Silicon Valley | Boston

China's Technology Transfer Strategy:

How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation

Michael Brown and Pavneet Singh

February, 2017

Executive Summary

This report explores China's participation in venture deals[1] financing early-stage technology companies to assess: how large the overall investment is, whether it is growing, and what technologies are the focus of investment. **Chinese participation in venture-backed startups is at a record level of 7-10% of all venture deals done** and has grown quite rapidly in the past five years. The technologies China is investing in are the same ones that we expect will be foundational to future innovation in the U.S.: artificial intelligence, autonomous vehicles, augmented/virtual reality, robotics and blockchain technology. Moreover, these are some of the same technologies of interest to the US Defense Department to build on the technological superiority of the U.S. military today.

Because the U.S. economy is open, foreign investors, including those from China, are able to invest in the newest and most relevant technologies we are developing for the future and gain experience with those technologies at the same rate as the U.S. does. **The U.S. government does not currently monitor or restrict venture investing and the potential transfer of early-stage technology know-how**. The primary tool the government has to block or mitigate foreign investment is the Committee on Foreign Investment in the United States (CFIUS); however, since CFIUS reviews specific deals on a case-by-case basis (rather than systematic assessments of acquisitions or acquirers) and only deals that involve a controlling interest by foreign investors (usually mergers and acquisitions), CFIUS is only partially effective and allows concerning activity beyond its jurisdiction. The other principal tool to inhibit technology transfer is export controls. Export controls are effective at deterring exports of *products* to undesirable countries and can be used to prevent the loss of advanced *technologies* but controls were not designed to govern early-stage technologies or investment activity. Importantly, to be effective, export controls require collaboration with international allies, which is a long process where cooperation is not guaranteed.

This report surfaces some of the more concerning investment trends by Chinese entities in the U.S. early-stage technology ecosystem. There is further detail on the strengths and weaknesses of the U.S. government's existing tools and specific recommendations on how to stem the transfer of technology and technical know-how from this asset class. **For the Department of Defense, in particular, the report highlights a series of actions to take from developing a critical technologies list to restricting Chinese investments in technologies on that list, enhancing counterintelligence efforts and increasing investment to stimulate technology development through DARPA.**

However, while these findings are concerning, venture investing is only a small part of China's investment in the U.S.--which includes all forms of investment and investor types. Investing is itself only a piece of a larger story of massive technology transfer from the U.S. to China which has been ongoing for decades. This report places venture investing within the larger context of China's long-term, systematic effort to attain global leadership in many industries, partly by transferring leading edge technologies from around the world. Therefore, the recommendation **for the U.S. government is to expand the scope of CFIUS to include any commercial activity that could result in technology transfer such as venture investing *and* to restrict investments and acquisitions of U.S. companies that own technologies the DOD identifies as critical to national security.**

Importance to the Department of Defense (DoD)

U.S. military superiority since World War II has relied on both U.S. economic scale and technological superiority. U.S. technological pre-eminence enabled the series of offset strategies which included being first with nuclear weapons (the First Offset) and the electronics-enabled weapons of night vision, laser-guided bombs, stealth and jamming technologies as well as spaced-based military communications and navigation enabling the U.S. to dominate a battlefield (the Second Offset). Much of this technology came from research sponsored by the U.S. government

[1] A venture deal is a financing that provides startup or growth equity capital provided by private investors, usually venture capitalists.

and the Defense Department specifically. However, the technologies which will create the Third Offset are being developed by early-stage technology companies with large commercial markets. If we allow China access to these same technologies concurrently, then not only may we lose *our* technological superiority but we may even be facilitating *China's* technological superiority.

That China will grow to be an economy as large as ours may be inevitable; that we aid their mercantilist strategy through free trade and open investment in our technology sector is a choice. As a result, while this strategic competition with China is a long-term threat rather than a short-term crisis, preserving our technological superiority and economic capacity requires urgent action today.

Key Supporting Points:

- **China is executing a multi-decade plan to transfer technology to increase the size and value-add of its economy from its base as the world's 2nd largest economy. By 2050, China will be 150% the size of the U.S.[2] (with the goal of being double the US economy by that time and decrease U.S.' relevance globally)[3].**
- This technology transfer to China occurs in part through increasing levels of investment and acquisitions of U.S. companies which are at record levels today. **China participated in about 10% of all venture deals in 2015 up from a 5% average participation rate during 2010-2016.**
- **China is investing in the critical future technologies that will be foundational for future innovations across technology both for commercial and military applications: artificial intelligence, robotics, autonomous vehicles, augmented and virtual reality, financial technology and gene editing.** The line demarcating products designed for commercial vs. military purposes is blurring in these new technologies.
- **Investments are only one means of technology transfer which also occurs through the following licit and illicit vehicles** where the cost of stolen intellectual property has been estimated at $300 billion per year.[4]
    - Industrial espionage, where China is by far the most aggressive country operating in the U.S.
    - Cyber theft on a massive scale deploying hundreds of thousands of Chinese army professionals
    - Academia, since ¼ of STEM graduate students are Chinese foreign nationals
    - China's use of open source information cataloguing foreign innovation on a large scale
    - Chinese-based technology transfer organizations
    - U.S.-based associations sponsored by the Chinese government to recruit talent
    - Technical expertise on how to do deals learned from US firms
- **China's goals are to be #1 in global market share in key industries, to reduce reliance on foreign technology and to foster indigenous innovation.** Through published documents such as Five-Year Plans and Made in China 2025, **China's industrial policy and national focus on innovation are clear.**
- **There are clear examples of Chinese indigenous innovation** where China is doing much more than copying technology.
- **The U.S. does not have a comprehensive policy or the tools to address this massive technology transfer to China.** CFIUS is one of the only tools in place today to govern foreign investments, but it was not designed to protect sensitive technologies and is only partially effective.
- **The U.S. government does not have a holistic view of how fast this technology transfer is occurring, the level of Chinese investment in U.S. technology or what technologies we should be protecting.**
- DoD has several areas of risk resulting from the scale of China's investments and its technology transfer:
    - Supply chains for U.S. military equipment and services are increasingly owned by Chinese firms

---

[2] According to the Economist, the U.S. GDP will be $70 trillion by 2050 and China's GDP will be $105 trillion. "Long Term Macroeconomic Forecasts--Key Trends to 2050," *The Economist Intelligence Unit* (2015).

[3] The U.S. has not competed with an economic rival that could be larger than its own economy in 150 years. Michael Pillsbury. *The Hundred-Year Marathon.* (New York: St. Martin's Griffin, 2016)

[4] "The IP Commission Report: The Report on the Theft of American Intellectual Property," National Bureau of Asian Research (May, 2013). Retrieved at http://www.ipcommission.org

- China's targeted investments to close the gap in capabilities between its military and the U.S. in key areas such as jet engine design.
- Industrial espionage and cyber theft mean key defense designs and plans are in Chinese hands.
- There is no agreed upon list of technologies to protect for the future though an effort exists today to delineate technologies critical to current acquisition programs (JAPEC[5]).

The appropriate policy recommendations depend on assessments of the urgency and importance of the strategic threat that China poses:

- A minimalist action would be to develop the data collection and analysis capability to better assess what is happening. DoD should invest in developing the critical technologies list we need to protect for the future.
- Defensive actions to slow the technology transfer include restricting China's investment in and acquisition of technology companies by reforming CFIUS and modifying both export controls and student visas to be consistent with protecting agreed-upon critical technologies. More investment in counterintelligence and cyber protection would deter future intellectual property theft.
- To be fully effective the U.S. government-as-a-whole needs to change its policy to reflect that China has become a strategic competitor and engage the private sector and academia.
- Any of these defensive approaches should be accompanied by an investment program to proactively reinforce our strengths in technology development and innovation.

To respond to this strategic competitive threat requires reforming CFIUS as well as a long-term and consistent government-wide plan and, more likely, a national strategy to engage the private sector and academia to prevent the transfer of sensitive technology. Existing US policy and processes governing the acquisition of sensitive technology and facilities by potential adversaries do not regulate venture-based investment. Nor does the U.S. government have the capability to restrict foreign investment in specific *technologies* on national security grounds, such as artificial intelligence and semiconductors that are so foundational to future military advantage. Developing and implementing such a national strategy goes well beyond what DoD alone can do to slow this technology transfer. In this report, there are recommendations to respond to China's investments but there would need to be additional study to fully address the strategic threat that goes well beyond DoD's responsibilities.

China's Growing Investment in the U.S. & in U.S. Technology

China's Global and U.S. Investment

China's global foreign direct investment (FDI) level is growing rapidly and is at a record level in a range of $200-250 billion, with $213 billion in announced acquisitions in 2016.[6] [7] **China's FDI investment in the U.S. in 2016 was $45.6 billion and cumulative FDI in the U.S. since 2000 now exceeds $100 billion.**[8] China's investment stems from a variety of motivations. As China's economy has grown to the world's second largest, there is a commercial interest in expanding to other markets and this also provides some diversification for companies and individuals who would like to diversify their investments both geographically and from a currency standpoint. With the recent concerns about devaluation of the currency relative to the U.S. dollar, the Chinese have made more investments overseas and this has led to an increased level of capital controls.[9]

---

[5] Joint Acquisition Protection & Exploitation Cell, described on p. 14 of this paper.

[6] Lingling Wei, "China Issuing 'Strict Controls' on Overseas Investment," *Wall Street Journal* (November 26, 2016). Retrieved at http://www.wsj.com

[7] While China's global FDI has been growing at 33% annually since 2003, a leading China think tank expects global FDI to decline in 2017 to a level closer to 2015 and well below $200 billion. Lingling Wei, "China's Overseas Funding to Shrink," *Wall Street Journal* (January 14, 2017)

[8] Thilo Hanemann and Daniel Rosen, "Chinese Investment in the United States; Recent Trends and the Policy Agenda" *Rhodium Group Report* (December 9, 2016). Retrieved at http://www.rhg.com

[9] These capital controls and the slower growth rate of the Chinese economy are likely primary causes for the forecasted China global FDI to decline in 2017.

China's **U.S. Technology** Investment

China's total investment in U.S. technology (electronics, information & communications technology, biotech & energy) for the past decade 2006-2016 totaled about $35 billion and in 2016 was about $8.5B.[10] Since the U.S. is a global leader of technological innovation, it is logical that China would seek to make increasing investments in U.S. technology companies. While it is likely that China's investment in technology is driven in part by commercial interests, it is unlikely this is the sole reason given China's explicit technology goals. Investment is one of the means for China to accomplish its technology transfer goals.[11] Both these technology goals and China's multiple vehicles for technology transfer are described in later sections.

China's **U.S. Early-Stage Technology** Investment

Chinese investment activity in *early stage technology* deals is also growing rapidly and peaked in 2015 at 285 deals valued at $12 billion, **almost 10% of the value of all technology deals in that year ($137 billion)**.[12] This means that China invested on the order of $3-4 billion in early stage venture deals. The specific areas of technology where these investments occurred are covered in the next section.

These investments are consistent with China's goals made clear in President Xi Jinping's statements, successive Five Year Plans, Made in China 2025 and Project 863,[13] namely, to:

- Establish China as one of the *most innovative* countries by 2020 and a *leading* innovator by 2030[14]
- Become a leading global science and technology power by 2049--the 100th anniversary of the PRC
- **Double down on R&D of core information and communications (ICT) technologies...to develop technologies on its own, *acquiring expertise from abroad when indigenous development is not possible.***

The growing investments in U.S. technology overall and early-stage ventures in particular, comprise a part of China's plan to acquire expertise from abroad and to develop indigenous innovation.

China's Investment in Critical Future Technologies

Investments from mainland China-based[15] investors into early-stage U.S. technology companies continue to grow in all sectors and are dispersed across all the stages of the investment lifecycle.[16] Some notable investment data include:

- China-based investors participated in 1,002 financings in the U.S. from 2010 to 2016 contributing to roughly $30 billion in venture-backed funding. Over the same period, overall funding into early stage technology was roughly $620 billion, indicating that **Chinese investors participated in 5% of overall deal value during this period (2010-2016) growing to almost 10% in 2015.**

---

[10] China Investment Monitor, Rhodium Group, January 17, 2017; Retrieved at http://www.rhg.com

[11] "This strategy seems to be increasingly the norm in the tech industry, with Chinese companies making investments to soak up strategic technologies, capabilities, talent and brands that they can then take home." Ana Swanson, "Gold Rush: Chinese Tech Companies Invest Overseas," *CKGSB Knowledge* (April 20, 2015). Retrieved at http://knowledge.ckgsb.edu.cn/2015/04/20/finance-and-investment/gold-rush-chinese-tech-companies-invest-overseas/

[12] "The Rise of Chinese Investment in U.S. Tech Startups" *CB Insights Blog* (December 2, 2016). Retrieved at http://www.cbinsights.com

[13] Project 863 is shorthand for the month (3/March) and year (1986) when it was introduced by China's leading strategic weapons pioneers to Deng Xiaoping. The proposal was approved and served as China's leading industrial R&D program, importantly reforming decision making to be less stove-piped and more collaborative; reorienting the procurement process; investing in training of technical experts; and developing technologies of strategic value.

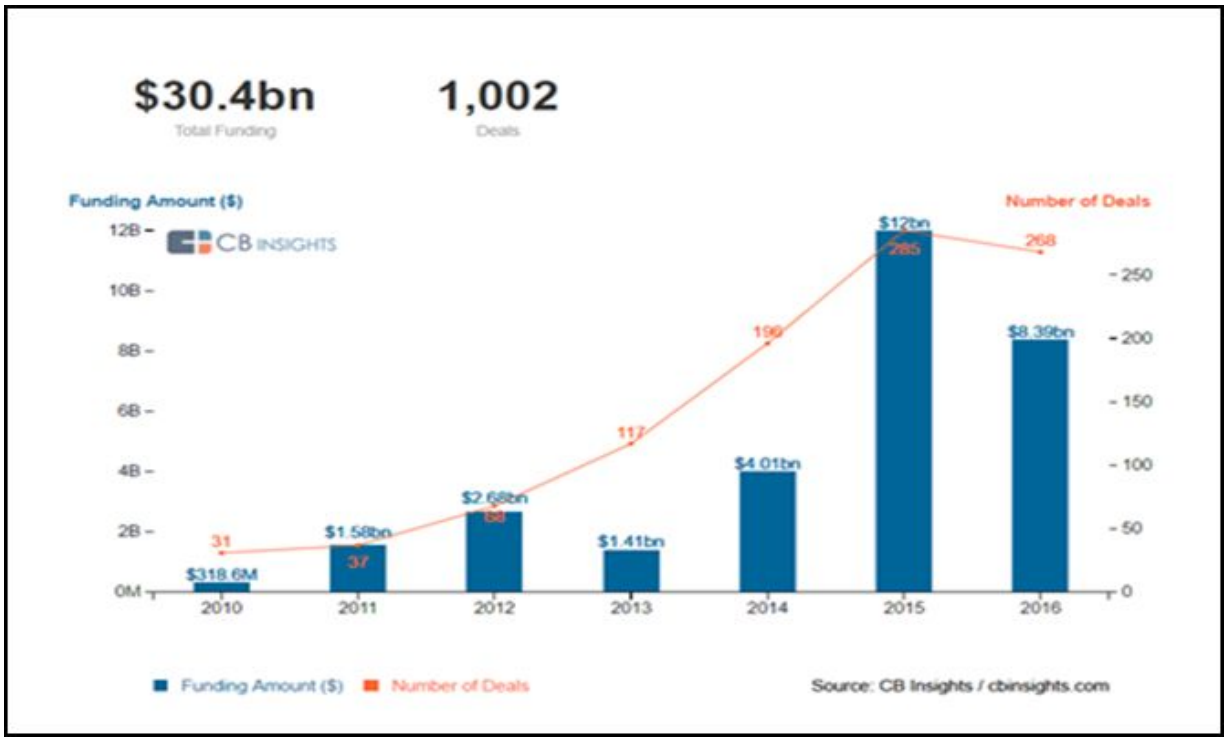
[14] "Xi Sets Targets for China's Science, Technology Progress" *Xinhua* (2016, May 30). Retrieved at http://www.xinhuanet.com

[15] For the purposes of this inquiry, China-based investors include investors from mainland China and Hong Kong.

[16] For the purposes of this study, we identified 439 unique investors from China that have invested in the United States from 2010 to 2016. These investors span from individual angel investors, Chinese entities serving as incubators or tech accelerators and traditional venture capital firms to corporations, banks, and hedge funds taking active stakes in early-stage companies The full list of Chinese investment vehicle types included in the CB Insights database include: Incubator/Accelerator; Venture Capital; Corporation; Corporate Venture; Private Equity; Asset/Investment Management; Holding Company; Angel Investor; Investment Bank; Sovereign Wealth Fund; Angel Investor (Group); Hedge Fund; Advisory; Government; Diversified Financial Services; Merchant Bank; Family Office; Debt & Specialty Finance; Business Plan Competition

- Activity from Chinese investors peaked in 2015 participating in 285 deals valued at $12 billion. In 2016, reflecting the broader decline in venture capital financings, Chinese investors participated in 7% of deals valued at $8.4 billion.[17]

Chart 1: Chinese Investment in U.S. Venture Capital Market, 2010 - 2016



Showing deals from Jan 01, 2010 - Dec 26, 2016

	Seed / Angel	Series A	Series B	Series C	Series D	Series E+
% of deals	32.47%	25.17%	16.70%	13.29%	6.23%	6.11%
Avg deal size	$1.55M	$12.5M	$28.6M	$42.4M	$55.5M	$185.7M

Table 1: Dispersion of Chinese Investment in U.S. Venture Capital Market, 2010 - 2016

- A majority of the investment occurred in the Seed/Angel stage (276 transactions and 33% of all deals), followed by Series A (214 transactions and 25% of all deals).[18] This corresponds with the recent increase in Chinese investment in early-stage technology deals and indicates that Chinese investors are interested in early looks at the most promising (even if yet unproven) technologies.

- By country, China invests more in early stage technology companies than any other country except the EU as a block. (Details on this comparison and a pie chart by country are in Appendix 1.)

[17] "The Rise of Chinese Investment in U.S. Tech Startups," *CB Insights Blog*.

[18] Seed/Angel stage is typically the first investment in an idea before the idea is proven and often attracts a different class of investors than those who might lead a later stage venture round (typically denoted by a letter such as "A", "B", etc.) leveraging a more proven idea or business model.

Investment in Critical Technologies

China-based investors are particularly active in the emerging technology sectors of Artificial Intelligence (AI), Augmented Reality/Virtual Reality, Robotics and Financial Technology. In 2016, Chinese investment in this portfolio of technologies represented approximately 16% of their overall investment.[19]

- ***Artificial Intelligence:*** During 2010-2016, Chinese investors participated in fifty-one AI financings, contributing to the roughly $700 million raised. Participation accelerated in 2015 and 2016, with Chinese investors participated in twenty-nine deals and $470 in financing.
- ***Robotics:*** Chinese investors contributed $253 million in financing in Robotics startups in 2010-2016. Deal activity peaked in 2016 with Chinese participation in fifteen deals and $80 million in financing.
- ***Augmented Reality/Virtual Reality (AR/VR):*** Chinese investors participated in $1.3 billion worth of deals during the period 2010-2016. In 2016, China-based investors participated in fifteen deals, contributing $1.06 billion in total funding value.
- ***Financial Technology (Fintech):*** Investments in Fintech, including blockchain technology, continued their rapid pace in 2016 with Chinese investors participating in twenty-one deals, valued approximately at $730 million. Overall, Chinese investors have participated in $2.8 billion in funding for Fintech companies during 2010-2016.

Two important trends stand out among the new wave of technology being funded. **First, the line demarcating products designed and used for commercial versus military purposes is blurring for these emerging technologies.** For example, VR for gaming is at a similar level of sophistication as the VR used in simulators for our armed forces.[20] Facial recognition and image detection for social networking and online shopping has real application in tracking terrorists or other threats to national security; and much of today's commercial autonomous vehicle technology and drone technology solutions find their genesis in DARPA grants over the last two decades when the Department of Defense sought to develop autonomy for war-fighting purposes.

The implication of this trend is that the current export control system, and policy apparatus for vetting foreign investment in the U.S., which are both designed to keep sensitive technology, companies, and infrastructure out of the hands of our adversaries, is built on a framework of being able to clearly distinguish the dual uses of a technology. This becomes a lot tougher when the technology itself is developed for commercial purposes and has widespread potential use as a fundamental technology building block such as artificial intelligence.[18] With the blurring of the line between civilian and military use, faster development cycles and the increasing mobility of human capital globally, our current export control system becomes even more problematic as a tool to manage how and where technology transfer occurs.

Second, these technologies–from artificial intelligence to robotics and virtual reality–will be foundational so that many applications or end-use technologies will be built upon them. These foundational technologies will be component technologies for future innovations much the same way that semiconductors have been components in all electronics, telecommunications and computing in the past several decades. This is especially true in the field of artificial intelligence, where the U.S. government is actively making investments to create the third wave of AI technology to achieve a future where machines can explain themselves to humans; where machines can create causal models, not just correlations; and where machines can take what they learn in one domain and apply the learnings to a completely different domain.[21] The breakthroughs that come with these new technologies will be the building

---

[19] Charts of the Chinese investment activity in these four critical technologies are in Appendix 1 and select deals for 2016 are provided in Appendix 2 which illustrates China's technology focus in venture investing.

[20] Major Loren Bymer, "Virtual Reality Used to Train Soldiers in New Training Simulator," *U.S. Army News & Information* (August 1, 2012). Retrieved at https://www.army.mil/article/84453

[21] Ed Felton and Terah Lyons, "The Administration's Report on the Future of Artificial Intelligence," *White House Blog*, October 12, 2016 Retrieved at: https://www.whitehouse.gov/blog/2016/10/12/administrations-report-future-artificial-intelligence

blocks for innovations in the decades ahead. There is likely to be an interaction between the new capabilities that are available (through innovations in robotics, artificial intelligence and virtual reality) and new generations of uses, applications and products. The same phenomenon occurred when faster microprocessors, more storage or higher networking bandwidth became available and led to future innovations such as cloud computing, mobile phones and consumer applications for GPS. Consequently, it becomes even more critical that exports, foreign ownership, and technology partnerships with foreign entities do not become conduits for technology transfers that will directly enable key means of foreign military advantage. What is at risk for the U.S. is not only losing an edge in the foundational technology, but also in successive generations of uses, applications and products that the foundational technology enables. According to Adam Siegel, a specialist in emerging technologies and national security at the Council on Foreign Relations, "The Chinese leadership is increasingly thinking about how to ensure they are competitive in the next wave of technologies."[22]

There are multiple ways Chinese invest in U.S. technology firms:

1. **Investments in U.S. venture-backed startups through venture firms.** In the past 10 years, China's investments in U.S. technology firms were limited to joint ventures or acquisitions, but now there are an increasing number of green field investments[23] in venture-backed startups (both as limited partners of U.S. venture firms and through Chinese venture firms) as well as investments through Chinese private equity firms. Examples of Chinese venture firms include West Summit Capital, Westlake Ventures (owned by the Hangzhou government), GGV Capital, GSR Ventures, ZGC Capital, Hax and Sinovation. Sinovation (formerly known as China's Innovation Works) provides a great example of an active Chinese venture firm investing in the U.S.: it was founded in 2009, manages three funds of $1.2 billion in total capital and has invested in almost 300 startups--including 25 in artificial intelligence. As evidence of its government sponsorship, Sinovation has received awards by China's Ministry of Science & Technology as well as the Municipal Science & Technology Committee of Beijing where the firm is headquartered. (An overview of Sinovation and Hax and their investments are profiled as case studies of Chinese venture capital firms in Appendix 3.) A sample listing of government-backed venture firms and their sources of capital are provided in Appendix 4.

2. **Investments by Chinese companies.** Increasingly, Chinese internet companies such as Baidu, Tencent, Alibaba and JD.com are aggressively investing in venture-backed technology deals. In 2015, these companies participated in 34 deals worth $3.4 billion, up from 7 deals in 2012 worth $355 million.[24] Tencent is by far the most active (with 2x the deals in 2015 than the others combined) having started earlier with its investing but Baidu and Alibaba are not far behind. Some Chinese internet companies are championing investments in specific technologies; Baidu, for example has a clear investment focus in artificial intelligence. The chart that follows shows the growth of investment from 2013 to 2016 from these Chinese internet companies.[25]

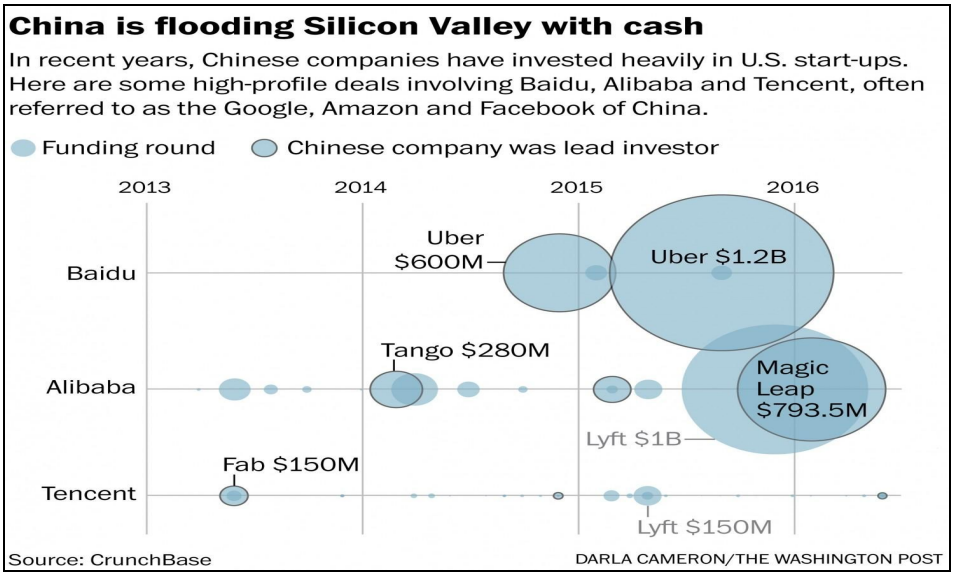
---

[22] John Markoff and Matthew Rosenberg, "China Gains on the U.S. in the Artificial Intelligence Arms Race," *The New York Times* (February 3, 2017). Retrieved at http://www.nytimes.com.

[23] Greenfield investments typically refer to new investments and sometimes a parent company's operations in a foreign country built from the ground up..

[24] "The Rise of China's Investment in U.S. Tech Startups," *CBInsights Blog*

[25] Elizabeth Dwoskin, "China Is Flooding Silicon Valley with Cash," *Washington Post* (August 6, 2016).



3. **Private equity (PE)**. Chinese private equity is expanding at an unprecedented pace with the number of globally active funds at 672 (2013-2015), the highest in 5 years. Total value of Chinese PE deals in 2016 (through June) is at a record $18 billion worldwide. This year Chinese PE firms participated in the $3.6 billion takeover of Lexmark, the $2.75 billion purchase of Dutch chipmaker NXP Semiconductors and the $600 million acquisition of Oslo-based Operat Software's web browser business.[26] Examples of Chinese private equity firms include AGIC, Legend Capital and Golden Brick Capital and these often partner with U.S. private equity firms, such as TPG (involved in acquiring a stake in China International Capital in 2012) and Carlyle (involved in purchase of Focus Media Holding in 2013). One of the most globally active China PE investors is Yunfeng Capital started by Alibaba Group founder Jack Ma.

4. **Special purpose vehicles**. There are also examples of special purpose investment vehicles like Canyon Bridge (an example of Chinese capital and U.S. management expertise combined) which are solely formed to purchase a company and obscure the source of capital for a foreign acquisition, in this case, Lattice Semiconductor. Presumably, a special purpose vehicle is formed to enhance the possibility that the transaction would be approved by CFIUS.

5. **Acquisitions**. Chinese acquisitions continue to increase dramatically with the largest globally being China National Chemical's proposed takeover of Syngenta (Swiss pesticides) for $43 billion. China's acquisitions of foreign companies are now equal to U.S.' acquisitions of foreign companies. In the U.S., the largest recent China-based acquisitions have been the electronics distributor, Ingram Micro ($6.1 billion) and the U.S. hotel owner, Strategic Hotels & Resorts--owners of the Waldorf-Astoria Hotel ($8.1 billion).

As long as U.S. policy supports open investment by all nations, we can expect increased investment from China through a broader number of vehicles, some cleverly designed to obfuscate Chinese capital and ownership. The investment activity *beyond acquisitions* is not tracked by the U.S. government and we have limited visibility into the investors, the technologies invested in, or the increase or decrease of investment flows, except through what is tracked by private data sources. However, even these private data sources are not comprehensively tracked by the U.S. government to assemble a holistic picture of what is happening.

[26] Cathy Chan, "Chinese Private Equity Funds Are Taking on the World's Giants", *Bloomberg News* (July 20, 2016)

China's Economic and Technology Goals

China has developed a leading global economy faster than any country in modern history. This transformation began with the reform and opening of China's economy under Deng Xiaoping in 1978. By 2015, China's GDP was $11.4 trillion compared to the U.S. at $18 trillion. However, in purchasing power parity (PPP), China is already slightly larger than the U.S. This represents the first time the US has not been the largest economy since it overtook the U.K. in 1872.[27] Since the US economy is growing at 1-3% and China's is growing at 5-7%, the trajectory is clear in narrowing the GDP gap (some projections show China's GDP exceeding ours within the next decade)[28]. The time scale during which this growth occurred is stunning as China's economy has grown from 10% of the US economy in the 1970s to the second largest global economy in just fifty years. Analogous growth in the U.S. economy to global leadership took a century to achieve.

From this point forward, China plans to further transform its economy through a national focus on technology and indigenous innovation with a goal to reduce U.S. relevance and be double the size of the U.S. economy by 2050.[29] To accomplish this, China aims to displace the U.S. in key industries using its large market size to promote domestic champions which can become global leaders through state subsidies, access to low-cost capital and limiting China's domestic market access to foreign companies. China already leads the world in many key industries including overall manufacturing (accounting for almost 25% of global manufacturing in 2012), autos, high-tech products, where China produced 2.5 times the value of goods that the U.S. produced in 2012,[30],[31] and e-commerce.[32] Beijing is home to the most Initial Public Offerings (IPOs) (2x the dollar value of the U.S.) and is the world's largest e-commerce retail market.[33] In fact, China has the potential to lead in all internet-based industries aided by discriminatory domestic policies such as data localization requirements, forced technology transfer and the Great Firewall. Chinese domestic champions such as Baidu, Tencent and Alibaba enjoy privileged market access in China and are market leaders domestically, while also becoming leading global technology companies.

China's leaders recognize that to achieve its economic goals, the economy must transform *even faster* in the future than in its recent past. The Chinese government wants to "revitalize the nation through science, technology and innovation."[34] President Xi's strategy is for China to develop its own industries to be leading globally, develop more cyber talent, double down on R&D especially of core ICT technologies and transform China to be a powerhouse of innovation. One area China has targeted for global leadership is the design and production of semiconductors. "China's strategy relies, in particular, on large-scale spending, including $150 billion in public and state-influenced private funds over a 10-year period aimed at subsidizing investment and acquisitions as well as purchasing technology."[35] Several official source documents clearly support these long-term economic and technology goals. (Summary descriptions of three documents are listed here with more documents and descriptions provided in Appendix 5.)

---

[27] Ben Carter, "Is China's Economy Really the Largest in the World?" *BBC News* (December 16, 2014)

[28] Malcolm Scott and Cedric Sam, "China and the U.S.: Tale of Two Giant Economies", *Bloomberg News* (May 12, 2016)

[29] Pillsbury, *The Hundred-Year Marathon.*

[30] High tech products in this case are defined by the World Bank as products with high R&D intensity such as aerospace, computers, pharmaceuticals, scientific instruments and electrical machinery

[31] Jeff Desjardins, "China vs. United States: A Tale of Two Economies," *Visual Capitalist* (October 15, 2015)

[32] By 2010, China already led the world in several commodity industries where the US previously led such as steel (with 8x our output), cotton, tobacco, beer, and coal.

[33] E-Marketer.com: "China Eclipses the U.S. to Become the World's Largest e-Commerce Market." Retrieved at https://www.emarketer.com/Article/China-Eclipses-US-Become-Worlds-Largest-Retail-Market/1014364 (August 18, 2016)

[34] "Xi Sets Targets for China's Science, Technology Mastery" *Xinhua* (May 30, 2016).

[35] "Ensuring Long Term U.S. Leadership in Semiconductors," Executive Office of the President, President's Council of Advisors on Science & Technology, January, 2017. Retrieved at http://www.whitehouse.gov/ostp/pcast

- **Made in China 2025** is a plan designed to align State and private efforts to establish China as the world's pre-eminent manufacturing power by 2049 emphasizing the integration of information technology. Key sectors prioritized include advanced information technology, automated machine tools and robotics, aerospace and aeronautical equipment, maritime equipment and high tech shipping, biopharma and advanced medical products, and new energy vehicles & equipment.[36]
- **13th Five Year Plan of 2016-2020 "Internet Plus"**[37] which deepens reforms and priorities called for in *Made in China 2025* and emphasizes stronger control by the government over national networks as China continues to control the internet domestically and gains access to global networks by controlling key component and telecommunications technologies. Key aspects include[38]:
    - Focus on catapulting China into a leading position in "advanced industries" including semiconductors, chip materials, robotics, aviation equipment and satellites;
    - Decreasing dependence on imports and innovation;
    - Increasing R&D spending to 2.5% of GDP (up from 2.1% from 2011-2015);
    - Creating a $4.4 billion fund to invest in startups and new technologies;
- **China's Mega Project Priorities** are 16 Manhattan-style projects[39] to focus on specific innovations. These are analogous to what is envisioned by Third Offset capabilities. In China these projects receive a *national* (not just a military) focus. Here are some selected examples (a complete list is in Appendix 6):
    - Core electronics, high-end general chips, basic software
    - Next generation broadband wireless mobile communications
    - Quantum communications
    - Classified defense-related projects (possibly satellite navigation and inertial confinement fusion)

Today, there are clear examples of Chinese indigenous innovation showing that China is doing much more than copying technology--making progress on President Xi's goal to become one of the most innovative economies by 2020:

- **Micius Quantum Computing Satellite.** The 2016 launch of the Micius Satellite suggests an aggressive push into quantum communications; expertise in quantum computing may someday enable the capability to break all existing encryption methods.
- **Sunway Taihu Light Supercomputer.** In June of 2016, China introduced the world's fastest supercomputer, the Sunway TaihuLight capable of theoretical peak performance of 124.5 petaflops. The TaihuLight is the first system in the world to exceed 100 petaflops (quadrillions of floating-point operations per second). More importantly, the previous version of this Chinese supercomputer used Intel microprocessors but the Sunway TaihuLight uses Chinese designed and manufactured microprocessors.[40]
- **Long Range Anti-Ship Missile (LRASM).** A cruise missile system with a high-level of artificial intelligence: a "semi-autonomous" weapon having the capability to avoid defenses and make final targeting decisions with a goal of destroying larger ships in a fleet like aircraft carriers.[41]
- **Consumer Drones.** JDI's (Dajiang Innovation) market leadership in low-cost, easy-to-fly drones and aerial photography systems which have made this company the standard in consumer drone technology accounting for 70% of the worldwide drone market.
- **Autos.** In the auto industry, China plans to take advantage of two paradigm shifts to further its lead in the

---

[36] Scott Kennedy, "Critical Questions: Made in China 2025," Center for Strategic and International Studies" November 7, 2016. Retrieved at http://www.csis.org/analysis/made-china-2025.

[37] "China Unveils Internet Plus Action Plan to Fuel Growth," The State Council for the People's Republic of China. *Xinhua* (July 4, 2015) Retrieved at http://www.english.gov.cn/policies

[38] Lulu Chang, "China Outlines its Latest FYP Called Internet Plus," Digital Trends (March 6, 2016). Retrieved at http://www.digitaltrends.com.

[39] Michael Raska, "Scientific Innovation and China's Military Modernization," *The Diplomat* (September 3, 2013), Retrieved at http://www.thediplomat.com

[40] Patrick Thibodeau, "China Builds World's Fastest Supercomputer without U.S. Chips," *Computerworld* (June 20, 2016), Retreived at http://www.computerworld.com

[41] John Markoff and Matthew Rosenberg, "China Gains on the U.S. in the Artificial Intelligence Arms Race," *The New York Times* (February 3, 2017).

world's largest manufacturing industry: autonomous vehicles and electric vehicles. China is investing in an electric vehicle supply chain including battery technology and aims to have 50% of the world's electric vehicle production and 90% of global battery production capacity.[42]

According to Tangent Link, a U.K.-based provider of defense reports, "one of the enduring myths in many Western CEO-suites is that the Chinese are great at copying and stealing, but will have difficulty 'out-inventing' the West. This arrogant and outdated hypothesis is crumbling fast."[43]

By some measures of innovation, China has taken the global lead but without question China's capacity to innovate is rising:

- In patent applications, China already surpasses the U.S. with over 1 million patent applications received by the China State Intellectual Property Office in 2015 (up 19% year over year) compared to 589,410 patent applications received by the U.S. Patent and Trademark Office (up 2% year over year).[44]
- In academic research papers, Chinese authorship of articles in peer-reviewed international science journals increased such that China is now in 2nd place (2011) up from 13th place just a few years earlier.[45]
- China spent 1.6% of GDP in R&D in 2011 but has a stated goal of spending 2.5% of GDP R&D by 2020--about $350 billion.[46] Combined U.S. business and federal government R&D spending is 3-4% of GDP.
- China awarded 1,288,999 Science, Technology, Engineering & Mathematics (STEM) degrees in 2014--more than double the degrees the U.S. awarded at 525,374 degrees.[47]

To assess the comparative innovation capability between China and the U.S., McKinsey recently analyzed the industries where China has an innovation lead and where it lags.[48] In traditional manufacturing industries where low costs provide a competitive advantage, China leads by leveraging a concentrated supply base and expertise in automation and modular design (examples: electronics, solar panels, construction equipment). In consumer markets, China leads given its market size (examples: smartphones, household appliances). In engineering markets, China has mixed results leading in high-speed rail but not in aerospace, nuclear power or medical equipment. In science-based industries such as branded pharmaceuticals or satellites, China is behind the U.S. but China is investing billions of dollars to catch up. (The McKinsey analysis is provided in Appendix 7.)

Many of the critical future technologies attracting venture focus today such as artificial intelligence, augmented reality and autonomous vehicles are likely to have large consumer-based markets implying that China will apply its advantages both in efficiency-driven and customer-focused industries to these new technologies with the potential to *lead in innovation and be global market share leaders.* The success of JDI in the consumer drone market with 70% worldwide share is consistent with this McKinsey analysis. In artificial intelligence, the race between the U.S. and China is so close that whether the Chinese "will quickly catch the U.S...is a matter of intense discussion and disagreement in the U.S. Andrew Ng, chief scientist at Baidu, said the U.S. may be too myopic and self-confident to understand the speed of the Chinese competition."[49] And in the field of advanced industrial robotics, China is leveraging its market and investment capital to ultimately lead in the design

---

[42] John Longhurst, "Car Wars: Beijing's Winning Plan" November, 2016.

[43] "Quantum Leap: Who Said China Couldn't Invent?" *Geo-political Standpoint (GPS) Report 85* (October 14, 2016), Tangent Link

[44] "China vs. U.S. Patent Trends: How Do the Giants Stack Up?", Technology & Patent Research. Retrieved at http://www.tprinternational.com

[45] Hannas, *China Industrial Espionage*, Chapter 3

[46] Hannas, *China Industrial Espionage*, Chapter 3 and "The U.S. Leads the World in R&D Spending", The Capital Group Companies (May 9, 2016). Retrieved at http://www.thecapitalideas.com

[47] Jackie Kraemer and Jennifer Craw, "Statistic of the Month: Engineering and Science Degree Attainment by Country", *National Center on Education and the Economy* (May 27, 2016). Retrieved at http://www.ncee.org

[48] Erik Roth, Jeongmin Seong, Jonathan Woetzel, "Gauging the Strength of Chinese Innovation," *McKinsey Quarterly* (October, 2015).

[49] John Markoff and Matthew Rosenberg, "China Gains on the U.S. in the Artificial Intelligence Arms Race." *The New York Time*s (February 3, 2017).

and manufacture of robots.[50] Given there are many industries where China already leads the world in innovation and given China's massive scale and national focus on science and technology advancement, it would be foolhardy to bet against China's continued progress even in the areas where they do not lead today.

Implications for the Department of Defense (DoD)

U.S. military superiority since World War II has relied on both U.S. economic scale and technological superiority. The size of the U.S. economy allows DoD to spend $600 billion per year (while remaining only 3% of GDP in 2016) which equals the defense spending of the next 8 largest nations combined. In 2016, China was the second largest spender at $215 billion, up 47% from the previous year while the U.S. spending remained flat.[51] U.S. technological preeminence enabled the series of offset strategies which included the First and Second Offsets and now DoD is currently working to maintain technology superiority in its Third Offset strategy.

China's goal to be the preeminent global economy combined with its emphasis on technology transfer and innovation constitutes a major strategic competition with the U.S. There are several areas of concern:

1. China's transformation to be the manufacturer for the world means more supply chains are owned by China, which creates risks to U.S. military technology and operations. For example, the Aviation Industry Corporation of China (AVIC) is a Chinese-state owned aerospace and defense company which has now procured key components of the U.S. military aircraft supply chain.[52] Additionally, as the U.S.-based semiconductor industry focuses on high-end designs and moves older, low-end designs offshore, the Chinese semiconductor industry now controls a significant percentage of the supply of older chips used in maintaining U.S. military aircraft and equipment designed 40 years ago and still in service.
2. China has targeted several key technologies such as jet engine design which will reduce current U.S. military superiority and is actively working to acquire companies that will close this gap.
3. China's industrial espionage and cyber theft efforts continue without adequate U.S. investment in manpower and programs to thwart these efforts. This allows technology transfer at an alarming rate.[53]
4. China's investment strategy (through venture and private equity investments as well as acquisitions) includes all of the fundamental technologies which will likely be the sources of innovation for the next several decades: artificial intelligence, autonomous vehicles, robotics, augmented and virtual reality, gene editing, etc. As a result, China has access to the U.S.-based innovation in the same areas and at the same time which could negate Third Offset advantages for the U.S. Further, when the Chinese make an investment in an early stage company developing advanced technology, there is an opportunity cost to the U.S. since that company is potentially off-limits for purposes of working with DoD.
5. Beyond the threat from investments alone, China's national focus on mega projects (analogous to the U.S. space program in the 1960s to not only develop technology but *create demand* for the technology) complements the increase in military spending as China gains experience in manufacturing and refining these new technologies for practical use.
6. The Defense Department does not currently have an agreed-upon list of critical technologies the U.S. must protect although there has been extensive work on export controls to protect technologies from being shipped to U.S. adversaries.

---

[50] Farhad Manjoo, "Make Robots Great Again," *The New York Times* (January 26, 2017).

[51] 2016 Fact Sheet, Stockholm International Peace Research Institute (SIPRI) and "The Military Balance", International Institute for Strategic Studies (IISS) 2016. Retrieved at http://www.en.m.wikipedia.org

[52] "How America's Giants Are Aiding China's Rise", *Geo-political Standpoint (GPS) Report 84*, October 13, 2016, Tangent Link.

[53] The IP Commission Report (2013)

DoD began developing a list of critical technologies in 2016 in an effort known as the Joint Acquisition Protection & Exploitation Cell (JAPEC). The mission of JAPEC is to "integrate protection efforts across the Department to proactively mitigate losses and exploit opportunities to deter and disrupt adversaries which threaten U.S. military advantage." JAPEC is working to identify critical acquisition programs and technologies that require protection as well as assess vulnerabilities associated with known losses and implement advanced protection mechanisms.[54] However, given the relative newness of this effort, there is much work left to do to consolidate the technologies across DoD requiring protection for current acquisition programs. The integration of the technologies critical to the Third Offset strategy is only beginning. The JAPEC effort complements the government's robust system of export controls which are designed to comply with trade agreements, embargoes, sanctions and other political measures to meet U.S. national security and foreign policy objectives.

Finally, there is no technology landscape map to help DoD understand the fundamental component technologies required to protect applications or end-use technologies embedded in acquisition programs. For example, semiconductor technology is a fundamental component technology today that would be required to protect capabilities inherent in almost all acquisition programs. This is likely to be the case in the future with such fundamental technologies as artificial intelligence, robotics, autonomous vehicles, advanced materials science, etc. With an agreed-upon list of critical technologies and a technology landscape to clarify the value-added map of technologies (from components to end-use applications), the U.S. government can be much clearer about what acquisitions to deny through a reformed CFIUS process, what foreign investments we should not allow and where to allocate resources to thwart industrial espionage or cyber theft.

China's Multiple Vehicles for Technology Transfer

Given the authoritarian nature of China's government, China is able to focus resources from a variety of different sources to enable a broad transfer of scientific knowledge and technology. Additionally, China coordinates these different sources to achieve a larger impact through a well-articulated industrial policy documented in its Five-Year and other plans. The principal vehicles discussed so far are investments in early-stage technologies as well as acquisitions. When viewed individually, some of these practices may seem commonplace and not unlike those employed by other countries. However, when viewed in combination, and with the resources China is applying, **the composite picture illustrates the intent, design and dedication of a regime focused on technology transfer at a massive scale.**

The following table compares these transfer vehicles on a relative scale of the level of activity for China in the U.S. compared to other countries. This illustrates that what differentiates China from other countries' activities in the U.S. is the *scale* of China's efforts. Naturally, the most troublesome of all the vehicles are the illegal ones--the outright theft of technology and intellectual property which is very cost-effective for China. In fact, China views borrowing, stealing and leveraging in efficiency terms rather than in moral terms.[55]

[54] Brian D. Hughes, "Protecting U.S. Military's Technical Advantage" presented at the 18th Annual NDIA Systems Engineering Conference in Springfield, VA, October 28, 2015. Retrieved at http://www.acq.osd.mil

[55] Hannas, *China Industrial Espionage*.

Vehicles for Chinese Technology Transfer from the U.S.

Legal		China-based research centers in U.S. China-based tech transfer orgs in U.S. Professional associations Leveraging U.S. deal expertise **Early-stage investments**	Foreign students sent to U.S. Open-source tracking of foreign innovation Requirement of JVs for U.S. companies doing business in China **Acquisitions**
Illegal			Cyber attacks Cyber theft Industrial Espionage
	Low Activity	**Medium Activity**	**High Activity**

China's Activity in the U.S. Relative to Other Countries' Activities in the U.S.

The 8 principal sources and methods for technology transfer *in addition to investments and acquisitions* are:

1. **Industrial espionage**

For years, the Chinese have been engaged in a sophisticated industrial espionage program targeting key technologies and intellectual property to enhance commercial enterprises and support domestic champions.[56] This has recently been on the rise as Randall Coleman, Assistant Director of the FBI's Counterintelligence Division observed in 2015 that espionage caseloads are up 53% in the past two years and that in an FBI survey of 165 companies, 95% of those companies cite China as the perpetrator. "China's intelligence services are as aggressive now as they've ever been" underscoring the pervasive nature of intellectual property and trade secret theft.[57] The FBI reports that China pays Chinese nationals to seek employment in targeted U.S. technology firms (where there is sensitive technology that China identifies it needs) to allow these "insiders" to more readily exfiltrate valuable intellectual property. Fortunately, convictions of Chinese nationals and naturalized citizens for industrial espionage are also on the rise, up 10X since 1985[58].

Despite the rise in convictions, there is no way to know how big this problem really is. The scale of the espionage (through some of the methods described below) continues to increase and it would be difficult to quantify this problem without more resources applied by both the FBI and the Defense Department's various counterintelligence agencies. The FBI Silicon Valley office, for example, only employs about 10 individuals in this work.

---

[56] *2016 Report to Congress of the US-China Economic & Security Review Commission* (November, 2016) and Hannas, *China Industrial Espionage*, Chapter 8

[57] Shanie Harris, "FBI Probes 'Hundreds' of China Spy Cases", *The Daily Beast* (July 23, 2015). Retrieved at http://www.thedailybeast.com

[58] Notes from briefing, "Economic and S&T Intelligence Collection" by Joseph P. O'Neill, Faculty Member, National Intelligence University, November 28, 2016.

2. Cyber theft

China's cyber capabilities are among the strongest in the world probably only exceeded by Russia and the U.S. although some have argued that China's cyber successes to date demonstrate more about U.S. system vulnerability than Chinese capabilities. Regardless, cyber theft is an ideal tool for China given this asymmetric vulnerability of the U.S. (given how much information is digitally accessible) and the plausible deniability given the difficulty of attribution in cyber attacks. Several documented high profile cyber theft incidents are described in Appendix 8 and may be the tip of the iceberg in terms of the numbers of incidents and their scale. As former NSA Director General Keith Alexander famously told Congress in 2012, this represents the "greatest transfer of wealth in history". At that time, it was estimated that U.S. companies lose $250 billion per year through intellectual property theft and another $114 billion due to cybercrime, totaling $338 billion of impact each year. "That's our future disappearing in front of us," warned General Alexander.[59]

As reported in the IP Commission Report of 2013, Verizon worked with 18 private institutions and government agencies to estimate that:

- 96% of the world's cyber espionage originated in China
- $100 billion in lost sales and 2.1 million in lost jobs result from this theft
- $300 billion worth of intellectual property is stolen *each* year[60]

What really distinguishes China from other nation-state actors in cyber attacks is the sheer scale of activity as China dedicates a massive amount of manpower to its global cyber activities. The FBI's former deputy director for counterintelligence reported in 2010 that the China deploys between 250,000 and 300,000 soldiers in the People's Liberation Army (3PLA) dedicated to cyber espionage. Within another part of the armed forces, 2PLA has between 30,000 and 50,000 human spies working on insider operations.[61] China's cyber activity is not solely focused on a national security agenda. In fact, much of this activity can be deployed to support China's *economic* goals in stealing valuable intellectual property to support China's technology transfer. Additionally, China recently passed two laws--the anti-terrorism law and the cybersecurity law--which are of concern since they could be used to gather sensitive commercial information from U.S. companies legally.[62]

3. **Academia**

For many years, China has sent an increasing number of students to the U.S. In 2016, there were 328,000 Chinese foreign nationals studying at U.S. colleges and universities (⅓ of all foreign students). Chinese foreign nationals represent ½ of all foreign applicants.[63] The U.S. educational system has come to rely on the financial contribution of these foreign students.

---

[59] Josh Rogin, "NSA Chief: Cybercrime Constitutes the 'Greatest Transfer of Wealth in History' " *Foreign Policy Magazine* (July, 2012). Retrieved at http://www.foreignpolicy.com

[60] The IP Commission Report (2013)

[61] Joshua Philipp, "Rash of China Spy Cases Shows a Silent National Emergency", *The Epoch Times* (April 25, 2016). Retrieved at http://www.theepochtimes.com

[62] **Anti-terrorism law** passed in December, 2015 which gives the Chinese government broad access to technical information and decryption codes when state security agents demand it for investigating or preventing terrorism. Telecommunication and internet service providers "shall provide technical interfaces, decryption and other technical support and assistance" when required. Chris Buckley, "China Passes Antiterrorism Law that Critics Fear May Overreach," *The New York Times* (January 6, 2016). Retrieved at http://www.nytimes.com.

Cybersecurity law passed in November, 2016 contains vague language aimed at preventing network intrusions that would require U.S. companies submit their technology, possibly including source code, to security reviews with Chinese officials. There are an expansive list of sectors defined as part of China's critical information infrastructure such as telecommunications, energy, transportation, information services and finance all of which would be subject to security reviews. The law does not specify what a security review will entail. Several U.S. companies are concerned about the increased costs of doing business in China as well as the need to provide company sensitive information to the Cybersecurity Administration of China to prove that their equipment, software and operations are safe. Josh Chin and Eva Dou, "China's New Cybersecurity Law Rattles Foreign Tech Firms," *Wall Street Journal* (November 7, 2016). Retrieved at http://www.wsj.com.

[63] Project Atlas, *Institute of International Education*, Fall 2015. Retrieved at http://www.iee.org.

Statistics on U.S. STEM programs highlight the large proportion of foreign students:

- 84% of foreign students in PhD programs were studying in science & engineering (2001-2011)[64]
- For doctoral programs, 57% of engineering, 53% of computer science and 50% of math and statistics candidates were foreign; half of these are Chinese[65]
- 54% of patents issued by universities include foreign student's work[66]
- 45% of STEM undergraduates are foreign and ⅓ of these are from China[67]

From this data, we can infer that **25% of the graduate students in STEM fields are Chinese foreign nationals**. Since these graduates do not have visas to remain in the U.S., nearly all will take their knowledge and skills back to China. Academia is an opportune environment for learning about science and technology since the cultural values of U.S. educational institutions reflect an open and free exchange of ideas. As a result, Chinese science and engineering students frequently master technologies that later become critical to key military systems, amounting over time to unintentional violations of U.S. export control laws. The phenomena of graduate student research increasingly having national security implications will inevitably increase as the distinction between military and civilian technology blurs. Further, since there are close ties between academia and U.S. government-sponsored research--including at our national laboratories--ensuring that foreign nationals are not working on sensitive research paid for by the U.S. government (including DoD) will become increasingly important.

Chinese companies are also approaching U.S. academic institutions to promote joint research and attract future talent. As an example, Huawei has partnered with UC-Berkeley to focus jointly on artificial intelligence research. Huawei made an initial commitment of $1 million in funding to cover areas such as deep learning, reinforcement learning, machine learning, natural language processing and computer vision.[68] More recently, Huawei has approached MIT with an offer for a grant to build a joint research facility.

4. China's use of open sources tracking foreign innovation

China has made collecting and distributing science and technology information a national priority for decades. "By 1985, there were 412 major science & technology intelligence institutes nationwide [in China]...employing ...60,000 workers...investigating, collecting, analyzing, synthesizing, repackaging, benchmarking and reverse engineering."[69] In 1991, the book, *Sources and Methods of Obtaining National Defense Science & Technology Intelligence*, detailed a comprehensive account of China's foreign military open-source collection (known as "China's Spy Guide") collecting all types of media (including verbal information prized for its timeliness over written information) and making them available in database form. The National Internet-based Science & Technology Information Service Systems (NISS) makes 26 million holdings of foreign journals, patents and reports available to the public around the clock. Chinese exploitation of foreign open-source science and technology information is a systematic and scale operation making maximum use of diversified sources: scanning technical literature, analyzing patents, reverse engineering product samples and capturing conversations at scientific meetings. This circumvents the cost and risk of indigenous research.[70]

---

64 "Survey of Graduate Students and Postdoctorates in Science & Engineering", *National Science Foundation,* November, 2015.

65 Drew Desilver, "Growth from Asia Drives Surge in US Foreign Students," *Pew Research Center* (June 18, 2015)

66 National Science Foundation Survey, November, 2015

67 Donisha Adams and Rachel Bernstein, Science (November 21, 2014); Retrieved at http://www.sciencemag.org

68 Li Yuan, "Chinese Technology Companies, including Baidu, Invest Heavily in AI Efforts", *Bloomberg News* (August 24, 2016)

69 Hannas, *China Industrial Espionage*, Chapter 2, p. 22.

70 Hannas, *China Industrial Espionage*, Chapter 2

5. Chinese-based technology transfer organizations

At the national level, China has more than a dozen organizations that seek to access foreign technologies and the scientists who develop them (not counting the clandestine services, open-sources, and procurement offices). These organizations are led by the State Administration of Foreign Experts Affairs (SAFEA). SAFEA's success is evident in the 440,000 foreign experts working in China annually. Complementing SAFEA is the State Council's Overseas Chinese Affairs Office (OCAO) which provides overseas Chinese (whether they have lived in China or not) with the opportunity to support their ancestral country. The Ministry of Personnel (MOP) is involved heavily in foreign recruitment and foreign technology transfer including the Overseas Scholars and Experts Service Center to interact with Chinese students studying abroad. The Ministry of Science & Technology (MOST) also dedicates significant resources to acquiring foreign technology including 135 declared personnel in overseas embassies and consulates.

The Overseas Scholars and Experts Service Center sponsors associations at many universities which serve as an organized means to transfer technology to China. Many of the national programs also have complementary provincial and municipal organizations specifically focused on the skills and talent than can benefit a local area. These organizations make available debriefing rooms, free translators, personnel to make travel arrangements, dedicated "transfer centers" and face-to-face meetings between technology experts and Chinese company representatives.

China also promotes "people to people" exchanges through a network of NGOs (e.g., the China Science and Technology Exchange Center and the China Association for the International Exchange of Personnel) that insulate overseas specialists from the potential risks of sharing technology directly with PRC government officials.[71]

6. Chinese research centers in the U.S. to access talent and knowledge

There are now increasing examples of Chinese firms setting up research centers to access U.S. talent and technology:

- In 2013, **Baidu** set up the Institute for Deep Learning in Silicon Valley to compete with Google, Apple, Facebook and others for talent in the artificial intelligence field.[72] Baidu recently hired former Microsoft executive Qi Lu as its group president and chief operating officer. Lu was the architect of Microsoft's strategy for artificial intelligence and bots.
- Another example is the **Zhong Guan Cun (ZGC) Innovation Center** opened in May, 2016 in Silicon Valley.
- Another type of research center is **TechCode** which is an entrepreneurs' network "committed to breaking down geographic barriers and eliminating potential inequalities of international cooperation" according to its website. As a network of entrepreneurs, Tech Code is a system of incubators ("startups without borders") worldwide (Beijing, Shanghai, Shenzhen, Gu'an, Silicon Valley, Seoul, Tel Aviv and Berlin) that leverages an online development platform for projects focused on China's development and funded by the Chinese government.[73]
- In addition, there are a number of research centers promoting a sustainable environment and clean energy including the **U.S.-China Clean Energy Research Center (CERC)** recently expanded and promoted together by President Obama and President Xi.

7. U.S.-based associations sponsored by the Chinese government

There are many professional and scholar associations which bring Chinese engineers together such as the Silicon Valley Chinese Engineers (6000 members), the Hua Yuan Science & Technology Association (HYSTA) and the Chinese Association for Science and Technology (CAST). The largest concentration of China's science and technology advocacy groups in the U.S. are in California and Silicon Valley in particular. "'The Valley' is ground

---

[71] Hannas, *China Industrial Espionage*, Chapter 4

[72] Li Yuan, "China Races to Tap Artificial Intelligence", *Wall Street Journal* (August 24, 2016)

[73] "Startups Nation" from the Tech Code website, http://www.techcode.com

[zero] for… legal, illegal and quasi-legal practices that fall just below the thresholds set by U.S. law."[74]

With these professional and scholar associations being the target, the Chinese have implemented a variety of programs such as the "Thousand Talents Program" to bring this technology home by recruiting Chinese engineers with offers of career advancement, increased compensation, the opportunity do basic research or to lead their own development labs in China. China set a goal of bringing back 500,000 Chinese overseas students and scholars from abroad by 2015.[75] Another example is "Spring Light" which pays overseas Chinese scientists and engineers to return home for short periods of lucrative service that may include teaching, academic exchanges, or working in government-sponsored labs. In addition, "Spring Light" includes a global database of Chinese scholars to match specific technology needs to pools of overseas talent.[76]

The Chinese diplomatic missions to the U.S. directly support technology transfer as embassy or consulate officials facilitate a wide variety of venues and forums supported by U.S. investors and local governments to promote Chinese investment. Seven examples of these are (descriptions of these forums are in Appendix 9):

- Silicon Valley Innovation and Entrepreneurship Forum (SVIEF)
- DEMO China
- Silicon Valley-China Future Forum
- China Silicon Valley
- The Global Chamber San Francisco (GCSF)
- U.S.-China VC Summit & Startup Expo
- Chinese American Semiconductor Professionals Association (CASPA)

The messaging for these associations and programs is often controlled by the "United Front" which is a propaganda arm for the Chinese government to promote a positive image of China and Chinese culture around the world.[77]

8. Leveraging technical expertise of U.S. private equity, venture firms, investment banks and law firms

As China has done more investing, its expertise has been enhanced by working with U.S. investment banks or law firms who benefit from increased business. As China works with U.S. private equity and venture firms to invest in deals, these firms benefit through the increased value of equity stakes in these investments. Many U.S. law firms have built a practice in advising Chinese companies on how to structure deals to increase the likelihood of CFIUS approval for transactions. Consulting organizations have also built a practice in structuring mitigation agreements that will be more likely to gain CFIUS approval. As China's investments have ramped up dramatically in the past 3 years, the level of deal expertise has increased considerably.

How are these multiple vehicles used together for coordinated impact?

Because the Chinese Communist Party is much more involved in planning economic activity and supporting companies (not only through state-owned-enterprises but also in favoring national champions it supports globally like Huawei), there is a great deal more coordination of investment along with other vehicles of technology transfer to accomplish the larger economic goals specified in China's documented plans. The scale of the Chinese economy is so large that not everything is coordinated centrally. However, the importance and degree of political control by

---

[74] Hannas, *China Industrial Espionage*, Chapter 5, p. 122

[75] Xu Liyan and Qiu Jing, "Beyond Factory Floor: China's Plan to Nurture Talent," Yale Global Online (September 10, 2012). Retrieved at http://yaleglobal.yale.edu/content/beyond-factory-floor-chinas-plan-nurture-talent

[76] Hannas, *China Industrial Espionage*, Chapter 5.

[77] The Confucius Institutes, launched in 2004, are a good example which offer Chinese language and cultural instruction often in partnership with local universities. However, their purpose is also to portray Chinese history and policy in the best possible light so that China can be seen as a "pacifistic, happy nation. In the past decade, these institutes have been welcomed on some 350 college campuses across the world including Stanford, Columbia and Penn." Pillsbury, *The Hundred-Year Marathon*.

the Communist Party ensures that investments support national goals and are not purely guided by commercial interest. The goals of many of the government-funded Chinese venture capital firms are focused on experience with advanced technologies and recruiting talent--not simply making money.

There are not enough examples to definitively say there is a standard playbook of all the vehicles used in combination. However, there are a few examples where several of these technology transfer vehicles are used together. Documented examples are targeted cyber attacks to understand the scope of technology and intellectual property of value and where that resides within a company followed by cyber theft or industrial espionage to steal that technology.[78] In another example, Chinese cyber attackers manipulated company sales figures to weaken that company's view of itself and make it more likely to accept a purchase offer from a Chinese company. In a variation on this theme, a Chinese customer placed large orders with a public company and then cancelled it to weaken a company's results as a market surprise. Finally, there is the example of Silicon Valley startup, Quixey, who relied on a large investor, Alibaba, as one of its most important customers promising access to the Chinese market. However, Alibaba refused to pay Quixey for a custom contract to provide specialized technology to search within apps in Alibaba's operating system. Alibaba subsequently took advantage of Quixey's cash squeeze to negotiate favorable financing terms which puts Alibaba in a better position to later make an offer for the technology or the company.[79] Thus, through a combination of these technology transfer vehicles, China can achieve more than it can with a single vehicle.

Before the U.S.-China Economic and Security Review Commission, a former forensic auditor and counterintelligence analyst testified that China is executing a series of campaigns targeting specific industries he studied including telecommunications & network equipment (to benefit global champions Huawei and ZTE), information security, semiconductors, media & entertainment and financial technology. He outlined a process that involves many of the vehicles described here as key technologies are targeted, studied, stolen and applied within Chinese companies. He characterized these as cyber-economic campaigns which "are persistent, intense, patiently executed and include the simultaneous execution of such a large and diverse set of legal and illegal methods, individuals and organizations, there's little chance the targeted U.S. competitors can effectively defend or compete in the future without significant support of the U.S. government." [80]

U.S. Government Tools to Thwart Technology Transfer

(1) The Committee on Foreign Investment in the U.S. (CFIUS) is one of the only tools in place today to govern foreign investments that could be used to transfer sensitive technology to adversaries, but it was not designed for this purpose and is only partially effective.[81] CFIUS was established by statute in the Foreign Investment and National Security Act of 2007 (FINSA) which formally gave an interagency working group the power to review national security implications of foreign investments in U.S. companies or operations. The Treasury Department is the lead agency among 14 participating agencies. The nine voting member agencies are Treasury, State, Commerce, the United States Trade Representative, Office of Science & Technology Policy, Defense, Homeland Security, Justice and Energy. While transaction reporting is voluntary, CFIUS can and does monitor transactions beyond those that are voluntarily submitted and can initiate a review of any of these. CFIUS is required to provide clearance for reviewed transactions on a short timeline: within 75 days unless a Presidential review is required and in that case, there are 90

---

[78] "APT1: Exposing One of China's Cyber Espionage Units", *Mandiant Report*, 2013. Retrieved at http://www.fireeye.com/content/dam/fireeye-www.services/pdfs

[79] Elizabeth Dwoskin, "China Is Flooding Silicon Valley with Cash," *Washington Post* (August 6, 2016).

[80] Jeffrey Z. Johnson, President & CEO of SquirrelWerkz, in testimony before the US-China Economic and Security Review Commission, January 26, 2017.

[81] CFIUS was established by executive order in 1975 during the OPEC oil embargo of the 1970s to prevent oil-rich nations with greatly expanding wealth from gaining too much control of U.S. assets.

days for a review and a Presidential recommendation.

As those involved in the CFIUS process readily acknowledge, CFIUS is a blunt tool *not* designed for the purpose of slowing technology transfer. **CFIUS only reviews *some* of the relevant transactions because transactions that do not result in a foreign controlling interest are beyond its jurisdiction.** There are many transaction types such as joint ventures, minority investments and purchased assets from bankruptcies that are effective for transferring technology but do not result in foreign control of a U.S. entity and are, therefore, outside of CFIUS' jurisdiction.

The workload for CFIUS is increasing rapidly. CFIUS reviews about 150 transactions per year but this is on the rise. At the same time, the number of transactions which have national security implications is also rising as Chinese purchases of U.S.-based companies or assets now represent the largest number of CFIUS reviews. Congress has not provided dedicated funding for CFIUS reviews which means that this critical process must be handled within existing agency budgets. A review of the strengths and weaknesses of the current CFIUS process are included as Appendix 11.

(2) Export controls are designed to prevent sensitive technologies or products from being shipped to adversaries.[82] In practice, there are several problems that may result from using export controls to thwart technology transfer to an adversary. First, export controls are often backward-looking in terms of specifying the technologies that are critical since most controls focus on products rather than broad technologies. Second, there is diffused responsibility for export controls since some are controlled by the State Department and some by the Commerce Department with DoD in an advisory role.[83] Third, with the technologies that are the focus of venture investing (far in advance of any specific products produced or military weapons), export controls have not been traditionally effective. From the U.S. government's perspective, this has largely been a function of having the foresight to place these technologies on an export control list and the political will to do so. In other words, the authority is in place for effective export controls if there is agreement among DoD, State and Commerce about what technologies to protect. From the private sector's perspective, since understanding and complying with export controls is a company's responsibility there is a question of whether early-stage technology companies understand the controls and have the resources within a trade compliance function to handle this complexity.

While the restricted export lists (EAR and CCL[76]) can accommodate the regulation of software-based technologies such as artificial intelligence, controlling a broad technology will be highly controversial within the venture and technology community where the largest markets are for benign, commercial purposes. In fact, there is great pressure to specify technologies as narrowly as possible when writing export controls to facilitate more U.S. exports especially if the technologies are available outside the U.S.. As the venture investment data indicates, the regulations do not prevent (or even deter) foreign investment in seed or early-stage companies. Additionally, it is not the purview of the export control enforcement authorities to proactively seek out companies developing new

---

[82] The current U.S. export control system is based on the requirements of the Export Administration Act, the International Economic Powers Enhancement Act (IEEPA), the Arms Export Control Act (AECA) and the resulting implementing regulations (most notably, Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR)). The EAR and ITAR each have a control list: the Commerce Control List (CCL) and the US Munitions List (USML). Several other Federal Agencies have niche export control regulations such as the Department of Energy, the Food and Drug Administration and the National Nuclear Security Administration, among others. The CCL lists certain dual-use, fully commercial, and less sensitive military items while items that are considered defense articles and services are included in the USML. USML is a list of articles and/or services that are specifically designed, developed, configured, adapted or modified for a military application and do not have a predominant civil application or civil performance equivalent; have significant military or intelligence applicability; and are determined or may be determined as a defense article or defense service. Taking a closer look at the dual-use paradigm, the CCL enumerates dual-use, commercial, and less sensitive military goods, software, and technology in categories ranging from materials processing, electronics, sensors and lasers, to navigation and avionics. Each item has an Export Control Classification Number ("ECCN") that specifies characteristics and capabilities of the items controlled in each ECCN. The definition of an export is intentionally broad and includes the provision of technical information to a foreign national anywhere in the world.

[83] Previous attempts at consolidating the organizational responsibility for export controls to a single government department focused on controlling a single list have not been implemented.

technologies or to investigate the relationship between investors and employees of a startup. Lastly, export controls are going to be much more effective if there is an international effort to protect the technology; otherwise, there may be an unintended consequence of the technology developing faster outside the U.S. aided by foreign investment through an allied country. If and when a dual-use technology is deemed worthy of control, the U.S. government can impose unilateral controls while it undertakes an effort to have the technology controlled internationally through the multilateral export control regimes but this process can take up to three years and may not be successful.

(3) VISAs for Chinese foreign national students studying in the U.S. are controlled by the State Department and not scrutinized for fields of study with the protection of critical technologies in mind.

Recommendations

The recommendations are divided into two sections: The first outlines actions DoD can take to deter China's technology transfer; and the second identifies areas where the whole of U.S. government needs to coordinate actions as part of a coherent policy.

Recommendations for DoD: <u>PROTECTING CRITICAL TECHNOLOGIES</u>

1. Develop three lists of **critical technologies** which must be maintained dynamically:
   A. Technologies (including fundamental component technologies) supporting *current* acquisition programs. This is what JAPEC is designed to do but JAPEC is hindered by a lack of resources and a single leader to accomplish the mission.
   B. *Future* technologies which will be the source of innovations for decades to come such as artificial intelligence, autonomous vehicles, advanced materials science, etc.
   C. *Defensive* technologies which deny China the ability to close the gap with current U.S. military capability (such as advanced semiconductors, jet engine design, etc.)
   D. Invest in the capability and process to maintain these lists on an ongoing basis.
   E. Decide on the resource and leadership model to accomplish this.

2. Develop a **technology *landscape*** map to identify the risks of key end-use and component technologies moving offshore adding to the government's understanding of what to protect. This will help ensure that critical technology lists are forward-looking.

3. Increase the **counterintelligence** efforts to deter Chinese foreign nationals from stealing intellectual property and technology from start-ups developing critical technologies.

4. Apply the DoD-led critical technologies list as the basis for CFIUS transaction denials and export controls. Since there is no agreement on this list across departments/agencies today, DoD should partner with the economic agencies (Commerce, USTR, Treasury and others) in sharing the rationale of technologies to be protected.

5. Review **export controls** to recommend to Commerce and State further limitations on entire classes of technology, products, tools and equipment consistent with the critical technologies we want to protect.

6. Develop an **intelligence sharing mechanism with allies** in reviewing foreign technology investments. To prevent China, for example, from acquiring a critical technology, we need to share the list of critical technologies and develop a mechanism to coordinate with allies facing similar decisions regarding foreign investment.[84]

[84] This worked on an informal basis recently when the U.S. worked with Germany to block the acquisition of Aixtron, a German company with U.S.

7. Request that the intelligence community collect and analyze the intelligence regarding China's capabilities as a strategic economic competitor on a regular basis.

8. Increase the new technology capabilities of DoD through focused efforts like the near-term Strategic Capabilities Office (SCO) and the longer-term Third Offset strategy to stimulate the demand for new technologies and gain the experience of refining these for military purposes

9. Allocate more budget to **DoD-sponsored research** such as DARPA programs as well as creating the demand for these advanced technologies (perhaps through new weapons programs) to ensure DoD and the supporting industrial base gets the experience with refining and producing the new technologies

11. Continue **fast prototyping and pilot projects** through the work begun by DIUx to ensure DoD benefits from the latest technologies developed.

Recommendation for U.S. Government: <u>RESTRICT CHINA'S INVESTMENTS IN CRITICAL TECHNOLOGIES & EXPAND OUR NATIONAL TECHNOLOGY STRATEGY</u>

Given the strategic competition underway with China, we propose **restricting investments and acquisitions by China in the critical technologies identified by DOD.** Since the vast majority of technology development today comes from the commercial sector (rather than from government research) and so many of these technologies are dual-use (such as autonomous vehicle capability which has commercial as well as military applications), restricting investments in a critical technology is the clearest and easiest policy to implement rather than attempting to distinguish between commercial technology and military technology where the difference is largely the field of use. To be effective, the restrictions should cover all transaction *types* that enable technology transfer under an expanded CFIUS jurisdiction (not only acquisitions but new investments, and joint ventures--whether located in the U.S. or abroad).[85]

To engage effectively with the private sector, **the U.S. government must be willing to acknowledge the strategic competition underway with China and change its policies regarding open investment and free trade in the technology sector.** The U.S. must be willing to acknowledge the strategic threat from equal access to U.S. technology, the unfair trading practices China engages in and share evidence regarding the degree of industrial espionage and cyber theft. With this change in policy, rationale and disclosure, the U.S. government can enlist the private sector and academia to further thwart the technology transfer to China.

<u>1. Data collection & analysis capability</u>. Since there is no comprehensive source on foreign investment across our economy, at a minimum, the U.S. government should develop a data collection & analysis capability for real-time visibility into foreign investments with a priority on countries which are a national security concern. DoD is not a natural home for this capability.

<u>2. Consider a lead agency for a new U.S. government China policy.</u> To coordinate all the departments and agencies with a coherent, well-articulated policy, this effort may need to be a National Security Council priority.

---

operations which provides important processing equipment (chemical vapor deposition) in the semiconductor industry.

[85] These recommendations are completely aligned with the 2016 Report to Congress of the US-China Economic & Security Review Commission. In fact, the Commission goes further to recommend authorizing CFIUS to bar Chinese *state-owned* enterprises from acquiring or controlling ***any*** U.S. company and not limiting this to technology companies. The Commission stresses that the U.S. should be much stronger in ensuring that China is abiding by its bilateral and multilateral commitments including with the WTO. This Commission for years has warned the Congress and the public about the technology transfers to China and the unfair competitive practices of Chinese companies and the Chinese government. *2016 US-China Economic & Security Commission Report.*

3. Reform CFIUS: expand jurisdiction to review all technology transfer transactions and restrict investments in and acquisition of critical technology companies by adversaries.

A. Mandatory reporting requirements of foreign investments above a certain threshold (e.g., $1M);
   (1) This does not imply that all of these investments will be reviewed or approved;
   (2) However, if the investments are in companies working on the agreed-upon list of critical technologies *and* the investment is from a country that represents a national security concern, these investments will be challenged by CFIUS. While the private sector will not like the mandatory reporting requirement and potential review by CFIUS, this alone will be enough of a deterrent in the certainty of closing a financing round that most startups will avoid foreign capital
B. Expand CFIUS' jurisdiction to include all technology transfer transactions: joint ventures (whether located in the U.S. or abroad because technology transfer can occur whether the joint venture is in the U.S. or abroad), green field investments, assets purchased from bankruptcies, reverse mergers, etc.
C. Develop a more formal and transparent risk scoring of transactions (discriminating by country and by sector) to facilitate the review of more transactions; strive to accept low-risk transactions quickly while dedicating more resources for the high-risk transactions
D. Provide the security agencies (Department of Defense, Department of Justice, Department of Homeland Security) the formal authority to reject transactions based on national security concerns arising from a formal risk scoring approach and when there is agreement among them
E. Given the cost and lack of proven effectiveness of mitigating agreements, strive to minimize these and standardize the ones that are needed; if mitigating agreements cannot be simple, CFIUS should deny the transaction
F. Allocate budget for CFIUS participating agencies to ensure sufficient resources to review a large number of transactions (e.g., 1500 per year or 10X the current level)
G. Formally collaborate with our allies in developing a coordinated strategy (especially with respect to China) that addresses international security[86]
H. Allow for a longer-time frame than 90 days if the complexity of the national security concerns warrants further investigation

4. Increase the FBI counterintelligence resources applied. Work collaboratively between DoD and the FBI to not only understand better the scale of the industrial espionage problem but set the goal of stopping the theft before it occurs as a measure of success in addition to the number of successful cases prosecuted. Be more proactive in canceling VISAs for Chinese agents engaging in industrial espionage.

5. Outreach to private sector: Invest in education and awareness in an outreach to U.S. businesses and the public.

A. Share the scale of China's industrial espionage and plans for global economic dominance: reveal cases of market manipulation, compromised supply chains, and espionage to make the case for economic losses rather than rely purely on private sector's patriotism
B. Develop a "Know Your Employee" program to educate companies working to develop sensitive technologies to mitigate the risks of employing foreign nationals
C. Develop a "Know Your Investor" program with outreach to the VC community to alert them to increasing foreign investments in critical technologies with the potential for technology transfer or intellectual property theft; share what we know from counterintelligence efforts
D. Increase cybersecurity protection of the technology sector. Since this is a source of very cost-effective illegal

[86] This paper did not undertake a comparative analysis of how other countries review foreign investments but we do know that some countries have an established mechanism for this and others do not. However, since technology transfer to China is a multinational issue, it only makes sense to coordinate with our allies in deterring this. The U.S. is already working with some allied governments on a limited and informal basis but to increase our effectiveness, we should make this a regular and formal process.

technology transfer, the U.S. government should consider what incentives and assistance it can provide to ensure that technology companies (and even early-stage technology companies) implement best practices to prevent cyber theft. One idea might be for the Department of Homeland Security to consider technology companies as part of its critical infrastructure programs.

6. Outreach to academia: Work with the State Department to ensure that student visas are appropriately scrutinized and used as part of this change in policy.

7. Create a national focus to stimulate technology development and innovation with the goal of creating an urgent national focus on U.S. leadership in these areas which have been traditional strengths. This would build upon and expand the work outlined in the current U.S. 21st Century Science, Technology & Innovation Strategy.[87] From a human capital standpoint, this would include an increased emphasis on STEM graduates in the U.S. and should consider immigration reform such that the large numbers of foreign graduate students can stay in the U.S. after graduation to contribute to our economy. This also implies a large increase in the basic research budget by government and the appropriate incentives (e.g., through tax policy) for the private sector. The U.S. should consider naming national innovation priorities and funding some moon shots to stimulate our efforts.[88]

Alternatives to these Recommendations

1. **Do Nothing.** Even though this is the de facto approach today, the cost of doing nothing is extraordinarily high: the loss of $300 billion worth of stolen intellectual property each year, $300 billion in lost U.S. sales resulting from this theft and 2.1 million U.S. jobs.[89]
2. **Restrict investments on a case-by-case basis.** This approach puts too much faith in the ability to appropriately discern which investments are problematic and which are benign. Given our recent experience with the semiconductor industry where there can be so many single transactions before the pattern emerges, this is a risky approach. There is more certainty and efficiency in the private sector and in government from a broader but simpler policy that all understand.
3. **Increased diplomacy and incentives to require China to more uniformly adhere to fair trade.** The cost of increased technology transfer is too high to wait the years that would be required to know if this diplomatic approach is working. Given the experience of the past 15 years since China became a member of the WTO, there is sufficient evidence already to know that there are many Chinese violations of fair trading practices and China is unlikely to put support of the international economic order ahead of its own economic interests as it continues to pursue a mercantilist strategy.
4. **Focus on U.S. technology development instead of restricting Chinese investment.** In fact, such a focus is what we are recommending (see #7 above) but feel this strategy alone is not a substitute for effective defensive steps to slow the technology transfer underway to China. A more successful policy is likely to combine what we can do to foster innovation and technology while we also deter further technology transfer.

[87] "A 21st Century Science, Technology & Innovation Strategy for America's National Security"

[88] In fact, this was recommended recently for the semiconductor industry by the President's Council of Advisors on Science & Technology in their report to the President in January, 2017. We are suggesting a much broader focus of future technology development rather than a narrow focus on a single industry.

[89] The IP Commission Report (2013).

Costs and Implications

A complete assessment of both the implications and game theory of potential reactions would require a much more significant analysis but an outline of the major areas of concern follows.

1. **China restricted investment in U.S. technology sector.**
   a. For the private sector, the costs of reporting foreign investment above a certain threshold level ($1 million) would be minor. The possibility of a CFIUS review would be the bigger burden if an early-stage company is contemplating foreign capital; this would likely reduce some of the foreign capital investment since companies would not be willing to undertake the risk of a time-delay in a financing.
   b. Limiting China's investment in U.S. technology companies would reduce the capital that China currently contributes to the venture rounds of financing and reduce the capital available for U.S. mergers and acquisitions (M&A) but the impact would be minor. China only participates in 10% of venture financing and the Chinese contribution is probably 2-3% of the total $137 billion in U.S. venture investment.[90] There would be a similarly minor impact on the U.S. technology M&A market which is about 12% of the total U.S. M&A market. China's acquisition of U.S. companies totaled $50-70 billion in 2016 or 2-3% of the total U.S. M&A market of $2.25 trillion.[91] However, the impact to an individual company could be significant as there are examples of weaker companies where the only reasonable acquisition offer is from a Chinese company interested in the technology for strategic reasons.
2. **China retaliation in trade.**
   a. Creating friction. According to early reports, China is preparing to create some friction for U.S. companies with operations in China as a first step if the Trump Administration pursues any trade war tactics as have been promised in the campaign. These tactics would include more scrutiny through investigations for tax compliance, anti-dumping and anti-trust probes. China would also scale back on its government purchases of products from U.S. suppliers.[92]
   b. Trade disruption. A likely outcome of the recommendations to restrict China's technology investments and acquisitions would be disruption of the trading flows with China potentially limiting imports and increasing tariffs. There could clearly be many examples of U.S. businesses which might be damaged by supply chain disruptions especially in the technology sector and these would be difficult to estimate. However, in terms of the macroeconomic effect, a disruption in trade would disproportionately negatively affect the Chinese economy in a ratio of 4 to 1. Total Chinese exports to the U.S. were $498 billion in 2015 (18% of China's total exports) and 4% of the Chinese GDP. U.S. exports to China were $161 billion in 2015[93] (7 % of U.S. total exports and 1% of U.S. GDP). Given the importance of growth to China's economy, it would be a painful decision for the Chinese government to implement a policy which would reduce its target growth rate of 7%. In the extreme case, if China were to stop *all* exports to the U.S., this would reduce China's target GDP growth rate by 4 points to 3%. Exports play a much smaller role in the overall U.S. economy and represent 12.5% of U.S. GDP while exports represent 21% of China's GDP as China is the world's largest exporter.
   c. Higher priced imports. The other significant impact to the U.S. economy of fewer imports from China would be cost increases for imported goods. Given the low-cost of manufactured goods from China, the resulting 1.0-1.5% higher prices paid for substitute goods would result in increased inflationary pressure for the economy and profitability pressure for U.S. businesses.[94] Given the low inflation environment we are

---

[90] "The Rise of Chinese Investment in U.S. Tech Startups", *CB Insights Blog*;

[91] "M&A in the U.S.", *Institute for Mergers, Acquisitions & Alliances*. Retrieved at http://www.imaa-institute.org

[92] Steven Yang, "China Said to Mull Scrutiny of U.S. Firms If Trump Starts Feud", *Bloomberg News*, January 6, 2017

[93] "U.S.-China Trade Facts", Office of the United States Trade Representative, 2016. Retrieved at http://www.ustr.gov

[94] "Understanding the U.S.-China Trade Relationship," Prepared for the U.S.-China Business Council by Oxford Economics (January, 2017)

currently enjoying, this risk would not be as significant as the potential disruptions in global supply chains.

While a significant judgment call, the costs of these recommendations are outweighed by the benefits of a stronger U.S. economy in the long-run buoyed by increased innovation and reduced risk of technology transfer. As history shows us repeatedly, a strong. globally-leading economy is the only means to ensure long-term national security.

List of Appendices

APPENDIX 1: Chinese Investment in Critical Technologies

Compared to other sources of investment, Chinese entities ranked only behind domestic U.S. sources ($469 billion) and Europe ($76 billion), but well ahead of Japan ($19 billion), Russia ($9 billion), Israel ($6.5 billion), India ($5 billion), and Korea ($3.3 billion).

Chart 2: Chinese Share of U.S. Venture Capital Market 2010-2016

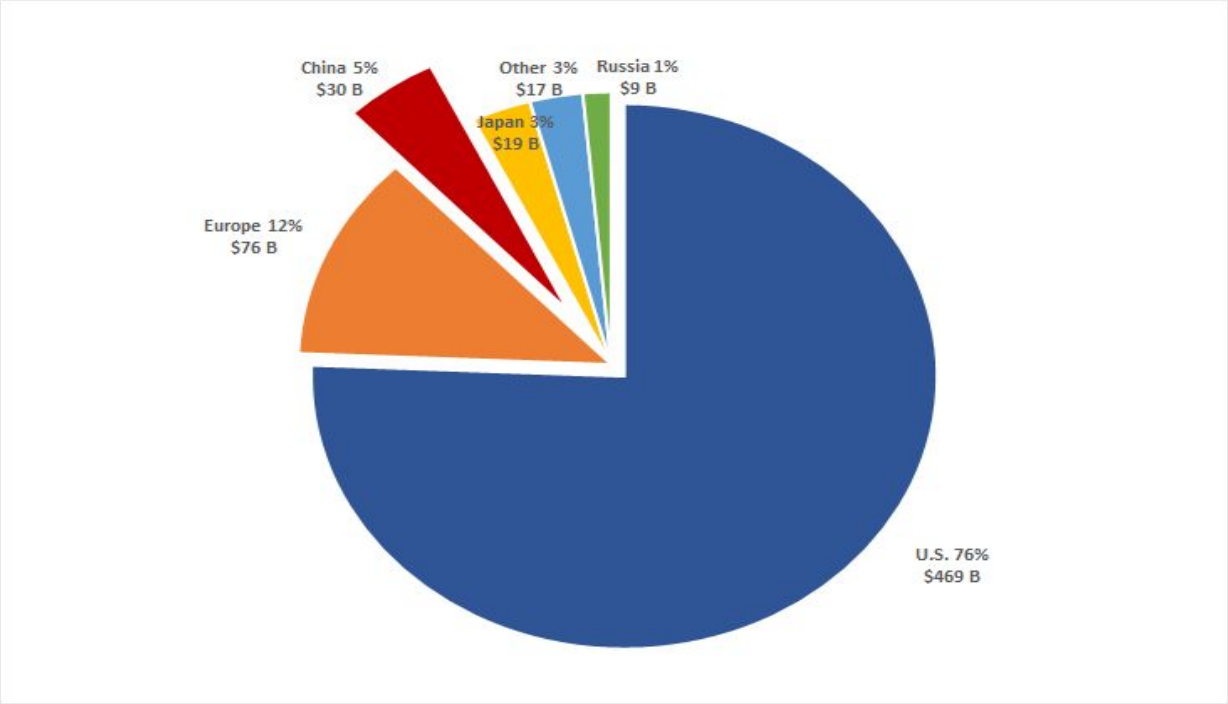


Chart 3: Chinese Investment in U.S. Artificial Intelligence Companies, 2010 - 2016

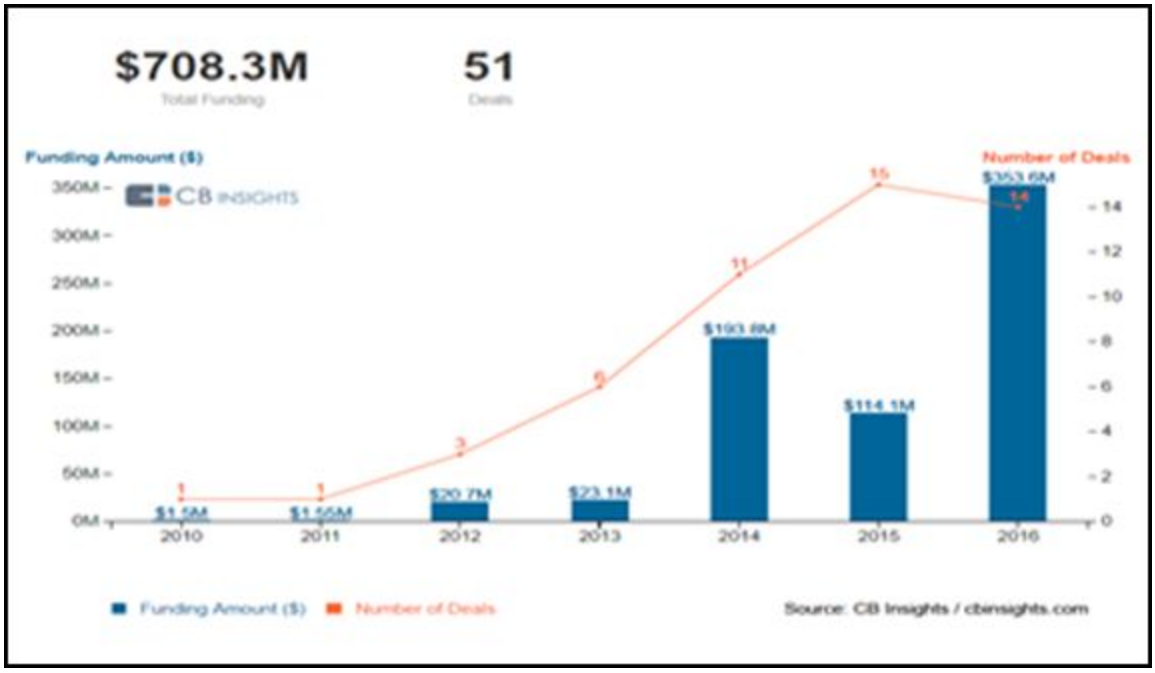


Chart 4: Chinese Investment in U.S. Robotics Companies, 2010 - 2016

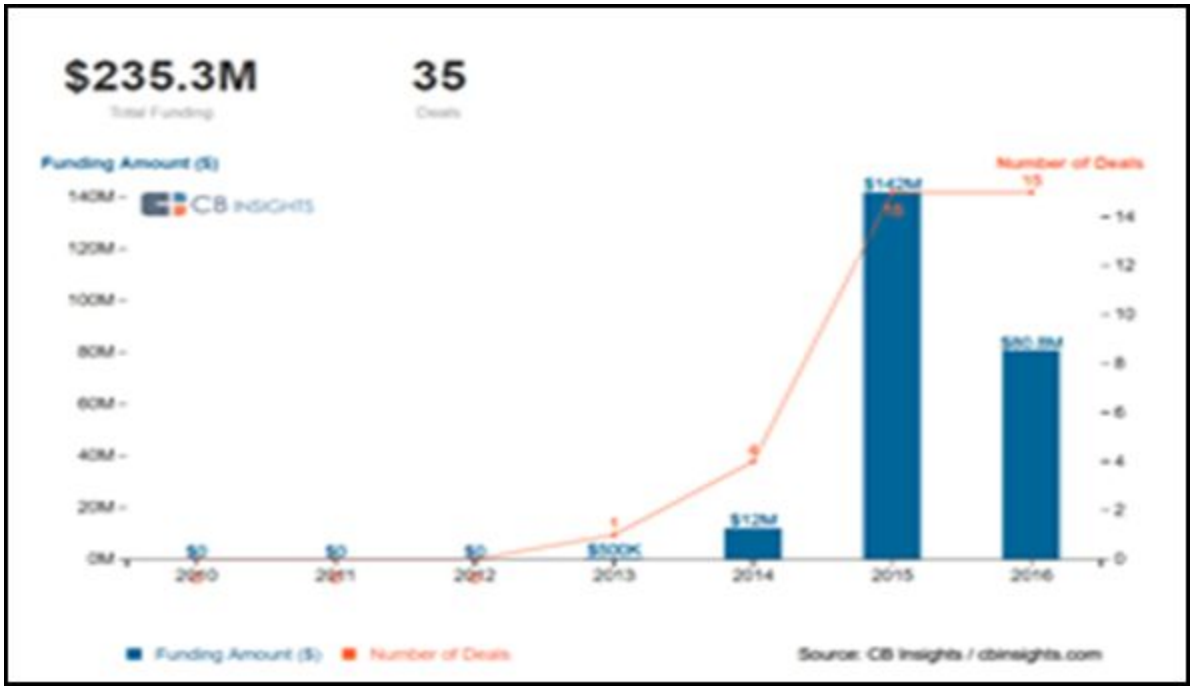


Chart 5: Chinese Investment in U.S. AR/VR Companies, 2010 - 2016

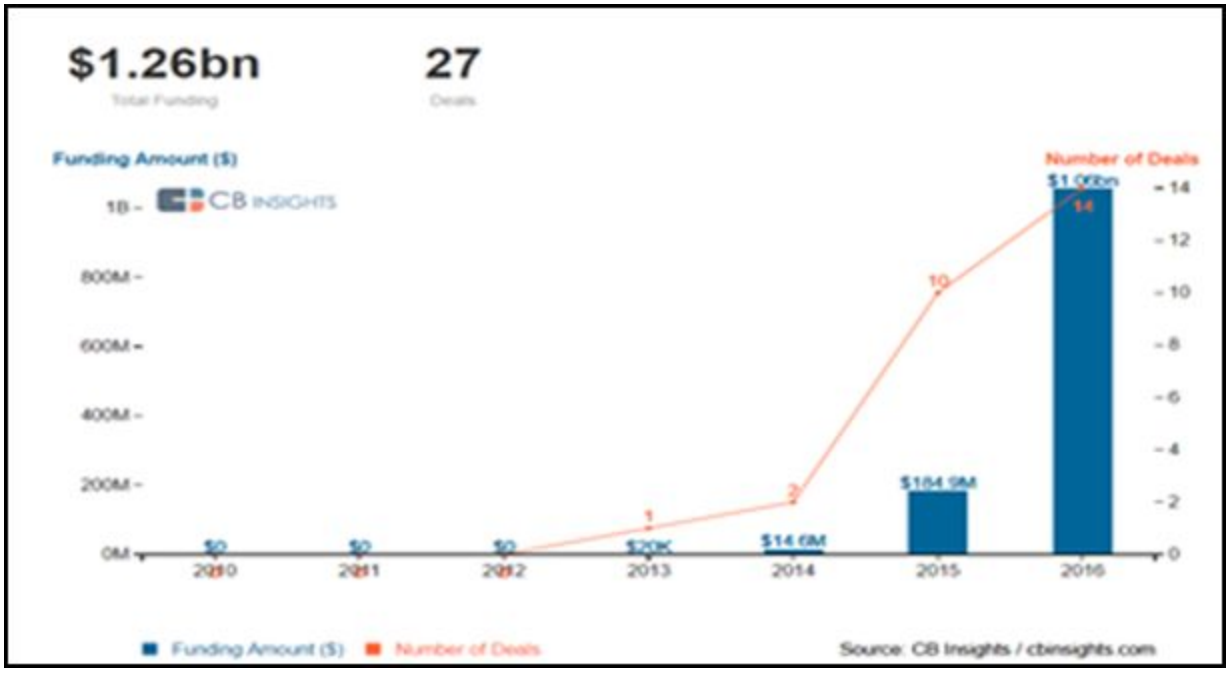
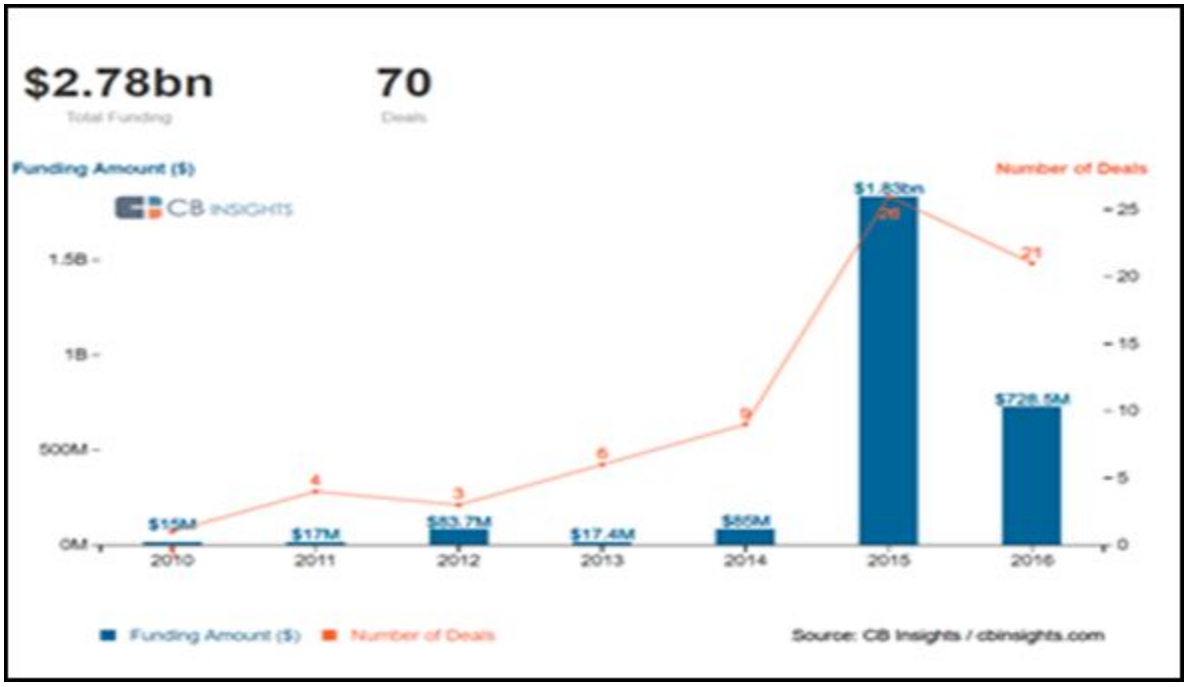


Chart 6: Chinese Investment in U.S. FinTech Companies, 2010 - 2016



APPENDIX 2: Select Chinese Venture Deals in 2016 Illustrating Technology Focus[95]

Company	Focus Area	Round Amount ($M)	China Investors	Date	Location
Magic Leap	Augmented reality	$798.5	Alibaba Group, Enjoyor Group	Feb-16	Florida
Zoox	Autonomous vehicles	$200	AID Partners	May-16	California
Unity Technologies	Game development platform	$181	China Investment Corporation, Frees Fund	Jul-16	California
Velodyne	LiDAR sensor technology	$150	Baidu	Aug-16	California
NextVR	VR content	$80	CITIC Guoan, NetEase Capital, China Assets Holdings, CMC Holdings	Jul-16	California
Razer	Gaming hardware and products	$75	Hangzhou Liaison Interactive	Feb-16	California
Circle Internet Financial	Consumer payments	$60	Baidu	Jun-16	Massachusetts
Meta	Augmented reality	$50	Tencent, Lenovo Group, Ningbo GQY, Horizons Ventures, Banyan Capital	Jun-16	California

[95] CBInsights data

Appendix 3: Case Studies of Chinese Venture Firms: SINOVATION and HAX

Sinovation Ventures

Sinovation Ventures is a venture capital firm domiciled in China with an office in Silicon Valley. The firm was founded by Dr. Kai-Fu Lee in September 2009 and invests in early stage companies (Series A and Series B) in the United States and China. The company focuses on the following investment areas: Internet of Things connected devices, developer tools; and online education. Sinovation's portfolio includes companies developing artificial intelligence, robotics, financial technology and AR/VR technologies.[96]

Some sample portfolio companies include[97]:

- ***Swivl:*** Swivl, owned and operated by Satarii, is the maker of a personal cameraman robotic video device. Swivl turns an iOS device into a personal cameraman with wireless microphone.
- ***Robby:*** Robby manufactures self-driving delivery robots that can autonomously navigate sidewalks to the consumer's door. This can reduce the costs for the on-demand meal, grocery, and package delivery industry by eliminating the high costs of human deliverers, which can ultimately lead to lower costs for the consumer.
- ***Deep Vision:*** Deep Vision is a deep learning company that is developing computer vision for cars, robots, drones and machines of all type. Deep Learning-powered breakthroughs are ushering in a revolution in computer vision which combine big data sets and powerful data centers.
- ***SPACES:*** SPACES is an independent virtual-and mixed-reality company based in Los Angeles, CA. SPACES is working with such companies as Microsoft, NBCUniversal, Big Blue Bubble and The Hettema Group, among others, to develop and produce a wide range of projects across all VR and MxR platforms and technologies, including Oculus Rift, HTC Vive, Microsoft HoloLens, Samsung Gear VR, PlayStation VR and Google Cardboard.

Sinovation Ventures has invested in almost 300 start-ups so far, including many well-known internet companies such as Zhihu, Dianxin, Umeng, Tongbu Network, Wandoujia, Anquanbao, Kuaiya, Qingting FM, Yaochufa, Weiche, Moji Weather, Elex, Kakao, Baozou Comics, Face++, VIPKID, Boxfish, U17, SNH48, ImbaTV, Molbase, Ebest, Maihaoche, EALL, The ONE Piano, Zaijia, Joy Run, Horizon Robotics, Niu, Planetary Resources, etc. and Meitu which is expected to go public on the Hong Kong Stock Exchange soon.[98]

The firm combines incubation and investment offerings to facilitate the growth of companies that suit the Chinese marketplace. It has been awarded as a cutting-edge "National-Level Technology Company Incubator" by China's Ministry of Science and Technology (MOST). It has also been recognized as an "Incubation Base for Strategic Emerging Industries in Beijing" and a "Zhongguancun National-Level Innovative Model of Incubator for Indigenous Entrepreneurship" by Municipal Science and Technology Committee of Beijing, where the Firm's headquarters is based. Sinovation Ventures has established itself as a top-tier venture capital firm in China and has been backed by leading investors around the world. It currently manages three U.S. dollar funds and two RMB funds, with a total asset under management of $1.2 billion (or about RMB 8 billion).[99]

---

[96] http://www.sinovationventures.com/

[97] Data retrieved from CB Insights Database

[98] https://www.crunchbase.com/organization/sinovation-ventures#/entity

[99] *Ibid.*

Hax

HAX is a hardware accelerator that has helped over 30 companies launch in the past 2 years. Based in Shenzhen and with an office in San Francisco, HAX provides end-to-end technical and financial support to early-stage hardware companies through its "Interactive Manufacturing Process", which enables rapid development of manufacturable products.

Between 2014 and 2016, Hax participated in nearly half of all deals involving Chinese investors (14 of 29 deals). HAX companies receive up to $25,000 to $100,000 each and access to the SOS Ventures Hardware scaling fund.[100]

Some examples of Hax investments include:

- ***Petronics:*** Petronics is the creator of "Mousr", a robotic mouse that has sensors, actuators, and intelligence that actually sees a cat and responds to its hunting movements like a real animal would.
- ***Dispatch:*** Dispatch is creating a platform for local delivery powered by a fleet of autonomous vehicles designed for sidewalks and pedestrian spaces.
- ***Clean Robotics:*** Clean Robotics provides trash sorting robots for offices.

HAX is backed by SOS Ventures, a venture firm with headquarters in Shenzen and an office in San Francisco. It funds a handful of accelerators similar to Hax – Indie Bio in the biosynthetic space; Chinaccelerator for pure software; and Food-X for food-related startups. SOS Ventures provides funding at the seed, venture, and growth stage, providing expertise and technical assistance to entrepreneurs in areas such as engineering, mass manufacturing, product/market fit, messaging, and presentation. The company's website claims funding for over 500 startups.[101]

[100] Retrieved at https://www.crunchbase.com/organization/haxlr8r#/entity

[101] Retrieved at https://www.sosv.com/

Appendix 4: Chinese Government-Backed Funds in Silicon Valley[102]

Company	Tie to Local Government	Total Money Raised	Select Investments
Westlake Ventures	**Owned by Hangzhou government**	**$66 million ($16 million already available and $50 million pending approval for transfer out of the country)**	**WI Harper Group, SVC Angel Fund, Amino Capital, FreeS Fund, Spider Capital, Benhamou Global Ventures**
ZGC Capital Corporation	**Indirectly owned by 17 state-owned enterprises, including China State Construction and Beijing Industrial Development Investment Management Company.**	**$60 million so far, plans to raise $500 million by 2020**	**KiloAngel, Danhua Capital, Plug & Play (in the process), Santa Clara office building**
HEDA Investment Co.Ltd	**HEDA is a fund set up by Hangzhou Economic and Development, an economic development zone under municipal government of Hangzhou**	**$500 million**	**None yet: Focusing on information technology and bio tech.**
Shanghai Lingang Economic Development Group	**Supervised by the state-owned Assets Supervision and Administration Commission of the State Council (SASAC) of Shanghai.**	**None yet; plans to raise an overseas fund this year**	**A San Francisco office building for $42 million.**
Research Institute of Tsinghua University in Shenzhen	**Half-owned by the municipal government of Shenzhen, and the other half is owned by Tsinghua University.**	**Tens of millions of dollars**	**TEEC (Tsinghua Entrepreneurs & Executives Club) Angel Fund, Early-stage startups**

[102] Yunan Zhang, "Chinese Government's Path to Silicon Valley," *The Information* (January 25, 2017)

Appendix 5: China's Economic and Technology Goals

Made in China 2025 is a plan aligning State and private efforts to establish China as the world's pre-eminent manufacturing power by 2049. "Its guiding principles are to have manufacturing be innovation-driven, emphasize quality over quantity, achieve green development, optimize the structure of Chinese industry and nurture human talent."[103] *Made in China 2025* highlights 10 priority sectors emphasizing the criticality of integrating information technology with industry. Key sectors prioritized include:

- Advanced information technology
- Automated machine tools and robotics
- Aerospace and aeronautical equipment
- Maritime equipment and high tech shipping
- Biopharma and advanced medical products
- New energy vehicles & equipment

12th Five Year Plan of 2011-2015 lists a "new generation information technology industry" as one of the seven strategic and emerging industries to develop. Policies and practices were put in place to (1) prioritize indigenous innovation, especially in high-performance integrated circuit products, (2) promote domestic champions and (3) encourage technology acquisitions

- ICT priorities include
  - Mobile communications,
  - Next generation internet
  - Internet of things
  - Cloud computing
  - Integrated circuits
  - New display technologies
  - High-end software & servers
- Policies and practices:
  - Prioritize indigenous innovation, especially in high-performance integrated circuit products
  - Promote domestic champions: pursue M&A, reorganizations and alliances between upstream and downstream enterprises
  - Encourage technology acquisitions, participation in standards setting & moving up the value chain

13th Five Year Plan of 2016-2020 "Internet Plus"[104] deepens reforms and priorities called for in *Made in China 2025* and emphasizes stronger control by the government over network-related issues as China continues to control the internet within China and gains access to global networks by controlling key component and telecommunications technologies

- Plan goal to "Encourage hundreds of thousands of people's passion for innovation, building the new engine for economic development"
- Leverages large internet base of 649 million users, 557 million of whom access the internet with a mobile phone
- Deliver to large cities 100 MBps internet bandwidth and provide broadband access to 98% of the population living in incorporated villages
- ICT priorities include:
  - Expansion of network economic space

---

[103] Scott Kennedy, "Critical Questions Made in China 2025," Center for Strategic and International Studies; Retrieved at https://www.csis.org/analysis/made-china-2025

[104] Lulu Chang, "China Outlines its Latest FYP Called Internet Plus."

- New generation information infrastructure,
- Advancements in Big Data
- Enhanced information security and cyberspace governance
- Fostering of domestic capabilities in:
  - Artificial intelligence
  - Smart hardware
  - New displays and intelligent mobile terminals,
  - 5th generation mobile communications
  - Advanced sensors and wearable devices

Medium and Long-Term Plan for Science & Technology Development is the most far- reaching of government plans to "shift China's current growth model to a more sustainable one, to make innovation the driver of future economic growth and emphasize the building of an indigenous innovation capability."[105] There are 3 strategic objectives:

- Building innovation-based economy through indigenous innovation
- Fostering an enterprise-centered technology system and enhancing Chinese firms' innovation
- Achieving major breakthroughs in targeted strategic areas of development and basic research and boosting domestically owned intellectual property

Project 863: China's National High Technology Program is designed to overcome the shortcomings in national security through the use of science & technology

- Encompasses development of dual-use technology (civilian and military applications)
- Lays a foundation for indigenous innovation

China's Mega Project Priorities are 16 Manhattan-style projects[106] to bring together the focus on specific innovations and the resources to ensure progress. These are outlined in Appendix 6.

Appendix 6: Chinese National Science and Technology Major Special Projects Mega-Projects

October 2016

Original Announced National Science and Technology Major Special Projects Contained in the '2006-2020 Medium and Long-Term S&T Development Plan'	**Agencies in Charge**
Core Electronics, high-end general chips, basic software	Ministry of Industry and Information Technology (MIIT)
Ultra large scale integration manufacturing technology	Beijing, Shanghai governments
High-end computer numerical controlled machine tools and basic manufacturing technology	National Development and Reform Commission, MIIT
Water pollution control and treatment	Ministry of Environmental Protection
Large-scale oil and gas fields and coal-bed methane	China Petroleum, China United Coal-bed Methane Co.

[105] Hannas, *Chinese Industrial Espionage*, Chapter 3

[106] Michael Raska, "Scientific Innovation and China's Military Modernization", *The Diplomat* (September 3, 2013), Retrieved at http://www.thediplomat.com

development	
Next generation broadband wireless mobile communications	Ministry of Science & Technology (MOST), National Energy Bureau, Tsinghua University
Genetic transformation and breeding of new plants	MIIT, Datang Electronics, CAS, Shanghai Institute of Microsystems, China Putian
Major new drug development	Ministry of Agriculture
High-resolution Earth observation system	MOST, Ministry of Health, People's Liberation Army (PLA) General Logistics Department
Prevention and control of major infectious diseases	State Administration for Science, Technology and Industry for National Defense (SASTIND), China National Space Administration
Large passenger aircraft	MOST, Ministry of Health, PLA General Logistics Department
Manned spaceflight and lunar exploration project	MIIT, Commercial Aircraft Corp. of China
3 Unidentified Classified Defense-Related Mega-Projects (candidates include Beidou Satellite Navigation System and Inertial Confinement fusion)	
New Additional National Science and Technology Major Special Projects Contained in the 'Science, Technology and Innovation 2030 Plan'	
Aero-engines and gas turbines	SASTIND, China Aircraft Engine Corp.
Quantum communications	
Information networks and cyber security	
Smart manufacturing and robotics	
Deep-space and deep-sea exploration	
Key materials	
Neuroscience	
Health care	

Source: Tai Ming Cheung, Associate Professor and Director of the Institute on Global Conflict and Cooperation (IIGC) at the University of California, San Diego

Appendix 7: McKinsey Study on Industries Where China Leads in Innovation

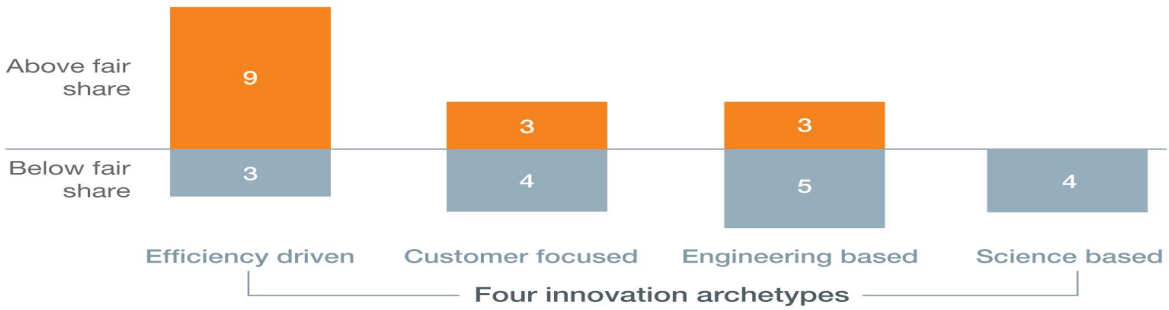
To assess the comparative innovation capability between China and the U.S., McKinsey recently analyzed in what industries China was developing an innovation lead and in what industries China is lagging.[107]

- In traditional manufacturing-based industries where low costs provide a competitive advantage, it is not surprising that China is leading the world. These industries would include electronics, solar panels and construction equipment where a combination of a large and concentrated supply base, agile manufacturing, modular design and flexible automation all provide benefits.
- In its consumer markets (which are customer-focused), China has a natural advantage given the sheer size of the market of 1.3 billion people (4x that of the U.S.) and this advantage is compounded when markets are protected. Industries where China again leads the world would include household appliances, smartphones (functionality delivered at low cost) and internet software companies (Alibaba, Baidu and Tencent).
- In engineering-based industries, the results are mixed. The best example is high-speed rail where innovation has been matched with local demand and government sponsorship. China accounts for 86% of the global growth in railroads since 2008. Other examples would be wind power and telecommunications equipment (Huawei and ZTE). China is not yet leading in automobile engines, aerospace, nuclear power or medical equipment.
- In science-based industries, such as branded pharmaceuticals, the results are poor. Here, the massive growth and national focus on R&D spending have not yet paid dividends. These investments naturally take a long time to pay off and the Chinese government is actively working to remove obstacles to enable Chinese firms to lead. This is an area where focus on national mega projects can be fruitful since they concentrate government sponsorship with focused resources and local demand. For example, China is rapidly improving its drug discovery and medical trials process to favor its domestic companies. Gene editing is a technology where the government sees tremendous promise and is actively supporting.

The following chart summarizes this industry-grouping analysis:

Chinese companies in industries that rely on efficiency-driven innovation perform well, science-based companies less so.

Chinese industries: actual vs expected performance in innovation
(based on China's share of global GDP[1]), number of industries = 31



[1]China's share was 12% in 2013.

Source: IHS Global Insight; International Data Corporation; annual reports; McKinsey Global Institute analysis

[107] Erik Roth, Jeongmin Seong, Jonathan Woetzel, "Gauging the Strength of Chinese Innovation," *McKinsey Quarterly* (October, 2015).

Appendix 8: Largest Chinese Cyber Attacks

- **Breach of more than two dozen major weapons system design**s in February, 2012 from the military and defense contractors including those for the advanced Patriot missile system (PAC-3), an Army system for shooting down ballistic missiles (Terminal High Altitude Area Defense, THAAD) and the Navy's Aegis ballistic-missile defense system, the F-35 Joint Strike Fighter, the F/A-18 fighter jet, the V-22 Osprey, the Black Hawk helicopter and the Navy's new Littoral Combat Ship[108]
- **"Titan Rain"** a series of coordinated attacks for multiple years since at least 2003 which compromised hundreds of government computers stealing sensitive information[109] " In 2004, an analyst named Shawn Carpenter at Sandia National Laboratories traced the origins of a massive cyber espionage ring back to a team of government sponsored researchers in Guangdong Province in China. The hackers, code named by the FBI "Titan Rain," stole massive amounts of information from military labs, NASA, the World Bank, and others."[110]
- **PLA Unit 61398** (a cyberforce within the Chinese military) which penetrated the networks of >141 blue chip companies across 20 strategically targeted industries identified in China's 12th Five Year Plan for 2011-2015 such as aerospace, satellite and telecommunications and IT. Among other areas of theft, source code was stolen from some of the most prominent U.S. technology companies such as Google, Adobe and others; Google announced this in January, 2010. This resulted in the U.S. indictment of 5 members of this organization. According to Mandiant, PLA Unit 61398 is just one of more than 20 cyber attack groups within China.[111]
- **"Hidden Lynx**" which according to Symantec has a long history of attacking the defense industrial sector of Western countries with some of the most sophisticated techniques has successfully attacked the tech sector, financial services, defense contractors and government agencies since at least 2009[112]
- "DHS says that between December 2011 and June 2012, cyber criminals targeted **23 gas pipeline companies** and stole information that could be used **for sabotage purposes**. Forensic data suggests the probes originated in China."[113]
- "Canadian researchers say in March, 2105 that Chinese hackers attacked U.S. hosting site **GitHub**. GitHub said the attack involved "a wide combination of attack vectors" and used new techniques to involve unsuspecting web users in the flood of traffic to the site. According to the researchers, the attack targeted pages for two GitHub users—Great Fire and the *New York Times*' Chinese mirror site—both of which circumvent China's firewall."[114]
- "**The Commerce Department's Bureau of Industry and Security** had to throw away all of its computers in October 2006, paralyzing the bureau for more than a month due to targeted attacks originating from China. BIS is where export licenses for technology items to countries like China are issued."[115]
- **Breach of the U.S. Office of Personnel Management (OPM)** in 2014 where the personnel files of 4.2 million former and current government employee as well as the security clearance background information for 21.5 million individuals was stolen. Former NSA Director Michael Hayden said that this would compromise our national security for an entire generation.[116]

---

[108] Ellen Nakashima, "Confidential Report Lists U.S. Weapons System Designs Compromised by Chinese Cyberspies", *Washington Post* (May 27, 2013). Retrieved at http://www.washingtonpost.com

[109] Nathan Thornburgh, "Inside the Chinese Hack Attack", *Time* (August 25, 2005). Retrieved at http://www.content.time.com

[110] Josh Rogin, "The Top 10 Chinese Cyber Attacks (that We Know of)," *Foreign Policy* (January 22, 2010) Retrieved at http://www.http://foreignpolicy.com/2010/01/22/the-top-10-chinese-cyber-attacks-that-we-know-of/

[111] "APT1: Exposing One of China's Cyber Espionage Units", *Mandiant Report*, 2013.

[112] "Hidden Lynx--Professional Hackers for Hire", *Symantec Official Blog* (September 17, 2013). Retrieved at http://www.symantec.com

[113] Robert Knake, "Five Chinese Cyber Attacks that Might Be Even Worse than the OPM Hack," *Defense One* (June 15, 2015). Retrieved at http://www.defenseone.com.

[114] Knake, "Five Chinese Cyber Attacks that Might Be Even Worse than the OPM Hack"

[115] Rogin, "The Top 10 Chinese Cyber Attacks (that We Know of)

[116] "The OPM Breach: How the Government Jeopardized our National Security for More than a Generation," Committee on Oversight & Government Reform, U.S. House of Representatives, 114th Congress (September 7, 2016).

Appendix 9: U.S. Events with Chinese Sponsorship

1. **Silicon Valley Innovation and Entrepreneurship Forum (SVIEF)**, according to its website "is an international conference designed to foster innovation and promote business partnerships connecting U.S. and Asia-Pacific region." SVIEF has expanded to hold two conferences per year, the main conference held in the fall of 2016 and Silicon Valley Smart Future Summit held in winter and focused on interconnected devices. Both events are held at the Santa Clara Convention Center in Silicon Valley. A U.S. Congresswoman (Judy Chu) is the honorary Chairwoman of SVIEF and a keynote speaker at the principal fall conference was former U.S. Secretary of Energy Steven Chu. This gathering of startup CEOs, venture capitalists, Chinese companies and Chinese venture capitalists makes this an ideal location to collect information on the state of U.S. technology. Chinese officials attend who are assigned to collect intelligence.

2. **DEMO China**, an annual event held in Santa Clara, California (the heart of Silicon Valley) showcasing promising startups to Chinese investors. The event includes a keynote by the Chinese Consulate General, and has panels throughout the day covering topics such as navigating obstacles to investment in the U.S. and China; tips on how to evaluate startups; advantages of technology accelerators; and discussion of other investment trends.

3. **Silicon Valley-China Future Forum** (August, 2016) to link Silicon Valley with Chinese capital specifically in the fields of augmented reality, virtual reality and artificial intelligence.

4. **China Silicon Valley** is working with Silicon Valley city governments to drive increased investment and job growth by facilitating talent, technology and business exchange and investment between cities and businesses in China and their Silicon Valley counterparts. The intent is to help provide a one-stop service for government relations, legal, tax, consulting, networking and talent acquisition to facilitate Chinese government, businesses and individuals to invest, establish a factory, R&D center or other business activities in Silicon Valley. China Silicon Valley has an extensive network of business partners from diversified industries in Silicon Valley to carry out these activities.

5. **The Global Chamber San Francisco (GCSF)** hosts a seminar for entrepreneurs, investors and service providers with an interest in U.S.-China markets on strategies and best practices to enter and capitalize on business opportunities in U.S. & China.

6. **U.S.-China VC Summit & Startup Expo** (October, 2016) hosts a conference in Boston for investors and entrepreneurs who want to collaborate on opportunities between the U.S. and China.

7. **Chinese American Semiconductor Professional Association (CASPA)** holds many dozens of events per year in Silicon Valley and China. For 2017, the published schedule includes 4 conferences, 4 tradeshows, 4 workshops, 3 career development events, 3 international trips to China, hosted delegations from China and 6 members networking events. These events are all gathering Chinese and American semiconductor talent with the purpose of recruiting American talent.

APPENDIX 10: Private Sector Largely Unaware of China's Technology Transfer Threat

The private sector is largely unaware of China's plans for economic domination (nor have companies spent time contemplating its potential consequences) and unaware of the scale of technology transfer to China underway except for well-publicized cyber incidents. This is largely due to the fact that the U.S. trade and investment policies towards China are encouraging of bilateral trade and engagement. The benefits of low-cost manufacturing and the promise of a large China market have been widely promoted--certainly by the Chinese business community and government but also reinforced by U.S. economic policies designed to foster the integration of the U.S. and Chinese economies as part of a calculated geopolitical embrace of China, begun under President Nixon, accelerated under Presidents Reagan and Clinton, and continued to this day.

While there have been FBI efforts to warn companies of industrial espionage risks, these are rarely the lead stories in the narrative with China even though the number of convictions have been rising. In cases where the information is classified, the FBI has greater difficulty sharing the evidence which would show China to be the perpetrator in cases of market manipulation combined with industrial espionage and cyber theft. In other cases, the U.S. government has not connected all the dots when China has used some of the technology transfer methods outlined above in combination.[117] Further, since economic espionage has not been a priority for the U.S. intelligence agencies, gathering and analyzing this intelligence has not been a focus for resources nor a planned, systematic effort. The FBI officials who spoke with the authors of this report noted that the bureau has very limited resources relative to the threat. Even where resources are applied, the measure of success for law enforcement is prosecutions rather than preventing the theft.

We spoke with some Silicon Valley technology executives and many venture capitalists in the course of this work (a list is available in Appendix 12). Most were not aware of the degree of threat China poses and were more focused on the market opportunity of selling to Chinese businesses or consumers than in long-term trends of technology transfer that threaten to erode U.S. global competitiveness and, along with it, military supremacy. Firms, like Cisco, who directly compete with a Chinese-backed global champion, like Huawei, represent the exception since Cisco is well aware that when Huawei competes for business in an emerging market, like Africa, that the Chinese government joins Huawei and brings a portfolio of additional offerings to bear on a deal. For example, the Chinese government might offer to build infrastructure in an emerging market, finance this with low-cost capital from the China Development Bank and, in the process, provide jobs in the community in addition to supporting Huawei with subsidies for extremely competitive pricing on telecommunications and networking gear. Cisco finds this is extremely difficult to compete with and has lost market share on a global basis to Huawei in emerging markets. By protecting Huawei's domestic market and backing them in the export market as described above, China has created a global champion that is today the world's largest telecommunications equipment manufacturer.

Many of the venture capitalists we spoke with were largely unaware of the participation of Chinese capital in early-stage technology companies. This is no surprise given that Chinese capital is in only about 10% of venture deals even though this percentage has increased dramatically from a few years ago. Several U.S. venture firms who have done deals with Chinese venture capitalists expressed their frustration about multiple rounds of re-negotiation on price and terms saying you never really knew if you had concluded a deal. Most were aware that the Chinese internet companies (Baidu, Tencent, Alibaba, etc.) were actively participating in deals as strategic investors. Naturally, the venture community and technology companies are pleased to have the benefit of this additional capital in the market when they benefit from the higher valuations that result; at least one venture capitalist was concerned about the asset pricing distortion that comes with what was seen as a willingness of the Chinese to overpay for assets. We also learned that Chinese capital is involved to a small degree as limited partners of U.S. venture firms. The lists of limited partners are very closely guarded but the venture capitalists we spoke with assured us that the Chinese limited partner stakes in their firms were well under 10%.

[117] Conversations with Department of Defense and FBI Counterintelligence revealed that with so little resource applied to cases of economic espionage, we are unable to do the forensic work to see where cyber theft has led to industrial espionage and market manipulation.

Appendix 11: Strengths and Weaknesses of CFIUS Process Today

Strengths

- An understood process defined by FINSA statute (2007)
- No clear view on what constitutes a controlling interest that triggers an assessment by CFIUS which allows CFIUS to review more transactions than if a quantitative metric were always applied such as a 51% equity stake
- Many problematic potential acquisitions by Chinese companies have been stopped

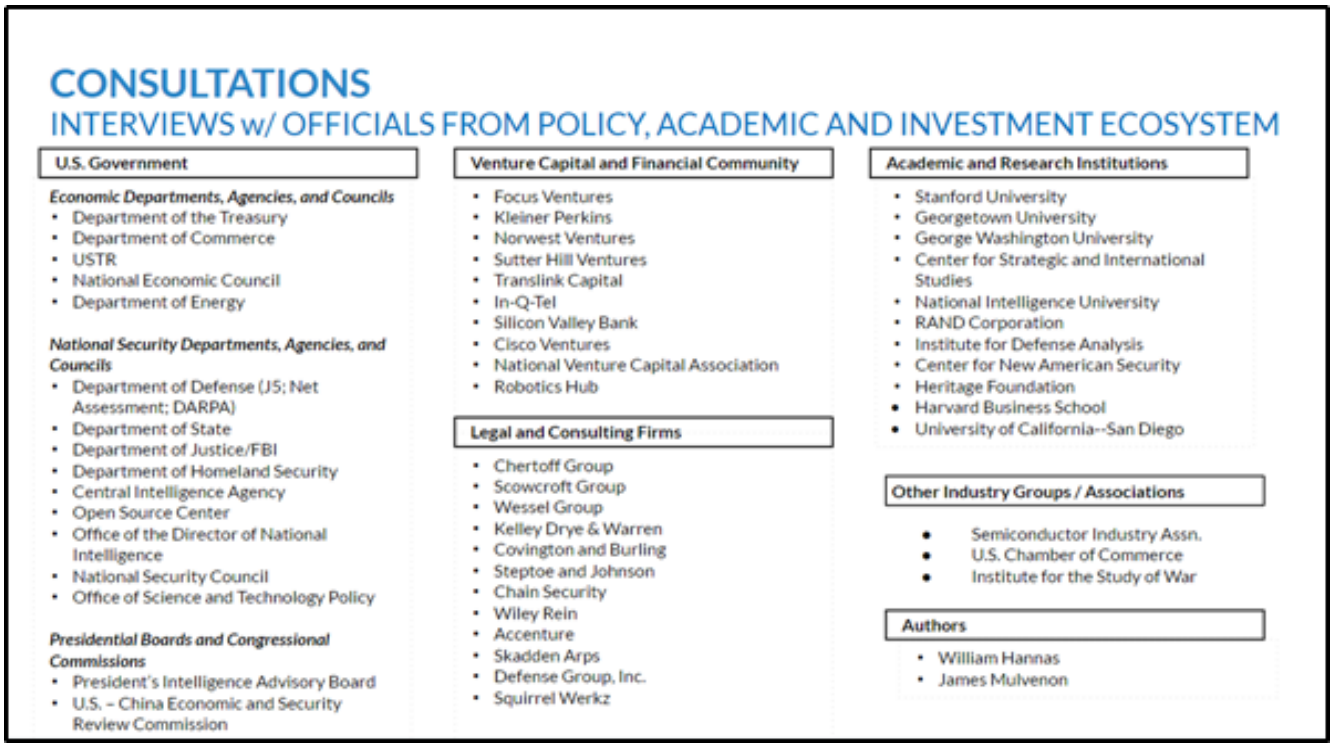
Weaknesses

- CFIUS reporting is voluntary--transactions do not have to be reported
- There are many types of technology transfer ***not*** currently covered by CFIUS
    - Joint ventures where the U.S. company contributes IP/technology rather than an entire business
    - Technology licenses
    - Private company transactions that are "below the radar"
    - Minority investments that do not rise to the level of a "controlling interest"
    - Reverse mergers
    - Greenfield investments
    - Assets purchased from bankruptcies
- There's an inherent bias to develop mitigation agreements[118] to allow transactions to proceed but mitigation agreements are difficult to construct and enforce. Mitigation agreements lock companies into uncompetitive cost structures; these are too often designed under time pressure resulting in one-of-a-kind agreements or agreements which are far too comprehensive. There are no government resources assigned to monitor these agreements which undoubtedly means they are unenforced. The likelihood of a costly mitigation agreement also reduces the incentive for friendly foreign companies to acquire U.S. companies.
- There is no formal risk-scoring (by country and by sector) to create a transparent, scalable process to manage large numbers of transactions; expecting consensus among the 14 CFIUS agencies is unrealistic
- Security agencies (Department of Defense, Department of Justice, Department of Homeland Security) are not tasked to collaborate in articulating the national security risks of foreign investment in sensitive technology and facilities
- No comprehensive view of the technology landscape exists, and since CFIUS is only designed to review a single deal at a time, there is increased risk of damaging a complete sector critical to national security such as is happening in semiconductors[119]
- Allied governments' view of threats are not incorporated
- Required certification to Congress of "no unmitigated security threats" is unrealistic; with an increasing number of complex transactions there will be unmitigated security threats that evolve
- 90-day timeline defined by statute does not allow for dealing with more complex transactions
- CFIUS transactions are expanding to >150/year and there is no dedicated funding by Congress to support this effort; resources are stretched in every participating agency

[118] Mitigation agreements incorporate conditions that satisfy the national security risks such as governance measures, security requirements, separating a sensitive operation from the transaction or monitoring/verification mechanisms. From 2009-2011, roughly 8% of all cases reviewed resulted in mitigation agreements. "Understanding the CFIUS Process," Organization for International Investment.

[119] "Ensuring Long-Term U.S. Leadership in Semiconductors," President's Council of Advisors on Science and Technology, January 2017

Appendix 12: Consultations



About the Authors

Michael Brown is a White House Presidential Innovation Fellow working with DIUx.

Through August of 2016, Michael was the CEO of Symantec Corporation, the global leader in cybersecurity. During his tenure as CEO (2014-16), he led a turnaround as the company developed a new strategy focused on its security business, sold its Veritas business, hired a new executive team, formed business units, improved operating margins and articulated a new culture fostering innovation. Michael served on the Symantec Board from 2005 until 2016.

Michael is the former Chairman and CEO of Quantum Corporation (1995-2003), a leader in the computer storage industry specializing in backup and archiving products. As CEO of Quantum, the company achieved record revenues as the world's leader in disk drives for PCs and the world's largest tape drive business. Michael joined Quantum in 1984 and served in various management roles before being named as CEO in 1995. Michael served on the Quantum Board from 1995 until 2014.

Michael has also served as the Chairman of EqualLogic and Line 6 and has served on the public boards of Nektar Therapeutics, Maxtor Corporation, and Digital Impact. He serves on the Board of Trustees of the Berklee College of Music in Boston. He has a BA degree in economics from Harvard and an MBA from Stanford University.

Pavneet Singh has served in several roles on the National Security Council and National Economic Council at the White House and is a consultant with DIUx.

Most recently, he served as director of international affairs and managed the U.S.-China and U.S.-India economic relationships including serving as the NSC's lead director for the Asia Pacific Economic Cooperation (APEC) Leaders' Summit in Beijing and developing the President's economic deliverables for the bilateral summit with Chinese President Xi Jinping.

From 2011 to 2013, Pavneet was the senior advisor to the Deputy National Security Advisor Mike Froman and provided strategic and policy guidance across a portfolio that included trade, energy, climate, exports and managing the U.S. economic relationships with emerging economies. Prior to the White House, Pavneet worked as an analyst at the World Bank and at the Brookings Institute. Pavneet earned his master's with distinction in international relations at Georgetown University and his undergraduate degrees in business administration and political economy from UC-Berkeley.

List of Sources

Venture Data sourced from CBInsights and Rhodium Group

"China vs. U.S. Patent Trends: How Do the Giants Stack Up?" Technology & Patent Research.

"The Rise of Chinese Investments in U.S. Tech Startups." CBInsights Blog and Webinar, December 2, 2016.

Hanemann, Thilo and Rosen, Daniel. "Chinese Investment in the United States; Recent Trends and the Policy Agenda." Rhodium Group Report, December 9, 2016.

Hanemann, Thilo; Rosen, Daniel; Gao, Cassie. "Two-Way Street: 25 Years of U.S.-China Direct Investment." Rhodium Group and the National Committee on US-China Relations. November, 2016.

Reports

2016 Fact Sheet, Stockholm International Peace Research Institute (SIPRI)

2016 Report to Congress of the U.S.-China Economic & Security Review Commission. November, 2016.

"2016 Special 301 Report." Office of the United States Trade Representative. April, 2016.

"APT1: Exposing One of China's Cyber Espionage Units." Mandiant Report. 2013.

"A 21st Century Science, Technology & Innovation Strategy for America's National Security." Committee on Homeland National Security of the National Science & Technology Council. May, 2016.

Adams, Donisha and Bernstein, Rachel. *Science*. November 21, 2014.

Cheung, Tai Ming; Mahnken, Thomas; Seligsohn, Deborah; Pollpeter, Kevin; Anderson, Eric; Yang, Fan. "Planning for Innovation: Understanding Chain's Plan for Technological, Energy, Industrial and Defense Development." Prepared for the US-China Economic and Security Review Commission by the University of California Institute on Global Conflict and Cooperation (IGCC). 2016.

"China Unveils Internet Plus Action Plan to Fuel Growth." The State Council for the People's Republic of China. *Xinhua*. July 4, 2015.

Cornell University, INSEAD and WIPO. "The Global Innovation Index 2016: Winning With Global Innovation." 2016.

Desilver, Drew. "Growth from Asia Drives Surge in U.S. Foreign Students." Pew Research Center. June 18, 2015.

"Ensuring Long-Term U.S. Leadership in Semiconductors." President's Council of Advisors on Science and Technology (PCAST). January, 2017.

Felton, Ed and Lyons, Terah. "The Administration's Report on the Future of Artificial Intelligence." *White House Blog.* October 12, 2016

"Hidden Lynx--Professional Hackers for Hire." *Symantec Official Blog*. September 17, 2013.

"Historical Trends in Federal R&D." American Association for the Advancement of Science. October 13, 2016.

"How America's Giants Are Aiding China's Rise." *Geo-political Standpoint Report 84*. Tangent Link. October 13, 2016.

Hughes, Brian D. "Protecting U.S. Military's Technical Advantage" presented at the 18th Annual NDIA Systems Engineering Conference in Springfield, VA. October 28, 2015.

"The IP Commission Report: The Report on the Theft of American Intellectual Property." National Bureau of Asian Research. May, 2013.

Kraemer, Jackie and Craw, Jennifer. "Statistic of the Month: Engineering and Science Degree Attainment by Country." National Center on Education and the Economy. May 27, 2016.

"M&A in the U.S." Institute for Mergers, Acquisitions & Alliances.

"The Military Balance." International Institute for Strategic Studies (IISS). 2016.

"National Outline for Medium and Long-Term Talent Development (2010-2020)." Xinhua Domestic Service. June 6, 2010.

Nichols, Gregory. "National Security Risks of Emerging Technologies." Homeland Defense and Security, Information Analysis Center. November 15, 2016.

O'Neill, Joseph P. "Economic and S&T Intelligence Collection." November 28, 2016.

"The OPM Breach: How the Government Jeopardized our National Security for More than a Generation." Committee on Oversight & Government Reform, US House of Representatives, 114th Congress. September 7, 2016.

"Project Atlas." Institute of International Education. Fall, 2015.

"Quantum Leap: Who Said China Couldn't Invent?" *Geo-political Standpoint, Report 85*. Tangent Link. October 14, 2016.

"Special Reports: Economic Impact of International Students." Institute of International Education. 2016.

"Startups Nation" from the Tech Code website.

"Survey of Graduate Students and Postdoctorates in Science & Engineering." National Science Foundation. November, 2015.

"Understanding the CFIUS Process." Organization for International Investment

"Understanding the U.S.-China Trade Relationship." Prepared for the US-China Business Council by Oxford Economics. January, 2017.

"The U.S. Leads the World in R&D Spending," The Capital Group Companies. May 9, 2016.

"U.S. China Trade Facts." Office of the United States Trade Representative. 2016.

"U.S. Treasury Issuance--Gross and Net." Securities Industry and Financial Markets Association. 2016.

Books and Articles

Areddy, James T. "U.S.-China Investment Flows Bigger than Thought." *Wall Street Journal*. November 17, 2016.

Auslin, Michael R. *The End of the Asian Century*. New Haven: Yale University Press, 2017.

Autor, David H.; Dorn, David; Hanson, Gordon H. "The China Shock: Learning from Labor Market Adjustments to Large Changes in Trade." *National Bureau of Economic Research (NBER) Working Paper 21906*. January, 2016.

Bader, Jeffrey. *Obama and China's Rise: An Insider's Account of America's Asia Strategy.* Washington: Brookings Institution Press, 2011.

Baker, Stewart. *Skating on Stilts*. Stanford, California: Hoover Institution Press, 2013.

Buckley, Chris. "China Passes Antiterrorism Law that Critics Fear May Overreach." *The New York Times*. January 6, 2016.

Bymer, Maj. Loren. "Virtual Reality Used to Train Soldiers in New Training Simulator." *US Army News & Information*. August 1, 2012

Carter, Ben. "Is China's Economy Really the Largest in the World?" *BBC News*. December 16, 2014.

Chan, Cathy. "Chinese Private Equity Funds are Taking on the World's Giants." *Bloomberg News*. July 20, 2016.

Chang, Lulu. "China Outlines its Latest FYP Called Internet Plus." *Digital Trends*. March 6, 2016.

Chin, Josh and Dou, Eva. "China's New Cybersecurity Law Rattles Foreign Tech Firms." *Wall Street Journal.* November 7, 2016.

Dwoskin, Elizabeth. "China Is Flooding Silicon Valley with Cash." *Washington Post*. August 6, 2016.

Fallows, James. "China's Great Leap Backward." *The Atlantic*. December, 2016.

Hannas, William C.; Mulvenon, James and Puglisi, Anna B. *Chinese Industrial Espionage*. New York: Routledge, 2013.

Harris, Shane. "FBI Probes 'Hundreds' of China Spy Cases." *The Daily Beast*, July 23, 2015.

Jesjardins, Jeff. "China vs. United States: A Tale of Two Economies." *Visual Capitalist*. October 15, 2015.

Johnson, Jeffrey Z. "Chinese Investment in the U.S.: Impacts and Issues for Policy Makers." Testimony before the US-China Economic and Security Review Commission. January 26, 2017.

Kennedy, Scott. "Critical Questions Made in China 2025." Center for Strategic and International Studies (CSIS). November 7, 2016.

Knake, Robert. "Five Chinese Cyber Attacks that Might Be Even Worse than the OPM Hack." *Defense One*. June 15, 2015.

Lanman, Scott. "China's Holdings of U.S. Treasuries Fall to Lowest Since '13." *Bloomberg News*. September 15, 2016.

Li, Cheng. *Chinese Politics in the Xi Jinping Era*. Washington: Brookings Institution, 2016.

Lieberthal, Kenneth. *Managing the China Challenge: How to Achieve Corporate Success in the People's Republic*. Washington: Brookings Institution Press, 2011.

Liyan, Xu and Jing, Qiu. "Beyond Factory Floor: China's Plan to Nurture Talent." *Yale Global Online*. September 10, 2012.

Longhurst, John. "Car Wars: Beijing's Winning Plan." November, 2016.

Manjoo, Farhad. "Make Robots Great Again." *The New York Times*. January 26, 2017.

Markoff, John and Rosenberg, Matthew. "China Gains on the U.S. in the Artificial Intelligence Arms Race." *The New York Times.* February 3, 2017.

Mingfu, Liu. *The China Dream: Great Power Thinking and Strategic Posture in the Post-American Era.* New York: CN Times Books, 2015.

Nakashima, Ellen. "Confidential Report Lists U.S. Weapons Systems Designs Compromised by Chinese Cyberspies." *Washington Post*. May 27, 2013.

Navarro, Peter W. *Death by China*. Upper Saddle River, New Jersey: Pearson Prentice Hall, 2011.

Philipp, Joshua. "Rash of China Spy Cases Shows a Silent National Emergency." *The Epoch Times*. April 25, 2016.

Pillsbury, Michael. *The Hundred-Year Marathon*. New York: St. Martin's Griffin, 2016.

Raska, Michael. "Scientific Innovation and China's Military Modernization." *The Diplomat*. September 3, 2013.

Rauhala, Emily. "America Wants to Believe China Can't Innovate. Tech Tells a Different Story." *Washington Post.* July 19, 2016.

Rogin, Josh. "NSA Chief: Cybercime Constitutes the 'Greatest Transfer of Wealth in History'. " *Foreign Policy Magazine*. July 2012.

Rogin, Josh. "The Top 10 Chinese Cyber Attacks (that We Know of)". *Foreign Policy Magazine*. January, 2010.

Roth, Erik; Seong, Jeongmin; Woetzel, Jonathan. "Gauging the Strength of Chinese Innovation." *McKinsey Quarterly*. October, 2015.

Schell, Orville and Delury, John. *Wealth and Power: China's Long March to the Twenty-First Century.* New York: Random House, 2014.

Scott, Malcolm and Sam, Cedric. "China and the U.S.: Tale of Two Giant Economies." *Bloomberg News*. May 12, 2016.

Stowsky, Jay. "The Dual-Use Dilemma" *Issues in Science and Technology*, Volume XIII, Issue 2, Winter, 1997.

Swanson, Ana. "Gold Rush: Chinese Tech Companies Invest Overseas." *CKGSB Knowledge*. April 20, 2105.

Thibodeau, Patrick. "China Builds the World's Fastest Supercomputer without U.S. Chips." *Computerworld*. June 20, 2016.

Thornburgh, Nathan. "Inside the Chinese Hack Attack." *Time.* August 25, 2005.

"Top 7 Worst Cyber Attacks in History." *Future Technology News*. September 23, 2010.

Trivedi, Anjani. "Subsidies Figure Big in China's New World." *Wall Street Journal*. November 17, 2016.

Tromblay, Darren E. and Spelbrink, Robert G. *Securing U.S. Innovation: The Challenge of Preserving a Competitive Advantage in the Creation of Knowledge.* Lanham, Maryland: Rowman & Littlefield, 2016.

Wei, Lingling. "China Issuing 'Strict Controls' on Overseas Investment." *Wall Street Journal*. November 26, 2016.
Wei, Lingling. "China's Overseas Funding to Shrink." *Wall Street Journal*. January 14, 2017.

"Xi Sets Targets for China's Science, Technology Progress." *Xinhua*, May 30, 2016.

Yang, Steven. "China Said to Mull Scrutiny of U.S. Firms If Trump Starts Feud." *Bloomberg News*. January 6, 2017.

Yuan, Li. "Chinese Technology Companies, including Baidu, Invest Heavily in AI Efforts." *Bloomberg News*. August 24, 2016.

Yuan, Li. "China Races to Tap Artificial Intelligence." *Wall Street Journal*. August 24, 2016.

Zhang, Yunan. "Chinese Government's Path to Silicon Valley." *The Information*. January 25, 2017.