of state-owned defense conglomerate China North Industries Group Corporation (中国兵器工业集团公司, NORINCO). NORINCO is one China's largest weapons and defense systems manufacturer.
- US firms received VC funding from PRC sources, including state-owned enterprises that create potential foreign ownership, control, or influence risks.

- PRC researchers have conducted (and published) detailed analyses of US Navy SBIR programs over time to deduce DOD technology development priorities and catalogue firms that receive the most SBIR funding.

The case studies examined in the SBIR study represented a very small sample of SBIR awardees, but nevertheless demonstrate the need for more robust due diligence for national security risks both pre- and post-award of a contract.

Implications of Other Federal Agency-Funded Research

Another challenge is the dual-use nature of STEM and biomedical research conducted in academia that is exploited by China. An illustrative example is a US university professor who received funding from the National Institutes of Health (NIH) to develop hearing aids using AI applications applied to audio signal processing and speech segregation. While working on this NIH-funded research, that professor was recruited through the Thousand Talents Program, holding a concurrent appointment at Northwestern Polytechnical University's School of Marine Science & Technology.[32]

Northwestern Polytechnical University (NWPU) is one of China's "Seven Sons of National Defense" universities and extensively supports PLA Navy programs. Its School of Marine Science & Technology conducts "scientific research and personnel training in the fields of underwater weaponry, hydroacoustic engineering, underwater vehicles, and marine engineering."[33] In other words, NWPU hired this US professor to help develop underwater warfare applications (probably involving submarines) from the NIH-funded signal processing technology.[34]

NIH is not equipped nor mandated to assess national security risks associated with potential future applications of the type of research it funds, and DoD has no oversight or control over what other federal agencies fund. The PRC has a history of diverting research to military use applications and although such research is not overseen by DoD, the research runs the risk of affecting or undermining the US military's future warfighting capabilities. The lack of oversight or scholarship over such exploitation of STEM and biomedical research makes it impossible to determine how pervasive or successful China's efforts in this area have been.

Conclusion and Recommendations

The examples discussed here provide a glimpse into the complexity of China's apparatus to target and exploit US research, expertise, and training pipelines that will be part of our future critical technology supply chains. This is not a comprehensive survey of all aspects to China's system. Nevertheless, an important implication is that concepts of "running faster," such as investing more in domestic R&D and reshoring critical supply chains will make little difference if there are insufficient efforts to identify and mitigate the various means China deploys to siphon, invest in, influence, or divert US innovation for its benefit.

---

[32] https://web.archive.org/web/20160624032139/http://www.nwpu.edu.cn/info/1279/12650.htm; and "Brief biography," http://www.freekaoyan.com/guide/daoshi/2019/05-27/1558903628393839.shtml.

[33] "西北工业大学 航海学院 (Northwestern Polytechnical University School of Marine Science & Technology), https://hanghai.nwpu.edu.cn/xygk/xyjj.htm.

[34] It is worth noting that the professor's Thousand Talents appointment and formal position at NWPU do not appear on his CV or faculty page (or were perhaps removed), raising integrity concerns as well.

China's extensive mechanisms to tap into US talent and R&D to "serve China while overseas," weakens the argument that high rates of PRC nationals who stay in the U.S. after receiving advanced degrees means America, not China is benefitting from this talent pool and thus the threats posed by PRC talent programs are overblown. PRC talent programs and related strategies are designed to transfer knowhow, technology, and research to China often without having individuals relocate there, and these programs target individuals *after* they have gained expertise and/or access to cutting edge technologies and research. Note these risks are not unique to the United States. China deploys the same methods, organizations, and supporting infrastructures throughout the developed world to exploit innovation wherever it occurs.

Another problem is the lack of systematic efforts to identify and assess China's defense R&D and industrial base and mass surveillance apparatus and their supporting entities and infrastructure, hampering the effectiveness of existing trade restrictions, export enforcement, supply chain risk management, and related measures.

Challenges and Limitations to Protecting Our Innovation

Effective recommendations require addressing our knowledge and regulatory gaps and their root causes. Here I will highlight some of the key challenges within the government, academia, and the private sector that limit our ability to protect earlier stages of our innovation ecosystem.

The examples provided in this testimony involve activities that are typically not illicit in nature and/or circumvent regulatory oversight. This limits both the scope and effectiveness of law enforcement tools in combating China's predations. The US Intelligence Community (IC) also has its own mission constraints. In 2020, the House Permanent Select Committee for Intelligence (HPSCI) issued a report that examined the Intelligence Community's (IC) competencies with respect to China. The report concluded that the IC "has not sufficiently adapted to a changing geopolitical and technological environment increasingly shaped by a rising China." The report noted the IC lacks sufficient language, cultural, and subject matter expertise on China.[35]

China's domestic S&T development relies heavily (at least for now) on tapping into international resources and expertise. Consequently, assessments of China's critical technology development and its defense R&D and industrial base require *both* an examination of China's domestic capabilities and infrastructure *and* its corresponding technology transfer apparatus. In my opinion, the IC and the government writ large are doing little in either space. As the HPSCI report states, "foreign science and technology (S&T) capabilities, plans, and intentions have been less of a priority for US collection and analysis than other traditional foreign intelligence topics, such as leadership, military, political, and economic intelligence."

Another cause of our knowledge gaps relates to the IC's over-reliance on classified information sources and the minimal use of or resources applied to publicly available information or open-source intelligence (OSINT).[36] A recent study by the Center for Strategic & International Studies, pointed out that the availability of publicly available information, commercially-acquired data, and AI or machine learning solutions developed outside of the IC, combined with

[35] House Permanent Select Committee on Intelligence, "The China Deep Dive: A Report on the Intelligence Community's Capabilities and Competencies with Respect to the People's Republic of China," 2020, https://intelligence.house.gov/uploadedfiles/hpsci_china_deep_dive_redacted_summary_9.29.20.pdf.

[36] OSINT is differentiated from publicly available information in how the information is acquired, used, and analyzed within the IC, not by the sources of information themselves.

the IC's unwillingness to exploit such information has resulted in the "IC's diminishing primacy as the source of intelligence analysis for policymakers."[37]

For instance, while I served in the government, I supported offices responsible for conducting CFIUS threat assessments. I observed that except for the Office of the US Trade Representative, federal agencies rarely used domestic PRC sources of information in the vernacular. At interagency meetings, I advised that CFIUS threat assessments could be substantially improved if the process utilized publicly available data sources in China that include information on corporate registries, securities filings, business and industry sector descriptions, and shareholder ownership stakes. To my knowledge, no such efforts have been made to use these Mandarin-language sources. This is unfortunate, as there can be significant differences in content between English and Mandarin sources related to company information. A government colleague described this discrepancy as "reverse marketing," i.e., companies downplay or minimize information in English discussions of their mission, customers, and types of products or services they provide to avoid international scrutiny.

Challenges, Risks Facing Academia, Private Sector

Table 2 (in Appendix) lists some key impediments that limit the US government's effectiveness at countering the PRC's technology transfer apparatus. In addition to the government, academic and private sector institutions face their own challenges that make them vulnerable to China's predations. These include (but are not limited to):

- Academia lacks resources, subject matter knowledge, or incentives to conduct due diligence on foreign research partners and foreign sources of revenue
- Ethical risks to research collaboration with the PRC and other authoritarian nations are rarely evaluated if the research does not involve human subjects; research institutions may be enabling human rights abuses and development of mass surveillance capabilities of adversarial nations
- Universities' lack of transparency on foreign revenue sources means there is little scrutiny over ethical, integrity, national security, or malign foreign influence risks
- Universities that employ faculty who have concurrent appointments in China (typically through talent programs) may create conflicts of commitment / interest or related compliance risks on federal grants
- University administrators are generally unaware of activities that violate the integrity of research by faculty who are under contract with PRC institutions and tasked with undermining merit-based hiring, filing patents in China based on US-funded research, exploiting US facilities to support "shadow labs" in China, etc.
- Research conducted at technology firms or corporate-sponsored research in academia receive little scrutiny, and risks to the security or integrity of that research are rarely assessed
- PRC state-sponsored talent programs and start-up contests recruit individuals working at US technology firms and startups that encourage unauthorized transfers of knowhow to PRC competitors, yet the private sector generally lacks capabilities to identify such risks
- The US VC community does not adequately vet investment partners or portfolio companies that represent substantial foreign ownership or control risk; PRC entities can exploit private deal flow and business plan information without US investors' awareness

[37] "Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation," *Center for Strategic & International Studies*, January 2021.

Recommendations

In a recent study, Jon Bateman provided a comprehensive catalog of the authorities, tools, and trade policies the US government has in its arsenal, many of which can be brought to bear with regards to safeguarding our critical supply chains.[38] When combined with IC and law enforcement authorities and operations, the government has a dizzying array of levers it can utilize. Yet many of the agencies that can deploy these tools lack sufficient resources to fully realize their potential. This is particularly true with respect to the inputs needed to conduct research and assessments on China.

As such, my recommendations focus on bolstering the supporting infrastructure that can make the existing arsenal of government tools more effective, rather than proposing new authorities, policies, or legislation. Much of the collection and analysis can come from publicly available information. Past hearings of this Commission have discussed the value and criticality of using OSINT and publicly available information; for example, previous testimony and a related report by Jason Arterburn offers an excellent framework for conducting due diligence on China entities of national security import.[39] However, this capacity building requires new paradigms that can address the structural impediments that have prevented federal agencies from adequately exploiting publicly available information and can also provide support to academic and private sector institutions.

A New Paradigm for Collective Action

Based on my experience working with many federal agencies and overseeing open-source collection and analysis programs, it is my view that no government agency or program can overcome their structural limitations without a radical transformation of their missions, priorities, and resources. That would be a difficult task and could create zero-sum game effects; other missions would need to be descoped that could have unintended or dangerous consequences. Additionally, constitutional and regulatory limits constrain certain missions of federal agencies (particularly the IC and law enforcement), for reasons that may not make sense to change.

Consequently, I recommend Congress and federal agencies support the buildout of an independent, non-governmental entity known as the Center for Research Security & Integrity (CRSI).

CRSI will be a non-profit organization whose mission is to protect the US research and innovation ecosystem from harmful foreign influence and interference. CRSI will assist academic, government, and private sector institutions in mitigating risks to the security and integrity of research from adversarial or authoritarian nations, starting with China. A key element can include data collection, analytic, and research support to our trade and export control regimes, such as nominating organizations to be added to the BIS Entity List and/or Treasury sanctions.

---

[38] Jon Bateman, "U.S. – China Technological 'Decoupling': A Strategy and Policy Framework," *Carnegie Endowment for International Peace,* 2022.
[39] Jason Arterburn, "Party Capital: A Blueprint for National Security Due Diligence on China," *C4ADS*, 2021.

I have initiated the process to incorporate CRSI as a nonprofit organization and an application for 501(c)(3) designation with the IRS is forthcoming. CRSI intends to operate on the following principles:

- CRSI serves the public interest by maintaining the highest standards of expertise and analytic rigor and offers unbiased, empirically driven products and services tailored to the needs of the research enterprise.
- CRSI will be built on public-private partnerships via a consortium of *select* private sector firms that conduct industry-leading open source and due diligence research, think tanks, NGOs, and academic institutions that have capabilities to support research security efforts. This consortium will combine unique capabilities and resources of each of its members which would surpass existing structures.
- CRSI will produce products and services tailored for stakeholders of all sizes and shared in a trusted manner that do not compromise privacy protections or sensitive matters. A core mission will also include projects designed for public sharing and awareness.

CRSI's will undertake three lines of effort: R&D, operations, and information sharing and outreach, all of which are centered on identifying ethical, national security, research integrity, and regulatory (compliance) risks for public and private sectors focusing on "left of theft" areas. Each of these efforts may overlap, and the R&D will be foundational to all activities as it builds the required technical and analytic infrastructure.

- **R&D efforts:** Build due diligence and data collection methods; develop risk assessment and risk rating schema; conduct studies on PRC state-directed knowhow transfers and malign influence on research; map China's defense and surveillance R&D and industrial bases; conduct critical technology vulnerability assessments
- **Operational efforts**: Provide risk advisory and due diligence services to academia, government, and private sector clients; support grant compliance monitoring and risk assessments for federal agencies; build training programs for government and academia
- **Information sharing/outreach efforts**: Publish studies, trends, and analyses; convene public and private workshops and seminars

CRSI's consortium structure allows for agility, cost savings, and unique advantages that other entities lack, such as:

- **Resource sharing:** CRSI's mission aligns with select NGOs and think tanks that are part of the consortium; some projects need not be funded or staffed entirely by the center; consortium member institutions can host and organize public/private events minimizing the need for large (and costly) physical office spaces
- **Unparalleled expertise:** in-house staff and consortium members are leading experts in technology protection, research security, and risk assessments relating to China
- **Cost savings to taxpayer:** grant compliance and monitoring support to both government and academic clients can result in cost savings in terms of avoiding litigation or return of federal grant dollars to federal agencies; as a non-profit, CRSI can also contract with the government to perform select research and analytic services at a lower cost than most private firms
- **Innovator of open-source intelligence:** the R&D projects, data exploitation and analysis, and published materials will be foundational to supporting new initiatives on building open-source capabilities the US government lacks

CRSI will seek revenues through federal grants and/or Congressional appropriation, philanthropic sources, as well as contracts with academia, government agencies, and the private sector. Diversifying sources of revenue will be important to maintain long-term sustainability,

independence, and to engage with numerous stakeholders across public and private sectors. CRSI's mission areas could also be expanded to support allied nations as well, particularly nations that are integral to our defense supply chains.

It is worth noting that the final report issued by the National Security Commission on Artificial Intelligence (AI) made a similar recommendation. It urged Congress to authorize the sponsorship of a university affiliated research center (UARC) that would act as a center of excellence on research integrity and provide information and advice on research security. It stated this center should "bridge the gap between the government and academic and private-sector research institutions and lower the barriers for research organizations to independently conduct compliance and informed risk assessments." The recommended lines of effort of that proposed entity align with CRSI's.[40]

However, I believe CRSI is a better model than sponsoring a UARC. While UARCs have capabilities that can contribute to these efforts, they are run by individual universities. Other universities would be reluctant to share potentially sensitive information affecting their organization with an outside UARC. An independent entity is better suited to engender trust among different stakeholders. Additionally, no single UARC has all the necessary capabilities to be fully effective, hence CRSI's consortium model would offer a more comprehensive approach.

[40] "Final Report," *National Security Commission on Artificial Intelligence*, 2021, https://www .nscai .gov /wp -content /uploads /2021 /03 /Full -Report -Digital -1 .pdf.

Appendix: Tables and Figures

Table 1: Sampling of CETC-Owned Semiconductor or Microelectronics Firms

Company Name	Description, Affiliation with CETC
Nanjing Zhongdian Xingu High-frequency Device Industrial Technology Research Institute Co. Ltd. (南京中电芯谷高频器件产业技术研究院有限公司)	CETC's 55th Research Institute holds a 55% ownership stake. The firm engages in R&D of semiconductor high-frequency components; consulting, technology transfer, and technical services in the semiconductor domain; design of semiconductor materials, integrated circuits, electronic devices, modules and components.[41]
Guoqi Optoelectric Science and Technology (Tianjin) Co. Ltd (国麒光电科技(天津)有限公司)	CETC's 53rd Research Institute holds an 80% ownership stake. The company conducts R&D in and sells opto-electronic countermeasures and passive radar jamming equipment. The firm also develops AI products such as facial recognition systems, Internet of Things services, information systems integration, equipment communication systems and automatic controls, security monitoring systems, electronic components, and semiconductor materials[42]
Shanxi Shuoke New Materials Co. Ltd. (山西烁科新材料有限公司)	CETC's 2nd Research Institute owns 63.75%, CETC Investment Holding Co. Ltd. owns 13.36%, and CETC's 55th Research Institute owns 9.54% of the company's shares. The firm engages in R&D and production of semiconductor materials, electronics components, jewelry products, software development and sales, and import and export of goods and technologies.[43]
Hebei Poshing Electronics Technology Co. Ltd (河北普兴电子科技股份有限公司)	CETC's 13th Research Institute owns 72.3% of the company's shares. The firm specializes in R&D and production of high-performance semiconductor materials, including silicon-based epitaxial wafers, gallium nitride epitaxial wafers, and silicon carbide single crystals and epitaxial wafers. Industries it serves include clean energy, new energy vehicles, aerospace, computers, tablets, and smart phones.[44]
Shanghai Nanpre Mechanical Engineering Co. Ltd (上海微高精密机械工程有限公司)	A CETC subsidiary, CETC Electronics Equipment Group Co. Ltd., owns 70% of the company's shares. The firm was originally established by CETC 45th Research Institute's First Research Laboratory, which specialized in lithography and reportedly contributed to the development of equipment for military-use integrated circuits.[45] The firm develops core subsystems for lithography machines and also engages in used semiconductor equipment refurbishment, remanufacturing, technical services, and parts sales.[46]

[41] https://www.qcc.com/firm/763b04d5d6328aaaa7a54c3c07e572c9.html
[42] https://www.qcc.com/firm/6bce9a27be356b82b1fc96d575920dea.html
[43] https://www.qcc.com/firm/351373d70d41f57aa7c04ff9fe95eabe.html
[44] https://www.qcc.com/firm/0389ab78278aa1f4338e9f381a54c5d8.html; and https://web.archive.org/web/20181220023844/http://www.poshing.cn/.
[45] https://www.qcc.com/firm/ed2eb764eea00d19da38fca7b738efdc.html
[46] http://www.nanpre.com/a/guanyuwomen/

Figure 1: Chinese Academy of Sciences / Institute of Automation Research Areas

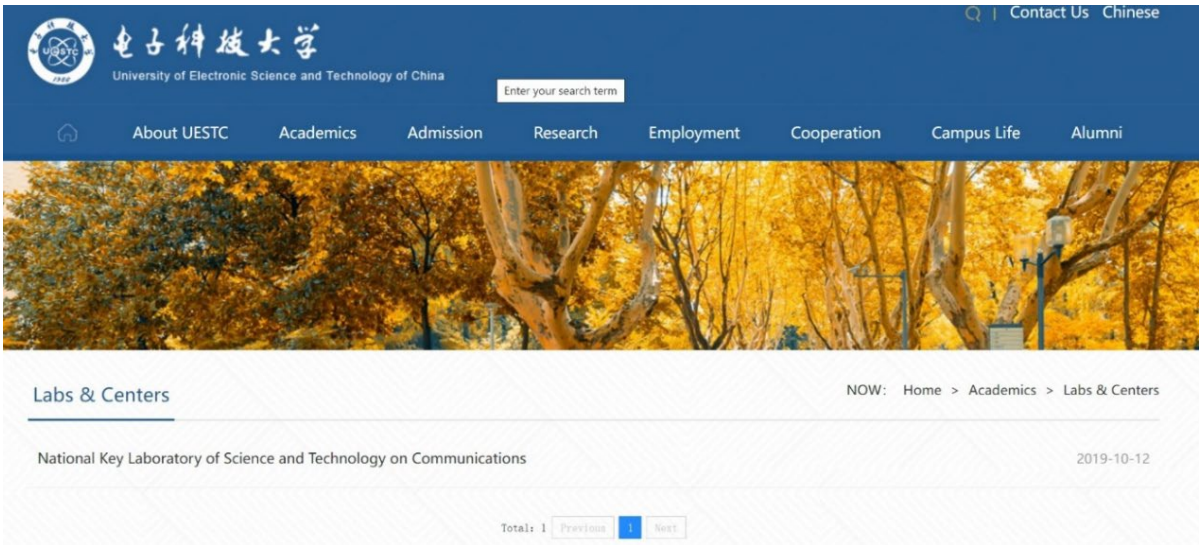
Beneficial or Benign Research Areas

- pattern recognition
- image processing
- speech and natural language processing
- neural computation
- cognitive brain modeling
- neuromorphic computing systems
- brain-inspired information processing
- brain mapping and function
- psychiatric disorders

Mass Surveillance Research Areas

- gait, iris, and facial recognition
- suspect targeting and tracking
- video / visual surveillance
- object recognition
- "abnormal behavior detection" for public security
- pedestrian monitoring

Figure 2: Screenshot of a University of Electronic Science and Technology of China (UESTC) English-Language Webpage



Screenshot of English-language webpage listing a single laboratory associated with UESTC

Figure 3: Screenshot of the Corresponding Chinese-Language Webpage of UESTC

Screenshot of the Chinese language webpage listing laboratories and centers at UESTC. The red arrow points to the official Chinese name of the one laboratory listed on the English webpage.

Table 2: Select Challenges and Impediments of the US Government

Government Element	***Impediments***
Intelligence Community	• A lack of sufficient language and subject matter expertise on China, particularly as it relates to the PRC's technology transfer apparatus • Restrictions on the collection and use of US Persons information limits access to data and impedes knowledge building and information sharing on threats to US research • The minimal use of and lack of reliance on publicly available information severely restrains the ability to collect, analyze, or share threat information related to research security
Law Enforcement	• Most threats to research security and integrity posed by China fall outside criminal activity and regulatory oversight, rendering most law enforcement efforts ineffective • Narratives of "IP theft, economic espionage, or academic espionage" used by federal agencies in public messaging fails in academic contexts • Inadequate resources in Offices of Inspectors General severely constrain their ability to investigate and mitigate abuse, undue foreign influence or interference in federally sponsored research
Other Agencies	• Program offices at federal agencies funding academic research lack capabilities to evaluate grant applicants for national security concerns • Few mechanisms are in place to monitor for national or economic security risks *post award* of an unclassified grant or contract