Statement before the House Permanent Select Committee on Intelligence

Testimony by:

Michael A. Brown

Presidential Innovation Fellow

July 19, 2018
U.S. Capitol Visitor Center, HVC-304

Thank you, Chairman Nunes, Ranking Member Schiff and Members of the Committee,

I'm pleased to be with you today to share findings of work I've led for the Defense Department in understanding the role that Chinese investments in early-stage technology firms have in China's systematic plan to transfer technology.

I came to this work as a former CEO of two Silicon Valley companies: Quantum, a computer storage provider where I worked for 20 years and Symantec, the cybersecurity firm where I was CEO through the fall of 2016. In the fall of 2016, I began serving as a Presidential Innovation Fellow working with the Defense Innovation Unit Experimental (DIUx) in Silicon Valley. However, I'm here today in my personal capacity as a Presidential Innovation Fellow and not as a spokesperson for the Defense Department.

In the fall of 2016, at the request of then Defense Secretary Ash Carter and Vice Chairman of the Joint Chiefs, General Paul Selva, I began researching along with Pavneet Singh *whether* and *how* China is transferring technology through investments in early-stage firms. Last year, we produced an unclassified report with our findings that we've shared widely within the U.S. government entitled *China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable a Strategic Competitor to Access the Crown Jewels of U.S. Innovation*. In summary, we learned that China's participation in venture deal financing was at a record level of *16% of* ***all*** venture deals financed in 2015 and remained at 10% in 2016 and 11% in the first ten months of 2017. This is concerning for six key reasons.

<u>Concerns with Chinese Investment in Early-Stage Companies</u>

First, the *growth* of these investments is up substantially from a level of 1-6% from 2010-2014. We identified more than 500 Chinese-based or affiliated entities investing in U.S. early stage companies in 2017.

Second, the technologies where Chinese firms are investing are the *same* as where U.S. venture capital firms are investing and will be foundational to future innovation such as artificial intelligence, autonomous vehicles, augmented/virtual reality, robotics, blockchain and genetic engineering. Moreover, since these technologies are dual-use--designed for commercial use but also equally important for military applications--these technologies will continue to be critical in advancing U.S. military capability.

Third, since venture investing depends on deal flow, investors see many more deals than they invest in. As a result, it's likely that Chinese investors, in aggregate, have seen *upwards of half* of recent U.S. venture financings; in other words, Chinese investors have a broad view of U.S.

innovation across a range of technologies. It's both logical and probable that China uses this broad view of U.S. innovation as a vantage point from which to target specific technologies including the underlying intellectual property (IP) and know how as well as the key talent that best understand the technology. Once targeted, China can then deploy one of ten different technology transfer mechanisms--both legal and illegal--to gain access.

Fourth, by investing in early-stage companies, Chinese investors are learning about these foundational technologies *at the same time and at the same rate* that the U.S. does--which precludes any time-based advantage for the U.S. with these technologies. Historically, the U.S. military has had exclusive use of critical technology for some period which could be called a period of overmatch; however, we are not likely to have overmatch in the future if China learns about leading-edge technology from U.S. startups at the same time as the U.S. military.

Fifth, without the proposed Foreign Investment Risk Review Modernization Act (FIRRMA) or CFIUS-reform legislation, there is no monitoring, reporting or control of investments in technologies important for national security by the U.S. government.

Sixth, the Defense Department, In-Q-Tel or other parts of the U.S. government will tend to avoid contact with an early-stage technology company that has a significant level of foreign ownership even if the company is developing technology important for national security. These are six reasons why the scale of Chinese investment in U.S. early-stage technology companies is concerning.

<u>Methods of China's Transfer of Technology</u>

What we found in the course of preparing the DIUx report is that Chinese venture investing is part of a larger story of technology transfer to China--ongoing for decades through both legal and illegal means. To be specific, some of the technology transfer mechanisms China engages in include industrial espionage, cyber theft, forced joint ventures in exchange for access to the Chinese market, tracking of open-source innovations, sponsoring professional organizations to target talent and using Chinese foreign national students by placing them in sensitive areas of U.S. research. Viewed individually, the legal practices may seem benign but when viewed in combination, and at the scale China is employing them, the composite picture illustrates the intent, design and dedication of a regime focused on technology transfer at a massive scale.

American Superconductor: Example of Industrial Espionage and Cyber Theft

Let me offer two specific examples. I'll start with American Superconductor where a Chinese firm employed both industrial espionage and cyber theft to steal an American company's technology. American Superconductor worked with a Chinese partner, Sinovel, to access the large China market for wind turbines. American Superconductor provided the control software or "brains" for wind turbines. Aware of the risk of IP theft, American Superconductor ensured its code was not available on the internet and kept engineering work on its code "air gapped" from connected networks on the internet. However, to gain access to this code, Sinovel turned an American Superconductor employee, Austrian Dejan Karabasevic who became an insider spy with a multi-year contract worth $1.7 million; women were also supplied to Mr. Karabasevic as a fringe benefit. Karabasevic stole the American Superconductor control software code and gave it to Sinovel. As a result, Sinovel no longer honored its contracts with American Superconductor and revenue plummeted from an annualized rate of $400 million to $36 million in just one quarter of 2011. Wall Street gave up American Superconductor for dead. According to the CEO of American Superconductor, Dan McGahn, "Participation in the Chinese market is for Chinese companies only. Your participation as a Western company...is a mirage. They're there to bring you in, be able to figure a way to harvest whatever they can from you, and then spit you out when you're no longer useful."[1]

As American Superconductor sued Sinovel in U.S. federal court and in China, Sinovel used cyber theft to better understand the American Superconductor legal strategy. Sinovel was found guilty of stealing trade secrets on January 24th of this year. It's a pyrrhic legal victory that took 5 years as the company lost $1 billion in shareholder equity value, laid off hundreds of employees, and lost its largest overseas market, now competing in a global market for wind turbines against its former customer using stolen technology.

Duke University: Example of Chinese Student Stealing Military-Sponsored Research

A second example illustrates the threats from Chinese foreign nationals working on cutting-edge research often paid for by the U.S. military at leading universities. In 2006, Professor David Smith at Duke University, an expert in metamaterials, developed a prototype "invisibility cloak" which could conceal objects from microwaves with potential applications for cell phones and antennas. Also that year, Ruopeng Liu, a Chinese student, joined Professor Smith's lab. Mr. Liu made the suggestion that the Duke lab should collaborate with a lab in China. China was willing to pay for the collaboration and Professor Smith saw this as a way for the technology to expand its use rapidly. Professor Smith's research sponsor was the U.S. Air Force Office of Science Research and the Pentagon was not pleased when it learned that the research had made its way to

[1] Jim Zarroli, "It Was a Company with a Lot of Promise. Then a Chinese Customer Stole its Technology" as heard on April 9, 2018 on *All Things Considered,* National Public Radio

China.

Mr. Liu published the Duke-developed research in China, taking credit for it, while mirroring the Duke lab that created it at the Southeast University in Nanjing, China. This research led to the founding of two well-funded companies in China: Kuang-Chi Science & Kuang-Chi Technologies which were initially funded by the Shenzhen and Guangdong provincial governments. Today, these two companies have market valuations of $3 and $7 billion, respectively, and use metamaterials to improve aviation, wireless internet and mobile payment solutions as well as disruptive space technologies.[2] China's People's Liberation Army (PLA) is a major customer.

Today, one-third of all foreign students in the U.S. are Chinese foreign nationals and 25% of our graduate STEM students are Chinese foreign nationals. Some have access to research funded by the U.S. military and work in our national laboratories despite efforts to ensure foreign nationals do not gain access to sensitive research. Enforcement of these restrictions varies at universities because, in general, the academic environment in the U.S. is very open to foster collaboration. We have the worst of both worlds with large numbers of Chinese foreign nationals benefiting from our world-class higher education system: we allocate a large proportion of our limited capacity to Chinese students and our immigration policy sends them back to China once they have graduated. In other words, rather than recruiting Chinese STEM graduates to stay and contribute to our economy as part of a world-class talent pool, they return home to support China's technological and economic growth.

Size of the Problem and Implications

Former Assistant Attorney General John Carlin said in 2016 that there are hundreds of cases where Chinese firms steal U.S. intellectual property.[3] In a study released a year ago, the Commission on the Theft of American Intellectual Property said the annual losses from IP theft range from about $225 to $600 billion.[4] The wide range indicates we do not have our arms around the problem except to say that we know the scale is massive.

Allowing China unlimited access to U.S.-developed leading-edge technologies not only speeds the decline of *our own* relative technological superiority but may even facilitate *China's* technological ascendance. While strategic competition with China is a long-term threat rather

[2] Neelesh Moorthy, "How One Graduate Student Allegedly Stole Duke Research to Create a Billion-Dollar Chinese Company," *The Chronicle,* October 29, 2017 and Daniel Golden, *Spy Schools: How the CIA, FBI and Foreign Intelligence Secretly Exploit America's Universities*. New York: Henry Holt and Company, 2017.
[3] Leslie Stahl, "The Great Brain Robbery," *60 Minutes,* January 17, 2016.
[4] IP Commission Report, March 8, 2018.

than a short-term crisis, preserving our technological edge is an important national issue today. In fact, the Defense Department is increasingly concerned about the risks today given that:

1. Chinese companies already own significant parts of the military supply chain,
2. Chinese companies already have significant designs of U.S. military equipment as a result of cyber theft and industrial espionage, and
3. China is targeting areas both to catch up to U.S. military capability such as in jet engine aircraft design and areas where China can gain a technology lead--especially where the U.S. military is developing technology with early-stage commercial companies such as in artificial intelligence and quantum computing.

The U.S. government does not have a holistic view--and by that, I mean a coordinated understanding amongst the economic and trade agencies and the purely national security agencies--of how fast this technology transfer is occurring, the level of Chinese investment in U.S. technology, or what technologies we should be protecting.

Actions to Take: Four Remedies

As a result, given the multiple means of technology transfer China employs today and the well-funded systematic approach the Chinese government oversees, the U.S. has not faced such a formidable strategic competitor with an expected trajectory to overtake our economy in size in our entire history. The U.S. needs a sense of urgency in developing four remedies:

1. Better defensive tools such as the CFIUS reforms included in the Foreign Risk Review Modernization Act (FIRRMA) of 2017 and expanded and updated export control reforms.
2. More aggressive enforcement of IP theft with the sanctions on Chinese firms that steal such as with ZTE, and changing our laws so that Chinese firms can be successfully sued in U.S. courts along with the ability to attach assets if they are found guilty
3. Increased investment in FBI Counterintelligence resources with a change of objectives to preventing IP theft rather than prosecuting cases
4. A long-term game plan to be successful in the technology race we now find ourselves in with China.

Need for Allied Coordination and Investment in Science & Technology

Let me conclude with two important points.

First, any of the steps we take to deter technology transfer from China--which include both CFIUS reform and changes to export controls--needs to be **coordinated with allies** to be effective. Otherwise, we create an incentive for talent and companies to move offshore. Additionally, we simply substitute one of our allies instead of the U.S. as the target for

technology transfer.

Second, while defensive measures like CFIUS reform and better export controls are important, they are not the key to winning a technology race with China. The more concerned we are about the national security threat that China represents, as Chairman of the Joint Chiefs of Staff Dunford indicated when he placed China as the #1 national security threat by 2025, the more important it is to **invest in science and technology, encourage Americans to pursue STEM education and increase federally funded R&D**. To enable the U.S. to win the last technology race with the Soviet Union, federally-funded R&D was 2% of GDP in the 1960s. As China invests a higher percentage of its GDP in R&D as its economy grows faster than ours, U.S. federally-funded R&D has declined today to 0.7% of GDP. We must be proactive to ensure we improve our technology base and innovation capability because our future economic security will be the principal determinant of our national security.

Thank you for your attention to this important issue and I look forward to answering your questions.