Defense Innovation Unit Experimental (DIUx)

China's Technology Transfer Strategy:

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

Updated with 2016 and 2017 Data

Michael Brown and Pavneet Singh

January 2018

UNCLASSIFIED

DEFENSE INNOVATION UNIT EXPERIMENTAL

Silicon Valley | Boston | Austin | Washington D.C.

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 10-16% of all venture deals (2015-2017)** and has grown quite rapidly in the past seven years. The technologies where China is investing are the same ones where U.S. firms are investing and that will be foundational to future innovation: artificial intelligence, autonomous vehicles, augmented/virtual reality, robotics and blockchain technology. Moreover, these are some of the same technologies of interest to the U.S. Defense Department to build on the technological superiority of the U.S. military today. The rapidity at which dual-use technologies are developed in the commercial sector has significant impact on the nature of warfare; mastering them ahead of competitors will "ensure that we will be able win the wars of the future".[2]

Because the U.S. economy is open, foreign investors, including those from China, are able to invest in the newest and most relevant technologies gaining 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 nor the potential transfer of early-stage technology. 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 in protecting national security since its jurisdiction is limited. The other principal tool to inhibit technology transfer is the U.S. export control regime. 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, a long process where cooperation is not assured.

Further, 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.

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 the battlefield (the Second Offset). Much of this technology came from research sponsored by the U.S. government and

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

[2] The 2018 National Defense Strategy recognizes the critical role of technology development in the commercial sector for national security purposes: "The drive to develop new technologies is relentless, expanding to more actors with lower barriers of entry, and moving at accelerating speed. New technologies include advanced computing, "big data" analytics, artificial intelligence, autonomy, robotics, directed energy, hypersonics, and biotechnology—the very technologies that ensure we will be able to fight and win the wars of the future. The fact that many technological developments will come from the commercial sector means that state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our nation has grown accustomed. Maintaining the department's technological advantage will require changes to industry culture, investment sources, and protection across the National Security Innovation Base." p. 3

the Defense Department specifically. However, the technologies which will create the Third Offset are to a large extent being developed by early-stage technology companies with significant 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 strategic competition3 with China is a long-term threat rather than a short-term crisis, preserving our technological superiority and economic capacity are important issues for national focus today.

Key Points

- China is executing a multi-decade plan to transfer technology to increase the size and value-add of its economy, currently the world's 2nd largest. By 2050, China may be 150% the size of the U.S.[4] and decrease U.S. relevance globally[5].
- Technology transfer to China occurs in part through increasing levels of investment and acquisitions of U.S. companies. **China participated in ~16% of all venture deals in 2015 up from 6% average participation rate during 2010-2015.**
- **China is investing in the critical future technologies that will be foundational for future innovations 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 with 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.[6]
  - 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 25% of U.S. 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 U.S. 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 is clear in its aims of import substitution and technology innovation.
- There are several 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. CFIUS is only partially effective in protecting national security given its limited jurisdiction.

- **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 specific 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.
  - China's targeted investments to close the gap in capabilities between its military and the U.S. military.
  - 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[7]).

[3] As discussed in the summary of the 2018 National Defense Strategy, the central challenge to U.S. prosperity and security is the "reemergence of long-term strategic competition" by revisionist powers such as China and Russia.

[4] According to The Economist, 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).

[5] The U.S. has not competed with an economic rival that could be larger than its own economy in 150 years.

[6] "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

[7] Joint Acquisition Protection & Exploitation Cell, described on p. 12 of this paper.

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) is growing rapidly and is at a record level in a range of $200-250 billion, with $213 billion in announced acquisitions in 2016.[8,9] 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.[10] 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 as well as a motivation for companies and individuals to diversify their investments geographically and politically as well as hedge against currency fluctuations. With the recent concerns about devaluation of the currency relative to the U.S. dollar and concerns about the underlying economic fundamentals, Chinese investors have made more investments overseas and this has led to an increased level of capital controls.[11]

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 U.S. has not been the largest economy since it overtook the U.K. in 1872.[29] Since the U.S. 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 U.S. GDP within the next decade)[30]. The time scale during which this growth occurred is stunning as China's economy has grown from 10% of the U.S. 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.

China plans to further transform its economy through a national focus on technology and indigenous innovation with a goal of import substitution. 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[31, 32] , and e-commerce[33]. 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[34]. 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 transfers and the Great Firewall which enables control over the content and flow of data on the internet. 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."[35] 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." [36]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.)

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

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

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

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

[33] 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.

[34] 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)

- **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 prioritized sectors include advanced information technology, automated machine tools and robotics, aerospace and aeronautical equipment, maritime equipment and high tech shipping and biopharma and advanced medical products.[37]
- **13th Five Year Plan of 2016-2020 "Internet Plus"**[38] 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[39]:
  - 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[40] to focus on specific innovations. These areanalogous 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 more than copying technology – China is making progress on President Xi's goal to become one of the most innovative economies by 2020:

- **Micius Quantum Communications 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 many existing encryption methods (based on factoring).
- **Sunway TaihuLight 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.[41]

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

[36] "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

[37] 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.

[38] "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

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

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

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

- **Cruise Missile Incorporating Artificial Intelligence.** 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.[42]
- **Consumer Drones.** DJI's (Da-Jiang 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 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.[43]

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."[44]

By some measures of innovation, China is already leading and 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).[45]
- 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.[46]
- 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.[47] 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.[48]

To assess the comparative innovation capability between China and the U.S., McKinsey recently analyzed the industries where China has an innovation lead.[49] In traditional manufacturing industries where low costs provide a competitive advantage, China leads in innovation 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

42 John Markoff and Matthew Rosenberg, "China Gains on the U.S. in the Artificial Intelligence Arms Race," The New York Times (February 3, 2017); and Lei Zhao, "Nation's next generation of missiles to be highly flexible," China Daily (August 19, 2016)

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

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

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

46 Hannas, William C.; Mulvenon, James and Puglisi, Anna B. China Industrial Espionage. New York: Routledge, 2013. Chapter 3

47 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

48 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

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

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 DJI 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."[50] And in the field of advanced industrial robotics, China is leveraging its market and investment capital to ultimately lead in the design and manufacture of robots.[51] 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. A further concern is that China's long-term, national focus on innovation and expertise in advanced manufacturing might make China a more attractive destination market for new technologies--especially hardware technologies--since there is both less funding appetite in the U.S. for non-software technologies and less of an ecosystem for developing and manufacturing these technologies.

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 eight 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.[52] 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

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

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

[52] 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

components of the U.S. military aircraft supply chain.[53] 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.[54]
4. China's investment strategy (through venture and private equity investments as well as acquisitions) includes 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 U.S.-based innovation in the same areas and at the same time which could negate 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 technology) complements the increase in military spending as China gains experience in manufacturing and refining new technologies for practical use.
6. DoD does not currently have agreed-upon emerging technologies the U.S. must protect although there has been extensive work on export controls to protect technology products from being shipped to U.S. adversaries.

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.[55] However, there is much work left to do to consolidate the technologies across DoD requiring protection and determine which of those are the most critical. 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 agreed-upon emerging technologies to protect 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 and resource allocation to thwart industrial espionage or cyber theft.

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

[54] The IP Commission Report (2013)

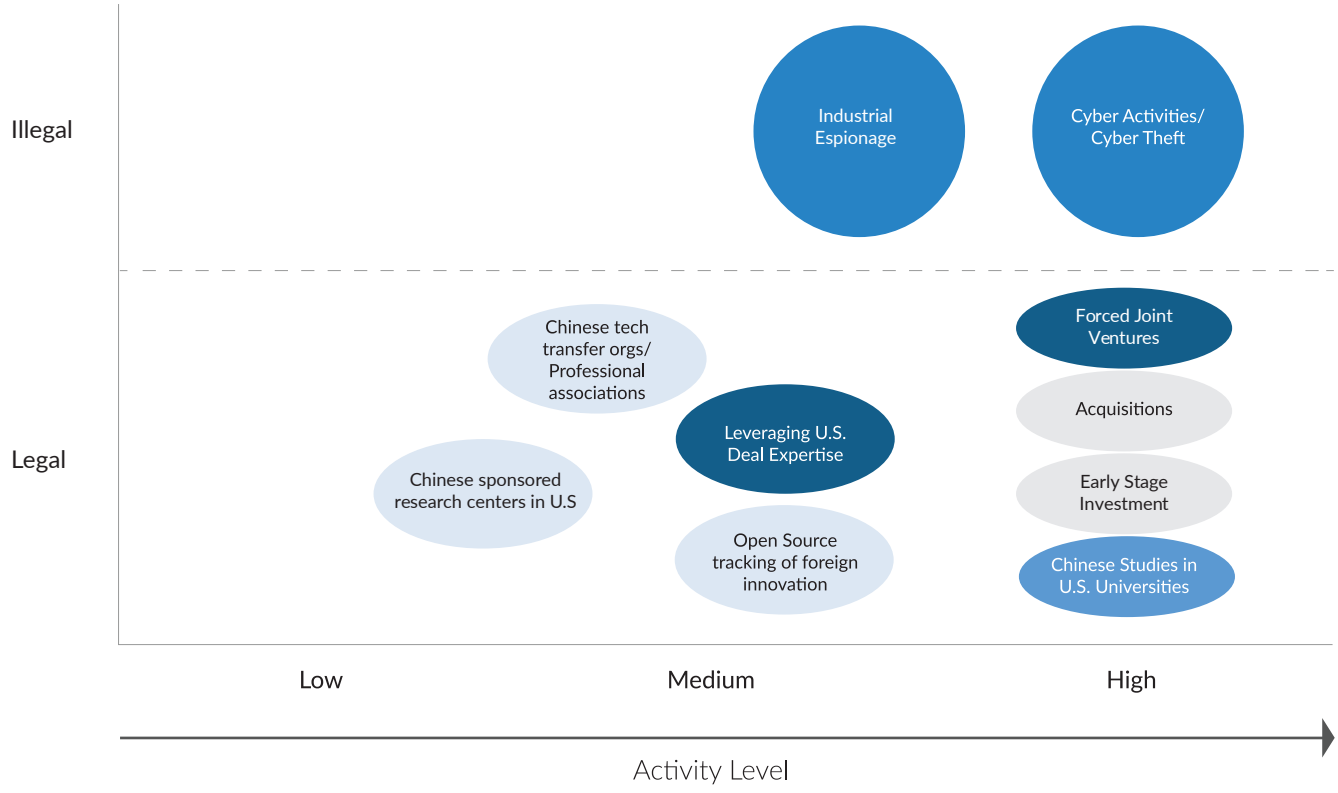
[55] Brian D. Hughes, "Protecting U.S. Military's Technical Advantage" presented at the 18th Annual NDIA Systems Engineering Conference in Springfield, VA, October 28, 2015. Retrieved at http://www.acq.osd.mil

China's Multiple Vehicles for Technology Transfer

Given the authoritarian nature of China's government, China can 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.

Vehicles for Chinese Technology Transfer from the U.S.



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 i*n 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) where they become "insiders" and 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.

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 the 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]

[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.

[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)

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 especially at the undergraduate level.

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

- 84% of foreign students in PhD programs were studying in science and 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 were 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

[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.

[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

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]

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 Human Resources and Social Security[71] 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.

[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

[71] Formerly known as the Ministry of Personnel.

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.[72]

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.[73] 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.
   - A new type of research center is TechCode: 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.[74]
   - In addition, there are several 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 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 [zero] for… legal, illegal and quasi-legal practices that fall just below the thresholds set by U.S. law."[75] With these professional associations being one of the primary targets, 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

[72] Hannas, China Industrial Espionage, Chapter 4

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

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

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

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.[76] 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.[77]

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.[78]

8. **Leveraging technical expertise of U.S. private equity, venture firms, investment banks and law firms**
As China has invested more in the U.S., its investment entities have enhanced their deal expertise 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 three years, the level of deal expertise has increased considerably.

[76] 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

[77] Hannas, China Industrial Espionage, Chapter 5.

[78] 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." as quoted in Pillsbury's The Hundred-Year Marathon. Given a history of trying to influence the curriculum of Chinese history and Chinese studies at colleges, there are now a number of colleges which are disbanding these institutes.

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 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 show 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.[79] 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 them 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 put Alibaba in a better position to later make an offer for the technology or the company.[80] Thus, through a combination of technology transfer vehicles, China can achieve more than 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 and network equipment (to benefit global champions Huawei and ZTE), information security, semiconductors, media and 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." [81]

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

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

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

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.**[82] 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 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 In 2017, Senators Cornyn (R-TX) and Feinstein (D-CA) introduced the Foreign Investment Risk Review Modernization Act (FIRRMA) which expands CFIUS' jurisdiction to cover the key transaction types beyond acquisition which might result in technology transfer. This legislation has broad support within the Administration including public statements by the White House, Secretaries of Defense, Treasury, Commerce and the Attorney General.

   The workload for CFIUS is increasing rapidly. CFIUS reviews about 150 transactions per year but this is rising. 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 so this critical process must be handled within existing agency budgets. The proposed FIRRMA legislation recognizes the need for increased resources to handle a growing CFIUS caseload. A review of strengths and weaknesses of the current CFIUS process are included as Appendix 10.

[82] 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.

2. **Export controls** are designed to prevent sensitive technologies or products from being shipped to adversaries.[83] 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.[84] 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. Failure in effectiveness has largely been a function of not having the foresight to place these technologies on an export control list nor 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. However, since complying with export controls is a company's responsibility, there is a question of whether early-stage technology companies understand the controls or have resources within a trade compliance function to handle this complexity.

   While the restricted export lists (EAR and CCL76) 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 technologies or to investigate the relationship between investors and employees of a startup. Lastly, export controls will 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.

[83] 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 U.S. 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.

[84] 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.

Appendix 8: Largest Chinese Cyber Attacks

- **Breach of more than two dozen major weapons system designs** 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[99]

- **"Titan Rain"** a series of coordinated attacks for multiple years since at least 2003 which compromised hundreds of government computers stealing sensitive information[100] " 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."[101]

- **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.[102]

- **"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[103]

- "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."[104]

- "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."[105]

[99] 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

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

[101] 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/

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

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

[104] 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.

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

- **"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."[106]

- **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.[107]

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

[107] "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: 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[108] 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

[108] 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.

- 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[109]
- 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

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