Testimony before the U.S. Senate Committee on Small Business & Entrepreneurship
on
"Innovation in the Crosshairs: Countering China's Industrial Espionage"

William C. Hannas
Research Professor and Lead Analyst
Center for Security and Emerging Technology, Georgetown University
July 23, 2025

Chair Ernst, Ranking Member Markey, distinguished members of the Committee and staff, I am grateful for the opportunity to testify on this topic.

I am a founding member of Georgetown University's Center for Security and Emerging Technology, where I track technology threats posed by China. Prior to that, I was a Senior Intelligence Service officer at CIA managing the same portfolio. These efforts led to two books on Chinese industrial espionage in 2013[1] and 2021[2] and to other studies on the topic.

My interest in Chinese foreign tech transfer began as a graduate student preparing a thesis on China's cultural predisposition for holistic thought, which has served China well in practical terms but hinders progress in basic science—and has plagued China since antiquity. I bring this up to emphasize that China's reliance on foreign ideas has historical roots not easily overcome.

Another factor that drew me to the topic was the discovery that China treats foreign technology acquisition as an academic discipline—科技情报学 or "S&T intelligence study"—on a par with other scientific fields, replete with degree programs, how-to manuals, academic journals, and career positions, supported by legislation and some 100,000 "S&T intelligence operatives."[3]

So, the notion that China's "informal" transfer of foreign technology is done by opportunistic individuals is pure myth. This is a state-backed, soup-to-nuts system that has been running at the central government's direction since the 1950s and is not abating, even as China's indigenous accomplishments grow.[4]

---

[1] William C. Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage*. (New York and London: Routledge, 2013).
[2] William C. Hannas and Didi Kirsten Tatlow, eds. *Beyond Espionage: China's Quest for Foreign Technology* (New York and London: Routledge, 2021).
[3] William C. Hannas and Huey-Meei Chang, "China's STI Operations: Monitoring Foreign Science and Technology through Open Sources," Center for Security and Emerging Technology, January 2021, https://cset.georgetown.edu/publication/chinas-sti-operations/.
[4] Ibid.

It's impossible to condense volumes of research into five minutes but here are the basics: China uses three types of transfer practices: legal, illegal, and extralegal—the last category so named because they occur without supervision and their legality is unknown.

Illegal transfers run from insider operations, patent infringement, and reverse engineering to the hacking and clandestine exploits we read about in the press. China tech espionage cases are so numerous that ODNI issues two annual reports: one on China, and one on the rest of the world. Noteworthy examples include next-generation battery technology, composites for jet engines, and self-driving technology.

Legal transfers done through China-based U.S. subsidiaries, start-up accelerators, targeted hires, direct and indirect investment, mergers and acquisitions, and tech-for-trade agreements are easy to spot but hard to counter because U.S. participants and oversight officials often confuse "legal" with "in the U.S. interest."

Finally, there are a dozen *categories* of "extralegal" venues that China uses, including front organizations for deniability, paid short-term visits to state debriefing centers, overseas technical support guilds, online recruiting and, of course, China's human talent recruitment programs.

In a 2023 book on artificial intelligence[5] we gave examples of U.S. tech firms in China, such as Microsoft, Intel, and IBM, working with China on AI development and credited by alumni of the programs as critical to China's success. In the same book, we named ten *types* of venues used to effect transfers from foreign academics, such as school-to-school "partnerships," co-authorship, and a practice called "using foreigners to draw in foreigners" (以洋引洋).

These practices threaten U.S. businesses large and small. The latter are especially vulnerable owing to a scarcity of research funds and investment capital, shrinking talent pools, fewer opportunities to commercialize breakthroughs, inadequate due diligence, and limited venues for redress. The impact on our proprietary technology, while not quantifiable, is obvious from the importance China attaches to this exploitative enterprise—acknowledged by Chinese scientists, policymakers, and business entrepreneurs.

So, what can be done? First, we must appreciate that the reason this is a problem at all is because our lead has shrunk to the point where theft matters, whereas before we were so far ahead it didn't matter. Rebuilding U.S. research, entrepreneurship and productive capacity—independently of whatever China is doing or stealing—is the only sure way out.

Meanwhile, we propose five commonsense measures.[6] They are:

---

[5] William C. Hannas and Huey-Meei Chang, eds., *Chinese Power and Artificial Intelligence*, (New York and London: Routledge, 2023).

[6] See William C. Hannas and Huey-Meei Chang, "Unwanted Foreign Transfers of U.S. Technology: Proposed Prevention Strategies." Center for Security and Emerging Technology, September 10, 2021, for a more complete list. https://cset.georgetown.edu/article/unwanted-foreign-transfers-of-u-s-technology-proposed-prevention-strategies/.

1. Data on China's transfer practices should be gathered and shared with U.S. firms and academic compliance offices. Persistent, dedicated efforts are needed to track China's activities as they evolve and change to evade the sunlight.

2. Clear guidelines on what is legally permissible should be communicated to foreign actors contemplating research in the United States, and to U.S. persons doing business in China.

3. Members of China's overseas support guilds, talent recruitment programs, lobbying groups, and other United Front operatives should register as foreign agents.

4. Recipients of U.S. government funding should report contacts with or travel to China to minimize China's ability to benefit from U.S. federal and state-level investment.

5. Finally, there are opportunities for U.S. authorities to stand China's transfer apparatus on its head by seeding these venues with persons disposed to support U.S. interests.

We are past the point where this problem can be ignored. The gap between tech breakthroughs and consequences is measured now in weeks, which puts a premium on keeping what we invent.

Thank you for the opportunity to address this important issue.

Wm. C. Hannas
Professor
Georgetown University