AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 115–126

EXAMINING THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES

HEARING

BEFORE THE

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS UNITED STATES SENATE

ONE HUNDRED FIFTEENTH CONGRESS

FIRST SESSION

ON

EXAMINING THE ROLE OF THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES

SEPTEMBER 14, 2017

Printed for the use of the Committee on Banking, Housing, and Urban Affairs

Available at: http://www.govinfo.gov/

U.S. GOVERNMENT PUBLISHING OFFICE

28–033 PDF WASHINGTON : 2018

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS

MIKE CRAPO, Idaho, *Chairman*

RICHARD C. SHELBY, Alabama
BOB CORKER, Tennessee
PATRICK J. TOOMEY, Pennsylvania
DEAN HELLER, Nevada
TIM SCOTT, South Carolina
BEN SASSE, Nebraska
TOM COTTON, Arkansas
MIKE ROUNDS, South Dakota
DAVID PERDUE, Georgia
THOM TILLIS, North Carolina
JOHN KENNEDY, Louisiana

SHERROD BROWN, Ohio
JACK REED, Rhode Island
ROBERT MENENDEZ, New Jersey
JON TESTER, Montana
MARK R. WARNER, Virginia
ELIZABETH WARREN, Massachusetts
HEIDI HEITKAMP, North Dakota
JOE DONNELLY, Indiana
BRIAN SCHATZ, Hawaii
CHRIS VAN HOLLEN, Maryland
CATHERINE CORTEZ MASTO, Nevada

GREGG RICHARD, *Staff Director*
MARK POWDEN, *Democratic Staff Director*

ELAD ROISMAN, *Chief Counsel*
JOHN O'HARA, *Chief Counsel for National Security Policy*
KRISTINE JOHNSON, *Professional Staff Member*

ELISHA TUKU, *Democratic Chief Counsel*
LAURA SWANSON, *Democratic Deputy Staff Director*

DAWN RATLIFF, *Chief Clerk*
CAMERON RICKER, *Deputy Clerk*
JAMES GUILIANO, *Hearing Clerk*
SHELVIN SIMMONS, *IT Director*
JIM CROWELL, *Editor*

C O N T E N T S

THURSDAY, SEPTEMBER 14, 2017

	Page
Opening statement of Chairman Crapo	1
Opening statements, comments, or prepared statements of:	
Senator Brown	2

WITNESSES

Clay Lowery, Managing Director, Rock Creek Global Advisors, and Former Assistant Secretary for International Affairs, Department of the Treasury	4
Prepared statement	29
Responses to written questions of:	
Senator Brown	38
Senator Menendez	39
Kevin J. Wolf, Partner, Akin Gump Strauss Hauer & Feld LLP, and Former Assistant Secretary for Export Administration, Department of Commerce	6
Prepared statement	32
Responses to written questions of:	
Senator Brown	40
Senator Menendez	43
James A. Lewis, Senior Vice President, Center for Strategic and International Studies	8
Prepared statement	34
Responses to written questions of:	
Senator Brown	45
Senator Menendez	46

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

Statement submitted by the Rail Security Alliance	47
Letter submitted to the Trump administration on Chinese Equity Caps Financial Services Sector	54
China's Technology Transfer Strategy	57

EXAMINING THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES

THURSDAY, SEPTEMBER 14, 2017

U.S. SENATE,
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS,
Washington, DC.

The Committee met at 10:02 a.m., in room SD–538, Dirksen Senate Office Building, Hon. Mike Crapo, Chairman of the Committee, presiding.

OPENING STATEMENT OF CHAIRMAN MIKE CRAPO

Chairman CRAPO. This hearing will come to order.

This morning, the Committee will receive testimony on the role of the Committee on Foreign Investment in the United States, or CFIUS, as it is known in the trade.

The role of CFIUS is to review certain types of foreign investment transactions to determine if there is: a threat to impair U.S. national security; a foreign investor present which is controlled by a foreign Government, like a State-owned enterprise; or something that can affect homeland security or result in control of any critical infrastructure that might impair our national security.

Yesterday's rejection of the acquisition of Lattice Semiconductor by a Chinese consortium with a U.S. presence provides a good example of that role.

According to press reports, the CFIUS review of the deal revealed that Lattice had valuable intellectual property that, if somehow transferred, would impair U.S. national security.

The purchaser was a Chinese consortium with strong ties to the Chinese Government and its space program. Additionally, the importance of the semiconductor supply chain integrity to homeland security and the use of Lattice's products by the U.S. Government was something that could further impair national security.

The Lattice case sounds like it should be considered textbook CFIUS, and it is reassuring that the President made this decision based on the careful due diligence of the various Government entities that comprise CFIUS.

Nonetheless, there are some congressional and Administration concerns over a broad-based set of potential risks arising from China's steadily increasing use of foreign direct investment, or FDI, to acquire companies and their sensitive technology in the United States.

We need to have a general discussion of whether or not the CFIUS process is functioning appropriately, to the extent that it

has sufficient authority to look at the transactions that are affected most by today's evolving national security considerations.

I look forward to hearing from the witnesses to what extent this concern is based on China's 2025 strategy and if there are any specific instances where this strategy has threatened to impair U.S. national security.

In that regard, I will be looking for the witnesses to identify and articulate the potential national security considerations at issue and their relevance to any attempt to address them through reform of CFIUS legislative or regulatory authorities.

If CFIUS is not looking at or is somehow missing transactions worthy of its national security review, I would also be interested in learning how many and what types of cases it is missing beyond the 250 or so CFIUS filings this year and what human financial resources would be necessary to review such new cases.

We should also discuss whether CFIUS is even the right agency to reform in order to address various complaints associated with China's investment strategies today.

The magnitude of any problem with CFIUS is defined by the intersection of U.S. national security with huge inflows of foreign capital supported by a world-renowned U.S. open investment policy.

The United States—with $7 trillion in total outward FDI and $6.5 trillion in inward FDI—is the world's number one investor overseas and the world's number one recipient of foreign investment.

FDI plays an essential role in increasing U.S. economic growth, creating highly compensated jobs, and spurring innovation and promoting exports.

Generally, it is in the national interest of the United States to sustain an open investment policy. The administrations of Presidents Reagan, Bush, Clinton, Bush again, and Obama have all reaffirmed the open investment policy of the United States. Likewise, Congress is a firm believer, on a bipartisan basis, in an open investment policy.

But with this unique position that the United States enjoys in the world comes a responsibility to assure that the national security of the United States is maintained against investments that may seek to undermine it.

CFIUS plays a critical role and it is important to have a Senate-confirmed individual to set policy and work with Congress. The Senate needs to quickly confirm Heath Tarbert as the Assistant Secretary of the Treasury for International Markets and Development.

Mr. Tarbert, who was voice-voted out of the Banking Committee in May, is the President's key person to oversee national security policy at CFIUS and also maintain a healthy, robust investment environment for the United States.

Senator Brown.

OPENING STATEMENT OF SENATOR SHERROD BROWN

Senator BROWN. Thank you, Mr. Chairman, and I appreciate your comments always, and this panel will be very helpful to us. Thank you.

As you know, Mr. Chairman, I supported, as almost every Member of this Committee did, Mr. Tarbert out of the Committee. I hope, too, he can be confirmed quickly. I do want to remind my colleagues, especially Senators like Senator Perdue and Senator Schatz, who are newer to this Committee, that so far this year the full Senate has already confirmed 11 times the number of nominees from the Banking Committee as this Committee confirmed in the last Congress. So we have confirmed 11 times the number of nominees from this President than this Committee did last session. Senator Tester remembers that well. Senator Crapo remembers that. So just a note to make.

Mr. Chairman, as is evidenced by the Committee's focus on Russia, Iran, and North Korea sanctions already this year, national security issues are more important than ever.

It makes sense that we should take a look at other national security issues in this Committee's jurisdiction, like CFIUS.

CFIUS is charged with reviewing certain foreign acquisitions of U.S. companies that potentially pose national security threats. It has been a decade since we have had a hearing, so I am particularly grateful to Chairman Crapo on this topic.

The U.S. continues to be one of the most attractive markets for foreign investment. We know that. Our country welcomes investment when it is part of a straightforward business deal. When they are done right, these deals can create jobs; they can grow American industries.

But we know it is not always that simple. Some transactions have national security as well as commercial implications. CFIUS has seen an increase in its reviews of Chinese acquisitions of U.S. companies. In the three most recent reported years, CFIUS reviews of Chinese acquisitions topped the list every single time.

In 2016, Chinese companies invested a total of $51 billion into the U.S. through 65 deals, a 360-percent surge from 2015. This year, it is already clear that CFIUS's workload has increased—with acquisitions from China and other Nations.

I have serious concerns about many of China's economic and industrial policies. That is not to say that every Chinese investment poses national security threats. Fuyao Glass invested in Moraine, Ohio, where there was once a GM plant. It is an example of a project which poses no such threat and is creating jobs.

Some foreign investments pose national security threats, such as intellectual property theft and espionage from U.S. industries crucial to our Nation's defense, as well as threats to the intellectual property of seeds potentially impacting the global food supply, and transfers of critical technologies. We have seen an increase in smaller private investments to obtain access to new technological know-how.

We do not know yet who perpetrated the hack of Equifax—exposing the personal information of 143 million Americans, essentially half our population. It could be domestic, it could be foreign criminals. But we do know that some foreign Governments and companies have tried to gain access to sensitive information about Americans and pose other cybersecurity concerns. That has to be considered as well. I will not even go into all the discussion about the

Russians last year. These are the types of threats we hear about from the national security agencies and others.

Today we have three people before the Committee who have extensive experience with CFIUS, with export controls, and with the other tools our Government uses to address national security threats. I look forward to their assessment how CFIUS is working, if its scope is appropriate—considering shifting national security threats—and if it has enough resources to review an increasing number of transactions and thoroughly investigate possible national security threats.

I would like the witnesses' opinions on the national security risks that I highlighted earlier, whether they believe it is, in fact, CFIUS's responsibility to try to address these risks, or if there are programs at the other national security agencies—DOD, Commerce, State, and others—that are better able to do that.

I do not think that CFIUS reform is the answer to addressing all of those national security risks, whether from China or elsewhere. But I am open to considering improvements to CFIUS if we believe there are resource concerns or gaps that are allowing certain investments that pose real threats to Americans to fall through the net, if you will.

Any solution is likely to be multifaceted, involving trade, economic, and defense policies, export controls, some of that in this Committee's jurisdiction, some of it outside.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you, Senator Brown.

And we will now turn to our panel for their testimony. We will hear from two former CFIUS officials: first, Mr. Clay Lowery from the Treasury Department, and then Mr. Kevin Wolf from the export control side of the Commerce Department. We will then turn to Mr. Lewis, who has long studied technology issues in the context of the CFIUS process at the Center for Strategic and International Studies, which published its 2-year review of the CFIUS process last December.

I remind our witnesses that we would like you to keep your oral comments to 5 minutes so we have plenty of time for questioning from the Senators, and your full written statements are already made a part of the record.

With that, Mr. Lowery, please begin.

STATEMENT OF CLAY LOWERY, MANAGING DIRECTOR, ROCK CREEK GLOBAL ADVISORS, AND FORMER ASSISTANT SECRETARY FOR INTERNATIONAL AFFAIRS, DEPARTMENT OF THE TREASURY

Mr. LOWERY. Thank you, Chairman Crapo, Ranking Member Brown, and Members of the Committee. Thank you for letting me testify today on examining CFIUS. In my testimony, I hope to briefly just touch on the nature of CFIUS and its processes, its performance over time, and some thoughts on CFIUS reform.

The easiest way to understand CFIUS is to know its mandate: ensure national security while promoting foreign investment. That is actually what the legislative language says. So when we read news stories about CFIUS, as will be the case today because of President Trump's blocking of a transaction yesterday, we only

hear about protecting national security. But that is only part of the objective of CFIUS. Promoting foreign investment is a part of our national security. It is core to our economic growth. It is core to our increasing productivity and for creating jobs. Thus, any reforms to CFIUS that are being considered should be thought about in that context.

CFIUS is an interagency Committee, chaired by Treasury, that includes a variety of members, including Defense, Justice, Commerce, the Intelligence Committee. It investigates cross-border mergers and acquisitions that could put our national security at risk.

M&A parties file with CFIUS, and CFIUS determines whether the acquirer will gain control of a U.S. business. If control is determined, CFIUS does a three-part analysis:

First, does the acquirer pose a national security threat?

Second, does the asset that is being purchased make our national security more vulnerable?

And, third, the consequences of permitting these threats and vulnerabilities to come together through this transaction, do they promote a specific risk to our national security?

CFIUS investigates this question for about 30 days. If at the end of those 30 days CFIUS is not satisfied, they can go to a second stage of investigation, which is up to 45 days, an additional 45 days. If CFIUS is still not satisfied, it can take the case to the President, who is the only one, not CFIUS, that can actually prohibit an acquisition. In the past 30 years, this has happened only four times, including yesterday.

Why is it so rare that the President blocks transactions? The first reason is most of these transactions do not raise national security risks. The second is, if they do, CFIUS has the ability to mitigate those risks. And the third is that if the President makes a decision like he did yesterday, it becomes public and puts the corporate reputation at risk, and so sometimes if you know that it is going to be a negative discussion by the President, you will withdraw and abandon your transaction.

In terms of mitigation agreements, these were put in place by Congress, and I view them as the pressure valve that enables CFIUS to find solutions to much more difficult transactions and to meet its mandate: welcoming foreign investment and protecting national security. Since Congress strengthened CFIUS 10 years ago, it has performed in an exceptionally professional and thoughtful manner. Scrutiny of cases is thorough. CFIUS protects information as well as anyone in the U.S. Government. And they have preserved the reputation of the United States to being open to investment from around the world.

That said, there is little question that the investment landscape has changed dramatically in 10 years. By far, the two most important changes have been the rise of China, as the Chairman said, and also the potential of new sensitive technology being transferred. Both Mr. Lewis and Mr. Wolf will elaborate on these issues.

These developments suggest that a close, sober evaluation by Congress, the GAO, and the Administration are in order, and as with any analysis, it is best to think of the potential reforms in a

cost-benefit analysis, including what are intended and unintended consequences.

Beyond that, I would take three more steps.

First, the CFIUS process, as Ranking Member Brown suggested, is currently under a lot of stress because of a significant increase in cases—many of them are complex—without a commensurate increase in resources.

Second, as Chairman Crapo mentioned, this Committee passed through in its bill back in 2007 a new Assistant Secretary for Treasury to oversee CFIUS. President Trump has nominated a highly qualified individual in Heath Tarbert. He was approved by this Committee with near unanimous support. He should be supported by the full Senate and let him get to work.

And, third, we should adopt a set of guiding principles to make sure that any CFIUS reform both safeguards our national security and remains the destination—keeps the United States the destination of choice for investment.

I have outlined a number of principles in my written testimony. I would just say three right now: minimize the opportunity for politicizing transactions; keep CFIUS narrowly focused on national security; and, third, increase the scrutiny of State-controlled cases.

Thank you very much.

Chairman CRAPO. Thank you, Mr. Lowery.

Mr. Wolf.

STATEMENT OF KEVIN J. WOLF, PARTNER, AKIN GUMP STRAUSS HAUER & FELD LLP, AND FORMER ASSISTANT SECRETARY FOR EXPORT ADMINISTRATION, DEPARTMENT OF COMMERCE

Mr. WOLF. Thank you, Chairman Crapo, Ranking Member Brown, and other Members of the Committee. Thank you also for convening this hearing to discuss an important national security topic.

I was last before this Committee in January of 2010 when you confirmed me as the Assistant Secretary of Commerce for Export Administration, which is a role I served in until January 20, 2017. And in that role, I worked with my colleagues primarily at the Departments of Defense and State in shepherding the U.S. export control system. And I was also a representative to CFIUS during that time.

Although I am now with a law firm, I am not speaking on behalf of any particular change or on behalf of anyone else. The views I discuss today are my own.

Mr. Lowery described well CFIUS and the background, so I will get straight to my main point, which is that the U.S. export control system and CFIUS complement each other. CFIUS has the authority to regulate the transfer of technology when there is a transaction, however you define "transaction." The export control rules have the authority to regulate the transfer of technology regardless of whether there is a transaction. This means that if there are specific concerns about particular types of technology or information, whether general or specific, whether as part or as a result of a CFIUS review or from any other source, then the focus, I respect-

fully submit, on addressing that national security issue should be on the transfer of the technology to the destination in question.

The U.S. export control system is perfectly suited for doing exactly that. Yes, I recognize it can be complex, but it is specifically designed to constantly evolve to new threats as they are identified, to change as a result of commercialization of technology and realizations about the effectiveness of other controls.

Now, in general, the most effective export controls are those that are multilateral—those that our allies impose to the same degree to accomplish a common objective. Unilateral controls—controls that only one country imposes—tend to be counterproductive because they create incentives for companies to simply do the work outside the United States, thus outside of U.S. control.

However, the temporary imposition of unilateral controls, when there is a specific threat or a new threat or an evolving threat identified, such as during a CFIUS review or in connection with some sort of acquisition, can be and is a very effective tool. And in the regulations administered by the Commerce Department's Bureau of Industry and Security, in coordination with the Departments of Defense and State, there is the ability to move quickly to respond to some of these threats, again, focusing on the technology itself to particular tailored destinations with or without any particular transaction, however you would define that.

These tools also can work very closely in connection with law enforcement resources to identify situations when there is a front company in the United States. And we can get into more details on some of these tools as well as how they work with the multilateral regime process.

So although I cannot get into specific cases, I can say that other types of national security issues created by foreign direct investment in my experience primarily were those involved with colocation issues, that is, acquisitions next to sensitive military facilities; those that create espionage risks; those that reduce the benefit of Defense Department technology investments; those that would reveal personal identifying information; those that create security of supply issues for the Defense Department and other parts of the U.S. Government; and those that create potential exposures for our infrastructure.

And so, in general, the CFIUS authorities in my experience in the agencies were well suited and well equipped to deal with these, its dedicated public servants working very hard. And that last point is the key. As mentioned earlier, they are stressed. They need help. They need assistance. And this is important not only for national security, but for our economic security so that the United States is known as a place that welcomes direct investment and can review the safe harbor process quickly and efficiently.

In my last couple of comments, it is focused on—when thinking about potential legislative change, my suggestion would be to first ask, What is there about the authority that cannot be addressed through changes in regulations or internal process, or if there is another area of law such as trade remedies or export controls that could be more suited to addressing the national security risks, or if the issue could be resolved through merely an increase in resources or change in resources in particular areas? If the answer

is no to those questions, then that is the sweet spot for statutory change.

Those who know me know I have a 3-minute and a 30-minute and a 3-hour version of every topic, so I will stop here and look forward to answering your questions.

Chairman CRAPO. Thank you, Mr. Wolf.

Mr. Lewis.

STATEMENT OF JAMES A. LEWIS, SENIOR VICE PRESIDENT, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

Mr. LEWIS. Thank you, Mr. Chairman, and I thank the Committee for this opportunity to testify. You have heard about how important CFIUS is, so I will not belabor the point. But the Committee, while it has done well in the past few years, faces a growing volume of cases, increased complexity of transactions, and Chinese industrial policies that pose an increasing challenge.

The U.S. created CFIUS in response to concerns that foreign competitors were acquiring strategic industries. CFIUS authorities were updated in 2007 in the Foreign Investment and National Security Act. That was 10 years ago. And it created new authorities for CFIUS and new timelines. FINSA is now 10 years old and faces challenges created by a changed global environment.

The most important of these comes from China, as you have noted. China seeks ways to circumvent CFIUS protections. China's goal is to end its dependence on foreign technology and to overtake the U.S.

If China followed international practices in trade, its decisions to invest in domestic industries would be unobjectionable. But China has not hesitated to extract technology or concessions or to block competition to advance its own firms. China has a strategy to build a high-tech economy and is willing to spend heavily to acquire foreign companies and the know-how they possess.

The fundamental issue for the U.S. is how to respond to a managed economy with a well-financed strategy to create domestic industries intended to displace foreign companies.

China appears to be attempting to circumvent CFIUS and export controls. Some important ideas for CFIUS reform include expanding the scope of covered transactions, particularly in regard to what are called "greenfield transactions," providing the Committee with extra flexibility for difficult cases by giving it the resources or support to better identify technology and business trends that create risk, finding ways to cooperate with foreign partners, and it is an indicator of how things have changed that now both Japan, Germany, and the European Union are adopting their own CFIUS-like processes. The Committee could use additional resources and information to make timely decisions.

U.S. efforts to get China to follow global norms on trade are long overdue, but it will not work without a strategy to promote U.S. technology. Reports that the Trump administration will challenge China over trade practices are good news, but it needs to be part of a larger strategy that includes export controls and investment in R&D.

It is important not to exaggerate China's strength. China faces immense problems, including its huge debt burden, pollution, and

corruption, but it does have a strategy, as you noted, in China 2025 to displace the U.S. and building globally dominant high-tech industries. However, China's leaders are practical, and their behavior can be changed if the U.S. develops a coherent strategy in cooperation with key allies. CFIUS is not the only tool we can use in this, but it is the most important for dealing with foreign investment, and the Committee could use additional authorities and resources.

I thank you for the opportunity to testify and look forward to your questions.

Chairman CRAPO. Thank you, Mr. Lewis, and I want to turn to you first with a couple of questions. In your testimony, you identify a number of concerns relating to China's industrial policy and transfers of U.S. technology. You also discuss how CFIUS may be improved to address some of the concerns while others may be better handled by export controls.

In your opinion, what changes specific to CFIUS authority are necessary to effectively protect U.S. national security? And what changes to the export control regime do you find necessary to prevent unwanted transfers of technology and know-how?

Mr. LEWIS. Thank you, Mr. Chairman. I think the most important issue for me remains the way that China has changed its investment policies to circumvent CFIUS, and the case that we all know the best is, of course, what we call "greenfield investments," which is Chinese companies opening facilities or subsidiaries in the United States. Those are not always covered. The Department of Defense put a report out on this some months ago. It was unclear to me why it was classified since, when you go to Silicon Valley, it is sort of an open secret that Chinese firms are all over the place trying to acquire brains, technology, trying to get around export controls and CFIUS. So I think the most important thing to look at is what are we doing about the alternate methods China has found to acquire technology.

Another good example might be Chinese companies, when they come to the U.S., do not face the same restrictions that American companies face when they attempt to do business in China. A word that the Chinese dislike is "reciprocity," so I think looking at the ways they circumvent, looking at greenfield investments, looking for reciprocity in investments would be a good approach for CFIUS.

For export controls, I recently had an unusual experience. I talked to one of the leading high-tech trade associations, and at the end of their briefing on their technologies, they said, "And we would like to see export controls strengthened." I said, "Wait a minute. You guys usually say the opposite. What is happening here?" And they said in some ways the control lists we have, both at State and Commerce, have not kept up with developments in technology and need to be updated. So I think the biggest change here would be to once again take a step back and look at the munitions list, the Commerce control list, and say, How do they need to be updated to reflect the current technological environment? This would help CFIUS as well.

Chairman CRAPO. Thank you.

Mr. Wolf, expanding on Mr. Lewis' response, would you please focus on any concern that transfers to China of foundational tech-

nologies present and what Congress and the Administration can do to address this?

Mr. WOLF. Sure, absolutely. The principal focus is to aggressively and with will think creatively about how to describe either in a unilateral fashion or a multilateral fashion the types of technologies that warrant control to China or other countries for these national security reasons. And the reason I put my emphasis there is because one should not have to wait for a transaction to occur, whether it is a covered transaction in the traditional sense or whether it is a joint venture or some other sort of arrangement. If there is a way in which some sort of foundational technology, even if broadly described, is going to be put to an end use or an end user of concern, then I would suggest using the authorities that already exist in the very flexible export control regulations to identify those.

Now, that is very hard. That is very hard to do in many situations because it may not be—one may not be able to clearly articulate it. But that difficulty, frankly, is a check on the system so that you do not inadvertently impose controls that are broader than necessary and you thus affect collateral controls.

By simply adding broader scopes to CFIUS to catch one situation of one type of technology with respect to really only one or a few countries of concern, you can end up harming the image of the U.S. as a country open to foreign direct investment more generally. So the direct answer is creative, clever use and aggressive evolution of existing export control rules.

Chairman CRAPO. Thank you. And, Mr. Lowery, in your opinion, does CFIUS lack authority to review any category of transactions to fulfill its mandate? Or is it a resource question?

Mr. LOWERY. It is a good question. My own view is that there is a significant resource question that they are going to have to address. It is just becoming very difficult to look at all the different transactions that are coming in and doing it in an efficient and effective manner so that we are still open to investment.

In terms of authorities, it depends. I mean, I think that Jim Lewis talked about CFIUS does not have the ability right now to look at greenfield investments. I am not sure that it should because I think that the idea of CFIUS is to protect national security with an investment that is buying actual U.S. businesses. But if you wanted to go after greenfield investments, it does not have that authority currently.

Beyond that, it does have most of the authorities. That does not mean that you could not make the regulations stronger. It also does not mean that they could—some of the guidelines—CFIUS puts out guidelines about how they think filing parties should be thinking about transactions. Those probably need to be updated. It has not been done in 10 years. And that could help make sure that we are capturing transactions that maybe we were not already capturing. But I think that in terms of the authority itself, it just depends on what you are trying to get after. One that Mr. Lewis said, it would need legislative authority to investigate greenfield investments.

Chairman CRAPO. Thank you.

Senator Brown.

Senator BROWN. Thank you, Mr. Chairman.

To begin with, I first want to apologize. I have, as a number of people on this Committee have, conflicts today. We are working on the farm bill in the Ag Committee. I need to go there. And we are working on tax reform in the Finance Committee, so I will not be sitting here as long as I normally do with the Chair. Usually, we both sit through these hearings for pretty much the whole time. I apologize for having to do that.

Mr. Lowery and Mr. Wolf, I want to start with you. Earlier this year, I raised concerns about potential conflicts of interest in the CFIUS process posed by a number of Administration officials with international business interests. So far, two matters regarding the Administration officials have come to light. It was reported in March that China's Anbang Insurance Group, a company familiar with CFIUS reviews, as you know, had ended its bid to buy the President's son-in-law's Fifth Avenue property. Then in July, after Anthony Scaramucci was announced as the new White House Communications Director, it was revealed that his hedge fund—SkyBridge Capital I believe was its name—was in the process of being acquired by China's HNA Group, possibly for more than the company was worth and was also under CFIUS review.

I am concerned, as I know all three of you are, and I think most of the country is, about the national security implications of foreign acquirers, but possibly and particularly if they have ties to foreign Governments trying to buy influence in this Administration. So I have a series of questions, and, Mr. Wolf, I will start with you, and I will ask the three, and then you can answer as a group, and then Mr. Lowery.

Do you believe Treasury and other CFIUS member agencies have a good understanding of Administration officials' business interests and possible conflicts of interest? Is Treasury aware of the range of business interests and possible conflicts of interest? Could more be done to ensure that all those ties are disclosed? And, third, are processes in place for officials involved in CFIUS or the President himself to be recused if necessary? And I will start with you, Mr. Wolf.

Mr. WOLF. Sure. On the first topic, Treasury as such, I do not recall ever asking those questions. The responsibility for compliance with conflict of interest rules are up to the individual, and they work closely with their counsel at their Department, and that was the primary driver.

With respect to the second question, it could not possibly hurt for Treasury to collect that information and to ensure that the same level of conflict of interest review that is supposed to be done and was done with us in-house by our Department counsel is also provided to the Treasury Department as a double check on what should already be done internally within the Department.

Senator BROWN. And that is not being done, to your knowledge?

Mr. WOLF. Again, the responsibility lies with the individual and compliance with law, and we received regular briefings from our ethics counsel within the Department of Commerce, not just with respect to CFIUS but all matters that we were involved in to ensure that we did not have conflicts of interest both with respect to

the annual disclosure process and regular updates and ethics briefings that the attorneys would give to us.

So, again, I do not know—I do not think that information is generally shared with the Treasury Department, but it should already exist within the Departments, and there could not be anything harmful in doing so because it is already existing information within the existing Department of the individual employee.

Senator BROWN. Mr. Lowery.

Mr. LOWERY. To my knowledge—I agree with Mr. Wolf. When I was working on this, I recall Secretary Paulson recusing himself on specific transactions, or there were others—he was not the only one—that sometimes it just happened to be something that they had been working on in their private sector career, and they saw a CFIUS transaction, and, you know, I would go down the hallway and say, "Hey, we have a CFIUS transaction on this," and the next thing you know, he would call the General Counsel and say, "I have to recuse myself." To my knowledge, that still goes on. I cannot obviously speak on the specific cases you mentioned, but I would assume that the individuals, as Mr. Wolf said, would basically say, "I need to recuse myself. I have business interests here." And they have disclosed that to their in-house counsel so the in-house counsel can also advise them on those issues.

Senator BROWN. And are you satisfied that the information from the Administration and from the President's family, that the information is available enough to you all—not to you all, but to the people in place now?

Mr. LOWERY. So CFIUS is a very—I mean, the people that work on CFIUS transactions, they are very protective of the information. So there are lots of people within the Government that do not have much to do with CFIUS, and they do not understand what is going on. There are two reasons for that. One is the classified information. Obviously, there is lots of classified information. There are national security issue at stake here. But the second reason is because of a little bit the issues you are getting at, but really it is proprietary information. These companies are filing. They are putting forward a lot of proprietary information. There are competitors on the outside that are sometimes very interested. And so you have to be very careful. That is why I think CFIUS over a 10-year timeframe, over a variety of Administrations, has basically been very protective of information. People call it like a star chamber, and the reason they do that is because of how well they protect their information, frankly, better than a lot of other parts of our Government.

Senator BROWN. Did you want to add something, Mr. Wolf?

Mr. WOLF. The issues you raise with respect to transparency of information regarding conflicts of interest of political officials and career employees is not unique to CFIUS because every day—so there is nothing unique about CFIUS that addresses your point, and the success in ferreting out any concerns lies in the existing procedures within each of the departments as opposed to something that is CFIUS qua CFIUS to address.

Senator BROWN. Did you want to add something?

Mr. LEWIS. I would simply echo your point, Senator, that most transactions are without risk to national security, and so it is im-

portant to bear that in mind when we think about the deals that are being looked at. We have seen movie theaters, hotels, all bought by the Chinese, and that does not pose any risk.

Senator BROWN. So while there might be conflicts of interest that might or might not disturb the American public, they are not necessarily national security concerns.

Mr. LEWIS. I think that would be correct.

Senator BROWN. OK. Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

Senator Perdue.

Senator PERDUE. Thank you, Mr. Chairman. Thank you guys for being here today.

Before I start my questions, I would like to make one comment for the Committee since it was brought up earlier. Senator Van Hollen, Senator Schatz, Senator Kennedy, Senator Rounds, and I are new Members of this Committee, but we are totally capable of understanding the full historical perspective around confirmation of this Congress. I certainly echo the comments that have been made this morning about nomination and confirmation of this Committee, but I would like to put into perspective that we are sitting in a period with the slowest confirmation process in the history of our country since George Washington put his first Cabinet together. I think it is outrageous that the last day before we left for August break we confirmed 65 nominations in 1 day because of a back-room deal. Prior to that time, we had only nominated and confirmed—we had only confirmed 48.

As we sit here today, this President has fewer than one-third of the confirmations that the prior President had. So I would like the record to show that some of us do have a full perspective on where we sit today.

Mr. Lewis, thank you for being here today. I lived in China—or I lived in Hong Kong, worked in China, lived in Singapore, and the thing that always bothers me, China over the last 10 years has a net outflow—an outflow of capital of about $3.8 trillion, an inflow of about $1 trillion, 1.3, and then a net—that is a net outflow of about $2.5 trillion. I cannot track it. I have a feeling you cannot either.

In 2016, the Bureau of Economic Analysis estimated about $10.3 billion of Chinese investment in the U.S., and yet AEI and Heritage and others had it as high as 56. So that is a wide range of estimate. And the reason is when you get under it, BEA actually had Luxembourg as the top foreign investor in the U.S. and China was 11th.

With the network of capital flows in the world, how in the world are we able to track the overall net inflows from particular players outside the U.S.?

Mr. LEWIS. That is a great question, and it is a very difficult problem. And as you noted, small Caribbean islands tend to come at the top of the list for foreign investment, not because they are wealthy but because they are vehicles for money laundering. Chinese capital is seeking to leave the country——

Senator PERDUE. And that is—I am sorry to interrupt. That is not just China. That is other people who have very nefarious intentions for the money, too, right?

Mr. LEWIS. Correct. But when you—that is true, and when you try to follow the funding for some Chinese acquisitions, it will lead you to some very strange places. So money laundering is a problem.

There is a desire in China to move money out of the country, which may be kind of a vote of confidence. So we see a very large outflow into many, many sectors, most of which do not cause strategic concern. It is difficult to track, and that is one of the challenges for the Committee, is tracking the money back to its source to see if it is the Chinese State.

Senator PERDUE. Mr. Wolf, with regard to the specific China investments that are of concern, obviously one reason we have been dominant militarily is the size of our investment, but China is now approaching that. So the technological innovation that we have benefited from, from private sector and military and academic research has always kind of kept us at the forefront. One of the things I am concerned about is that China, not only in the United States, but their investment in infrastructure in Africa and other parts of the world, they are leading toward investments of next-generation technologies, and that is really concerning, things like artificial intelligence, autonomous vehicles, augmented reality, blockchain, robotics. They are recruiting actively kids that are graduating from our colleges, our PhDs, our Master's candidates, our scientists, our technicians, our engineers. And there is an immigration issue. I do not have time to get into that today with you guys, but what I would like to know is: How does CFIUS interact with the military, commerce players, and so forth to make sure we find the right balance of this foreign direct investment, which, as Mr. Lowery talks about, is very critical? When you have a $20 trillion debt, you better hope you can attract FDI. And we are the largest recipient of FDI in the world. Thank God. With the size of our economy, we need to keep that up. But there has to be a balance, and I am looking for some input as to things we need to be aware of as we consider this in any potential legislation.

Mr. WOLF. Sure, happy to. With respect to the first topic that you asked Mr. Lewis about, the answer, frankly, is resources and aggressive use of intelligence resources to be able to do the deep digging and the deep dives into transactions. That was a critical part of every CFIUS case that we reviewed. It is what was behind the fund, what was behind the company, who were the parties behind it. And that is not always obvious. And that is just a pure function of manpower and attention and will to do the deep dive. And that is critical to the outcome.

With respect to working with the military, the technical experts at the Defense Department were a critical part of the CFIUS and the export control process in terms of identifying the types of technology that were of concern.

With respect to your concern about investment around the world, that is why working with our allies in the multilateral export control regimes is key, because the U.S. is not the only target for the very anxieties that you raised. And the existing export control system is precisely defined to do that.

With respect to the topics at issue, it goes back to my main point. It requires the resources, the manpower, and the will to focus not just on technologies of yesterday or what is being used now, but

creative thinking on all the topics that you just listed to see if there is a way in which to identify the sweet spot of that part of the technology that is of concern without otherwise trying to interfere or get in the way of commercial development.

Senator PERDUE. Thank you.

Thank you, Mr. Chairman.

Chairman CRAPO. Senator Van Hollen.

Senator VAN HOLLEN. Thank you, Mr. Chairman. And I thank all of you for your testimony here this morning.

I was recently on a bipartisan codel to China, Japan, and South Korea, really focused on the North Korea situation. But while we were in China, we heard from a number of American businesses complaining a lot about the lack of reciprocity generally, especially with respect to Chinese curbs that bar American financial companies access, and that has been referenced here this morning. And while I agree that CFIUS is not the tool we use to respond to reciprocity issues, I do think it is important that we continue to push China really hard on that front.

Let me ask you, Mr. Lewis, you talked about how China—and, look, we all agree that, overall, foreign direct investment has benefited the United States, but we want to make sure that it does not hurt us in our strategic interests, especially national security. The question is how we may broaden that to look at some key national economic security issues.

You mentioned China buying up small firms in the Silicon Valley area, and my question for all of you is: When you have one big purchase, you know, you may very clearly be able to decide this is going to have an impact on national security or not. But do we have the tools to look at sort of a pattern of a purchase and say, hey, this one in and of itself, this purchase may not trigger a national security problem. But China has the ability, you know, it is not like a bunch of free market companies that are out there purchasing. They have got a strategy, you know, driven by the Government. Do we have the capacity to say, OK, this one by itself may not be so bad but, you know, if you go down the line, one, two, three, four, then you are talking about a serious national security issue?

Mr. LEWIS. I will start. Thank you, Senator. That is a great question. One thing that has been touched on a couple times in all of our remarks so far and in the questions is the question of intelligence support for CFIUS. And to the extent this can be discussed in an open hearing, it would be beneficial if there were additional resources given to the National Intelligence Council.

The U.S. relies on two sources of intelligence to track both money laundering and the kind of activities you are talking about: human intelligence, which faces grave problems in China, as you know; and signals intelligence, which also is pressed considerably by the Chinese. So we need to think of how to make resources and collection priorities evolve to reflect these kind of economic problems you have raised.

We do not have the ability yet to adequately track these larger patterns, so CFIUS tends to be a transactional focus, and it would be beneficial if the NIC or some other body had the ability, the wherewithal to supply things on long-term trends in semiconduc-

tors, artificial intelligence, cloud computing, hypersonic strikes. There is a whole range of things, so, yes, better intelligence support, better tracking trends would be valuable.

Senator VAN HOLLEN. All right. I would be interested in any other comments, but also I would like to throw in there the greenfields issue. I take it from your testimony, Mr. Lewis, that you think we should expand the jurisdiction, the authorities here to include greenfields. Is that right?

Mr. LEWIS. Yes.

Senator VAN HOLLEN. And as the others answer that earlier question, if you could also respond to that issue.

Mr. WOLF. Sure. The issue with respect to trends was very important to me when I was in the Government, and the first direct answer that is not really a CFIUS issue is just a straight up law enforcement effort. If there are a particular series of individual acquisitions that are all on their face benign but in the aggregate are used for an ulterior motive such as creating front companies in order to hide the ultimate objective, then using the existing domestic law enforcement tools of getting to that motive and pursuing intellectual property theft, espionage under existing statutes is absolutely critical. And that can be done without CFIUS.

Within the CFIUS process, it is important that in the intelligence estimate that is provided with respect to an intelligence—or with respect to a particular case, an answer given as to whether this is an individual transaction or part of a trend or pattern, and that is absolutely something that we reviewed, and I would want to make sure that the authority exists to be able to block or deny or mitigate a case if the information exists that this is only one part of a whole.

So your question and your concern about the trend is absolutely valid and something that we spent a significant amount of time looking into.

Mr. LOWERY. The only thing I was going to add is that the trend is something that CFIUS does look at. In fact, actually in their annual report to Congress, CFIUS actually does try to point out here is where a number of transactions have actually happened, and we are now concerned that a specific country—and it would be a classified report, so Congress could see it; I could not see it—is able—is going after a certain technology. So this is done with CFIUS, but it is usually—Treasury leads the effort, but really it is the intelligence community and the Commerce Department that does a lot of the heavy work, as well as the Treasury Department. So there is a way of trying to get at that through CFIUS, though I think Mr. Lewis makes a good point about there are other things that need to go beyond that.

Senator VAN HOLLEN. Thank you. I look forward to following up with all of you.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

Senator Rounds.

Senator ROUNDS. Thank you, Mr. Chairman. This has been an interesting discussion, and it leads me back into another responsibility. We all have multiple committees up here. I serve on the Armed Services Committee, and as such, I also serve as Chair of

the Subcommittee on Cybersecurity. One of my concerns about the increased foreign investment in the United States is what kind of electronic and cyber-vulnerabilities that increased foreign investment poses for our country. For example, there is already significant concern in Congress and the Administration that countries like China are acquiring intellectual property from American companies. I am concerned that foreign investment in our country would give potentially malicious actors a back door into the United States and leave us perhaps more vulnerable to IP theft or cyberattack.

My question for you is: Can you discuss the nexus between cybersecurity and foreign direct investment? And is the CFIUS review process robust enough to account for vulnerabilities in this area? Or is it simply one part of a chain, and how does it fit into that chain with other investigations as well? Mr. Lewis.

Mr. LEWIS. Thank you, Senator. That is a major concern, so I am glad you raised it. Let me just talk about the potential risk to cybersecurity.

You have supply chain risk, which is that the components or the software that goes into critical infrastructure defense products may be contaminated at the source, creating cyber-risk for the U.S., military risk. This is no longer a hypothetical concern, so there have been some incidents.

You have a critical infrastructure risk that the CFIUS Committee has been good at blocking acquisitions of critical infrastructure or in mitigating potential risk. So when you think about, say, Alcatel–Lucent, the conditions that the Committee imposed were sufficient to mitigate the risk. And following up on these mitigation agreements is an important part—an important improvement I have seen in the last few years with CFIUS.

You have real estate concerns. That always sounds funny, but we know about the potential of the wind farm to be next to a Navy research facility. You have to think about real estate now. Ten years ago, real estate was not on the CFIUS agenda.

And, finally, a new one is data. The access to huge swaths of Americans' personal data by a foreign competitor could create intelligence risk.

So I think there is a whole area where we need to think about how an acquisition will affect or increase the risk to cybersecurity.

Senator ROUNDS. Any other thoughts, gentlemen?

Mr. WOLF. Those are excellent points. Just to emphasize a significant number of the cases that we have reviewed over the years involved situations where the U.S. Government or its contractors or suppliers were consumers of critical infrastructure, telecommunications equipment, computers, et cetera. And to the extent that there was a possibility of foreign control over the content of the components or malicious software being installed surreptitiously, that was factored into our decision to either propose a block or aggressive mitigation, such as a requirement to spin off the U.S. side of the business for a certain number of years so that the U.S. Government, Defense and other departments, could find other alternative sources of supplies that were domestic. So that is a critical part of the CFIUS review.

The other part of it, frankly, with or without an individual transaction, is the regular cybersecurity work that the Government and its contractors do in terms of knowing who their suppliers are of their components and what the source of the information is that they are receiving. And that is in addition and separate to CFIUS, and, again, unrelated to particular transactions. But it was one of the most significant, most discussed, most critical elements of the cases that we saw in the last several years. It is a key point.

Mr. LOWERY. The only thing I would add, just as Mr. Wolf and Mr. Lewis said, CFIUS has done this part extremely well, is my view. But some of the aspects go beyond CFIUS, and that is where there are other tools within the Government that we try to work on, but remember, CFIUS has on its Committee the Defense Department, Homeland Security, Justice Department, the intelligence services across the Government, which include the FBI, the CIA, the DIA, the Treasury Department's intelligence services. So all of these folks are working together to try to see whether or not there is an actual risk because of a purchase of a U.S. business.

Senator ROUNDS. Do you find that the focus, which right now is on the entity itself that may very well want to make a purchase within the United States, is there adequate focus also on the product itself or the different products, whether it be data, whether it be a specific product that is vital within another part of the chain? Do we have the ability right now and are we focused enough on both—not just the entity itself but the different products that may very well be the issue of concern?

Mr. LOWERY. My view is that is what CFIUS is at least attempting to do the whole time, and I think that they have done pretty well. So they look at the threat, which is the entity that is purchasing. They look at the vulnerability, the product that they are actually purchasing. What is that asset? Does it have any nexus to national security or not? And then trying to figure out is it OK for those two things, the threat and the vulnerability, to come together? Or do you need to mitigate it or do you need to block it? That is what CFIUS is trying to do the whole time.

Senator ROUNDS. Yes, sir?

Mr. LEWIS. Thank you. The two agencies that provide the support to CFIUS in this regard are both the intelligence community and DOD. So we really rely on them to be able to say when a particular technology or product creates cybersecurity risk or any other kind of risk.

Senator ROUNDS. Thank you. My time has expired.

Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

Senator Warren.

Senator WARREN. Thank you, Mr. Chairman. And thank you to our witnesses for being here today.

CFIUS, the Committee on Foreign Investment in the United States, is responsible for reviewing the acquisitions by foreign companies to ensure that they do not threaten U.S. national security. And, unfortunately, this applies only to certain transactions, and our adversaries know that.

So according to news reports, an internal Pentagon report issued last year found that China was making significant targeted invest-

ments in cutting-edge American startups with expertise in areas like autonomous vehicles, artificial intelligence, robotics. These types of investments provide access to potentially sensitive technology, but they do not trigger CFIUS review.

The Pentagon is worried—and I think they should be worried—about this. In June, Secretary Mattis told the Armed Services Committee he thought CFIUS "needs to be updated to deal with today's situation." So I wanted to start by asking you, Mr. Wolf, are you concerned about the national security impacts of these early stage investments in sensitive technology?

Mr. WOLF. Yes, I am, and that is why I would put a particular emphasis on identifying what the technologies of concern are, and in addition to the CFIUS authorities, making sure that they are adequately described within the existing export control system.

Senator WARREN. Actually, can you just say a bit more about what you would do by way of response? Can you expand on that a little bit?

Mr. WOLF. Absolutely. So instead of waiting for a transaction to occur, however it is defined, whether it is a joint venture or a covered transaction or a greenfield investment, the Department of Defense, working with its colleagues in State, Energy, and Commerce, should identify the key sweet spot of those types of technologies that you described that are of national security concern and make sure that our existing export control rules govern them and, to the extent possible, work with our allies so that their regulations control the same types of technologies. That magnifies the benefit of the effort.

Senator WARREN. Actually, that is very helpful. You know, as you know, a lot of today's technologies look very different from what the world looked like back when we built CFIUS originally. And the defense technologies of tomorrow are going to look even more different. So we need an approach to it that keeps changing, iterating over time. And I think that means it is time to expand CFIUS's mandate.

But before we do that, we are going to need to deal with the fact that CFIUS has serious staffing and resource problems already. In recent years the number of cases coming before the Committee has skyrocketed. Both current and former Government officials have argued that CFIUS must be strengthened, but so far the opposite seems to be happening. President Trump has failed to appoint certain key positions in the CFIUS process, including the Director of the Office of Science and Technology Policy, which is kind of important here. And the President's budget proposes significant cuts at some of the CFIUS agencies, including a 16-percent cut to the Commerce Department and a 32-percent cut to the State Department.

So could I ask, what impact do budget cuts have on the positions at non-DOD CFIUS agencies? What impact will this have on the work of the Committee?

Mr. WOLF. It is potentially devastating. It is all a function of resources and manpower and attention spent to complex situations, complex technologies, and difficult transactions. And you need lots of people or you need more people than are there now in order to address all the issues that you identified.

Senator WARREN. Well, thank you. I think this is urgent. It is about national security. We do not want to wake up one day and discover that our adversaries have components of our national security technology because Congress and the Administration were asleep at the switch on this. We need to modernize this process, but we also need to make sure it is fully staffed.

Mr. WOLF. I agree.

Senator WARREN. Thank you, Mr. Chairman.

Chairman CRAPO. Thank you.

Senator Kennedy.

Senator KENNEDY. Thank you, Mr. Chairman.

Tell me, gentlemen, what triggers CFIUS review?

Mr. LOWERY. So CFIUS is technically a voluntary process, so if you are in an M&A transaction and it is in the national security realm and that realm is not defined, but there are a number of factors in the law that suggest what those national security issues are. So M&A transactions are voluntarily filing transactions. That is how you trigger a review.

It is important to note that if the Government or CFIUS sees that a transaction has not been filed, they do have the power to compel a filing, if need be.

Senator KENNEDY. What should trigger a review? How would you change it?

Mr. LOWERY. The only way I would change it—so I think that that actually is a good approach, because there are lots of transactions that happen—in fact, the bulk of the cross-border mergers and acquisitions that happen are in areas that have nothing to do with national security, and so we should not be doing national security reviews of them because we just waste resources by doing that.

But I think that it should be explored at least. One idea is—so right now CFIUS does high, high scrutiny of State-owned companies when they make a purchase in the United States. I think that it might be worthwhile at least exploring the idea of should those filings be mandatory as opposed to voluntary. And then you could through the regulatory process try to narrow that scope down because there could be State-owned cases or State-controlled entities that buy something, again, that has nothing to do with national security. So I think that is worth something to explore. That is right now not in legislation, so you would have to change the legislation for that.

Mr. WOLF. One additional idea would be with respect to acquisitions or any kind of an arrangement next to a sensitive facility. Right now, the colocation issue that I described only gets triggered if it is a covered transaction as defined in the legislation. And I do not have an exact answer for you, but to the extent that there is a joint venture or a greenfield investment or any other kind of investment near a facility, there should be a Federal way in which to limit the access, proximity next to a sensitive facility by a foreign entity.

Mr. LEWIS. And perhaps a final point is that Wall Street and the investment community knows in much greater detail the transactions that are underway or being contemplated, and particularly if it is a publicly traded transaction, we might have a publicly trad-

ed company, we will get some regulatory insight. But if it is not publicly traded, we may miss it. So finding ways to better take advantage of the knowledge on Wall Street and to look for private deals would be helpful.

Senator KENNEDY. Well, what if it is not a merger and acquisition? I think this is Senator Warren's point. Let us suppose you have a startup developing a pharmaceutical drug, and someone in China wants to put in $20 million for Phase I trials. Is that something we ought to look at?

Mr. WOLF. Well, in general, that type of investment should be welcome, and we want to make sure that the U.S. remains welcoming to that. And the key goes back to the points that I was raising earlier, which is: Is there something about that investment that creates a national security issues or is it an economic issue better left to bilateral deals or trade remedies outside of CFIUS?

So in that type of fact pattern, I would think about it, not waiting for a transaction, however you define it, whether covered or joint venture or just a flow of money, but identifying the information that is of concern and trying to address the information in any setting.

Senator KENNEDY. But how do you know? Let us suppose the pharmaceutical drug is a vaccine for HIV, and it appears to work, so the Chinese just keep pouring money into it, and they get control of the company, and they take it back home, and they keep the vaccine and say, "We are not going to share it with America."

Mr. WOLF. Then that becomes economic and other issues. Then it really is a function of what our intelligence agencies can tell us about the intentions of the parties engaged in particular transactions.

Senator KENNEDY. They are not clairvoyant, though. They cannot tell the future.

Mr. WOLF. No, they cannot. And we can do what we can do, but there are a lot of very clever people who can think aggressively and prospectively about the types of technologies that, if cutoff or no longer able to be developed in the U.S., would create national security threats. And that should be the emphasis of the thinking.

Senator KENNEDY. Let me ask one other question quickly, gentlemen, and any of you can jump in. When, if ever, should CFIUS be used as a sword with respect to reciprocity? I do not mean to pick on the Chinese. They are not the only ones. But they are beating our brains out. They are stealing all our technology. It is a condition of doing business there.

Mr. LOWERY. So my own view on—should CFIUS be used as a reciprocity tool? My own view is no, and I have a few reasons for this. One is that if there is an investment that makes sense that is coming into this country, but American firms would not be allowed to invest in China, why should we penalize the company that is receiving that investment, when it is not a national security issue whatsoever, just because maybe some of their competitors could not go out and buy something in China? I think that, in essence, we would be importing the policies of another country—China—as opposed to using our own—the policies of what we want in this country, and the policies that we want in this country are to welcome foreign investment. So I do not think that CFIUS is the

way to get at reciprocity. I think there are trade tools that we can be using, and that is a much better way of approaching the problem.

Mr. LEWIS. I disagree with that a little bit. I think we need a comprehensive strategy for approaching China on these trade issues. They have gotten away with things for decades, and you need to approach them thinking about CFIUS, foreign investment, export controls, trade provisions. You have to have the full package. And as a negotiator, you may not want to take anything off the table until you see if it is worth doing. So go in with the whole deck. See what they offer you.

Senator KENNEDY. Gentlemen, I am out of time. Thank you.

Senator SCOTT [presiding]. Senator Donnelly.

Senator DONNELLY. Thank you. And thanks to all of the witnesses.

My home State of Indiana is home to a big portion of the American steel industry, and it is an integral part of our national defense manufacturing base. Increased levels of foreign steel imports, particularly from China, and a lot of it is with dumping, illegal Government subsidies, it has weakened our domestic steel industry, and it has provided foreign companies greater access to our markets. So this is to all of you. When you review transactions, does CFIUS consider foreign industrial policy that weakens U.S. industries vital to defense manufacturing and critical infrastructure?

Mr. LOWERY. So CFIUS would look at—if an investment, not an export but an investment into a company in Indiana or any company was actually harming maybe the supply chain for the Defense Department on steel or could potentially—by getting access to specific technology, could actually harm the United States' national interest, that is what CFIUS would look at. CFIUS would not look at whether or not a country is dumping. That is something that would be done through trade remedies.

Mr. WOLF. He said it very well.

Senator DONNELLY. OK. Let me ask you this: Are there U.S. industries important to our national defense or critical infrastructure that have been particularly challenged by aggressive foreign trade policies? As you look at the national defense area, obviously one of concern is steel. What are other ones? And what do you see as the biggest challenges they face? I know that is a little bit to the side of what we are doing right now.

Mr. WOLF. Sure. Within the CFIUS context, the evidence shows based on public filings of cases during the Obama administration and now that the semiconductor industry is obviously the hottest topic with respect to the issue that you raised. To the extent that it is a trade remedy issue, that is not the role nor does CFIUS have competence or expertise to be able to focus on that. It is focused just on the national security implications. But, you know, by the evidence, that plus issues involving foundational technologies for aerospace have been hot topics, absolutely.

Mr. LEWIS. Generally, anything that you could label as high tech is a concern, and so avionics, not only semiconductors but the broad information technology industry, including robotics and artificial intelligence, these are all places where we have seen efforts

by China and a few others to acquire U.S. know-how in companies in ways that would harm our national security.

Senator DONNELLY. Currently, CFIUS reviews foreign direct investment transactions for national security implications. Do you believe CFIUS or a process modeled off it should also review the economic considerations of foreign investments to see that the American economy actually benefits in any way, shape, or form from the transaction?

Mr. LOWERY. So I think that there is a portion of that that CFIUS does, but not a big portion, and that is basically if there is a mitigation agreement—the Department of Labor actually sits as an ex officio member of CFIUS to make sure that labor issues are looked at carefully. But in terms of do I think that CFIUS should expand its mandate to go beyond national security to kind of an economic benefits test, a benefits-cost test, I do not. But that is because I think that we are welcoming foreign investment and we have to be very careful about how much we are dictating to companies about how they handle things. As long as they treat their employees well and follow the laws of the land, then that is not something I think CFIUS should be looking at.

Mr. WOLF. I agree. I believe that CFIUS should continue to be narrowly focused on national security implications. The implications of expanding its scope to pure economic considerations runs the risk of politicization and overall harming the U.S. as a destination for foreign direct investment. To the extent that there are economic harms with respect to investment, there is an entire body of law dealing with trade remedies that is much more tailored, much more specific, much more robust to address that. CFIUS does not have the history, the expertise, the personalities to be able to address it, even if the authority were to expand.

Mr. LEWIS. The dilemma of what you have raised is a serious problem, and so we do need to address it. But CFIUS may not be the right tool. There are other tools that we either have or that we need to deal with this because it is something that increasingly is affecting the American working population.

Senator DONNELLY. You talked a little bit about the stretches on the CFIUS tool as it is, as the volume increases and complexity of transactions continues to increase. What additional resources, if any, such as personnel and information-sharing technology do you think CFIUS needs to process a higher volume of transactions and to be able to make sure they are covering what they need to do?

Mr. WOLF. A significant number of more people involved in handling the mitigation agreements. After a deal is reached, often there is a condition of the sale that requires a lot of manpower, a lot of oversight. They last for a very long time, and there are more every day. And so the number of people that need to be focusing on that needs to be substantially higher.

Similarly, the number of people who spend their days reviewing transactions, public and otherwise, to see if any of them warrant being pulled before CFIUS for consideration, that is a straight up issue of manpower and resources in reviewing data. Those are the two biggest resource constraints right now.

Mr. LOWERY. I would only add one, which is—I agree totally, but it is important to get some of our political officials confirmed, and

the reason is because—look, the CFIUS people doing their analysis do an excellent job. But they are civil servants. These transactions by nature involve a lot of risk. There is risk. And so taking that risk is something that Senate-confirmed people are paid to do, to be frank. They are the ones that have to come in front of this Committee and answer to what decisions are made. It is much harder for the civil servants, who are doing an excellent job, to do that, and so sometimes having the resources to do mitigation agreements so that you can actually welcome that foreign investment and protect national security, but you then also need some of your political appointees who can provide air cover and make the tough calls.

Mr. LEWIS. One agency we have not mentioned yet—and we have mentioned a lot—is the Defense——

Senator DONNELLY. Mr. Lewis, I apologize. I am out of time.

Mr. LEWIS. Just let me say DSS, they are the ones who do the mitigation agreements. Give them a little more help.

Senator DONNELLY. OK. Thank you.

Thank you, Mr. Chairman.

Chairman CRAPO [presiding]. Thank you, Senator Donnelly.

Senator DONNELLY. See, I was doing your work for you there.

Chairman CRAPO. I appreciate it.

Senator Scott.

Senator SCOTT. Thank you very much. Thank you to the panel for being here this morning as well.

There is no question that South Carolina benefits from FDI. In the past 5 years, our State's economic activity based on FDI has increased by 30 percent. Over 130,000 South Carolinians are employed as a result of global investment.

That said, it is clear to me that bad actors are taking advantage of our system of trade. Senator Cornyn and others have pointed to gaps in CFIUS around the purchase of foundational technologies of AI and biotech. These gaps have allowed the Chinese to strategically invest in key sectors of our economy while stealing our intellectual property and eroding our military superiority.

I will ask the panel and start with Mr. Lewis: What techniques are the Chinese using to circumvent CFIUS? The second question is: How can Congress fill these gaps in our protections?

Mr. LEWIS. So I think we have talked a lot about the greenfield problem, which is that—this has come up a couple times. Our regulations are post facto. So if you have not invented the technology, it is not going to be caught. And so how do we deal with that? And the Chinese are looking to buy brains, right? And it is very hard to control brains, especially if they are in the country. So we need to think about how we track, monitor, and occasionally—not always but occasionally, because of the benefits you cited, occasionally block transactions where China is making bets in the future technologies.

Mr. WOLF. On the intellectual property theft issue, that is much more of a law enforcement issue and attention and resources of the Justice Department to investigating whether it is a sensitive technology or otherwise that is being stolen or exfiltrated. So CFIUS may not be the best tool because if there is going to be IP theft, there is going to be IP theft with or without a transaction, however you define it, so focus the resources on the theft of the technology

in the traditional way, and that would be my suggestion for an emphasis on that question.

Senator SCOTT. Anything to add?

Mr. LOWERY. The only thing I was going to add is that if the technology is in an area that is concerning potentially for export controls, that is when some of Mr. Wolf's comments from earlier come into play, I think, where looking through what powers and abilities through the flexibilities of our export control laws as opposed to CFIUS, which is there to—if there is an investment actually in a company or in a business that actually gets some of those assets that could be a national security concern, that is when CFIUS should play its role.

Senator SCOTT. Thank you.

Considering the topic of today's discussion, I want to point something out that I think is very important. A majority of Chinese deals make it through our approval process. Yet American companies are not given that same courtesy in China. In fact, China dramatically restricts our financial services sector's presence in its country. That does not seem fair to me, because it is not.

That is not a level playing field that our President is advocating on behalf of. I was joined by Chairman Crapo—thank you very much—and 14 other Senators in asking the Administration to focus its efforts on the lack of reciprocity.

Mr. Lowery, can you discuss the hurdles that American financial services firms face in China?

Mr. LOWERY. Yes, this is something I had to work on when I was in Government. So it has been a problem for a while. I was glad to see the letter from the 14 Senators. I wish it was 100 Senators, because I think that it is a problem, which is that U.S. firms cannot actually—there are equity caps in insurance companies, there are equity caps for investment banks, there are equity caps for banks. The way that we have made progress on that in the past has usually been through dialogue, and so I recall back in 2006, 2007, we were running into a lot of problems. Through a dialogue that Secretary of the Treasury Paulson set up at the time, we were able to make progress—not as much as we should have. Under the Obama administration, they also had a dialogue which also made even further progress on getting these equity caps raised.

I think that that is something that the Trump administration should work on, my guess is they are probably starting to work on. But I think that that is a way to get at it. But your point is exactly right. There is a problem when in an area such as financial services where it makes very little sense for them to have equity caps that China still has those. But I think that through the force of our will and diplomacy, that is the best way to get at that problem.

Senator SCOTT. Thank you very much, Mr. Chairman.

Chairman CRAPO. Thank you.

Senator Tillis.

Senator TILLIS. Thank you, Mr. Chairman. Gentlemen, thank you for being here.

China, I think, constitutes about 1.6 percent of our total inward foreign direct investment, so relatively small scale. A lot of what we are talking about here are things that they have done that are really outside of this that need to be dealt with, and I think prob-

ably dealt with in a way that is perhaps outside of CFIUS. One thing, Mr. Wolf and Mr. Lowery, you both have said is that trying to keep the scope tight—I could be concerned with CFIUS scope creep moving into other areas that we probably should consider, but not necessarily within the lanes of CFIUS.

Mr. Lewis, I want to talk about one of those. As China's economy emerges and as it matures and as they try to build infrastructure for things that are not related to national defense—you know, pick an area, health care, insurance, whatever—they are likely to look at Nations that have mature platforms, the technology platforms that they would like to use to accelerate, you know, really actually rounding out an economy that is still growing. And if they do that, if they are to acquire somebody—you made me think about this because of a comment you made about maybe an acquisition would involve a company that has a significant amount of data on U.S. citizens, say health care information. How do we strike the balance between allowing that investment to occur, which may be needed by a technology provider that is in a mature market, to let them leverage their technology for purposes that are purely, you know, in this case let us say for the Chinese population, how do you do that in a way that does not create an impediment for companies that have data that we clearly want to protect but not necessarily disadvantage them as having a large platform and growth opportunity in a country like China?

Mr. LEWIS. Thank you. Great question. China has gotten sort of a pass on the trade rules ever since they joined the WTO, and their argument was, "Well, you know, we are small and we are growing and we are poor, so it should not apply to us." And that just does not work anymore. So part of it is we need to think about how do we get China to live up to its commitments under international trade. I am optimistic that they can do that. This Administration appears to be making an effort. That is good. But it will take a long time because they get so much benefit out of it.

In the near term and on specific cases, I think this is one of the strengths of the CFIUS process, is the ability to impose mitigation agreements on the acquirer that limit the risk, and those have been relatively successful. There is this issue of tracking them afterwards, and that is where——

Senator TILLIS. On that, I have one other question I want to direct specifically toward CFIUS. But I think that so much of what we need to do to get China to a good place in behavior is probably not something that would come through CFIUS but would come through trade agreements, a number of other devices that we can use to actually incent them to exhibit good behavior.

Now, with respect to CFIUS, I have had this discussion in Senate Armed Services on cyber. You know, what we seem to be focused on are the—you know, it is an artificial intelligence application, maybe it is next-generation communications technology, biotech. But what about the risk of focusing on those big rocks and missing some of the little rocks that if China had significant investment in could be disruptive? I always use the example of if I were trying to think about a way to disrupt the U.S. economy or the DOD, the DOD would be the last place I would attack. It would be

their supply chain. And it would be to the most vulnerable part of their supply chain, and I am talking about a cyberthreat.

Well, similarly, I would make investments in companies that could ultimately be disrupted. We think about the end product. I think about the supply chain that gets to that end product. So to what extent does CFIUS take into account maybe seemingly innocuous minor investments in companies and technologies that ultimately play a very important role in that supply chain link to these other highly important technologies that we focus on?

Mr. LOWERY. I think that the answer is that is exactly what CFIUS is trying to look at, so——

Senator TILLIS. How well do you think we are doing it for the fully supply chain?

Mr. LOWERY. I think that CFIUS does a very good job of looking at companies that are part of the supply chain. The reason is because the Defense Department, some of the officials there—not just the Defense Department. It could be Homeland Security or the Justice Department. They know kind of where the supply chain exists, because actually some of the people that work on CFIUS are some of their procurement experts. And so they actually look at the supply chain and think—there are transactions that I know CFIUS has looked at which were tiny transactions, and no one would—they would never make it into the newspapers. But CFIUS actually goes out and says, "We need to look at that because that is a small part of our supply." And that is something that—if it is a purchaser that is a threat to our national security, that may make it—either block it, get it to abandon the transaction, or as Mr. Lewis said, come up with a mitigation agreement so that you might wall them off from certain parts of that technology.

Senator TILLIS. And, Mr. Chair, since I am the last one, I want to ask just one more question, if I may. To what extent does CFIUS—let us say that, again, with China only being 1.6 percent of the internal FDI right now, but they have great relationships and growing relationships with many of our allies that constitute a significant portion of that. To what extent is CFIUS instructive by the nature of the relationships that China has with other—let us say a company domiciled in Australia that is making a significant investment in a technology that would be subject to immediately flag if it comes from China? Is that all instructive to the CFIUS process.

Mr. WOLF. It is, and it should be more so. One of the changes I would recommend considering that we often discussed is sometimes we were limited in our ability because of either classified information or proprietary information issues from sharing concerns we had with allies and getting information from them with respect to similar concerns by similar investments in their countries. And a serious topic, I would think, for legislative consideration would be expanding the ability of CFIUS to share information, both commercial as well as intelligence, with allies for exactly the purpose that you just described.

Mr. LEWIS. That is an important area for reinforcement because when you look now at our NATO allies, at Australia, at Japan, they are all concerned about Chinese investment. They are all looking to the U.S. to provide them at least an example on how to regu-

late it, and CFIUS is an example. And they are looking for the kind of information and intelligence support that Mr. Wolf was discussing.

Senator TILLIS. Thank you all.

Thank you, Mr. Chair.

Chairman CRAPO. Thank you, and, Senator Tillis, I will take one more question also.

This will be the final question, and it is for the whole panel, if you have a response to it. In your opinion, are there any instances where a gap in CFIUS authority either could have or did result in a threat to U.S. national security? And if so, please discuss the CFIUS shortcomings that led to such a breach.

Mr. LEWIS. So I believe the thing that we would all want to look at is the Defense Department report that talked about—and I hate to say it over and over again—greenfield investments in Silicon Valley, looking at advanced information technologies for robotics and artificial intelligence. The Chinese have been able to acquire technology in a way that circumvented the process.

Mr. WOLF. So in my 7 years, I am confident that there were no unresolved national security risks with any case that we addressed. I would go back to the point I made earlier about activities outside of CFIUS authority with respect to colocation near sensitive military facilities. And I do not have visibility into that, but it would be something worthy of further analysis along the lines of your question.

Chairman CRAPO. Thank you.

Mr. Lowery.

Mr. LOWERY. I am unaware of anything, any problem that has existed. I think the DIUx report does some excellent analysis. I think that some of their policy conclusions need more work.

Chairman CRAPO. All right. Thank you. And, again, let me thank each of you for your written testimony and for being here and responding to the Senators today. This is a very critical issue, and there is a significant amount of interest and activity here on the Committee and outside the Committee here in Congress, and we intend to explore it, and we want to get it right. So we appreciate your help. Thank you for being here today.

This Committee is adjourned.

I should have said for the record that questions from Senators may come to you, and we urge you to respond to them promptly, and the Senators have until the 21st to submit those questions.

[Whereupon, at 11:28 a.m., the hearing was adjourned.]

[Prepared statements, responses to written questions, and additional material supplied for the record follow:]

PREPARED STATEMENT OF CLAY LOWERY

MANAGING DIRECTOR, ROCK CREEK GLOBAL ADVISORS, AND FORMER ASSISTANT SECRETARY FOR INTERNATIONAL AFFAIRS, DEPARTMENT OF THE TREASURY

SEPTEMBER 14, 2017

Chairman Crapo, Ranking Member Brown, and Members of the Committee, I would like thank you for the opportunity to testify on Examining the Committee on Foreign Investment in the United States (CFIUS). My name is Clay Lowery and I am currently Managing Director of Rock Creek Global Advisors, a consulting firm that advises clients on international economic and financial policy matters. My testimony should be considered my own views alone.

I served in the U.S. Government from 1994 to 2009, principally with the Treasury Department, although I also had a stint at the National Security Council. From 2005 to 2009, I served as the Assistant Secretary of International Affairs for the Treasury Department, and one of my primary responsibilities was overseeing CFIUS during the last time substantial CFIUS reform occurred.

I am pleased to be testifying alongside Kevin Wolf and Jim Lewis, both of whom I respect and of whose views and expertise I think highly.

In my testimony, I will discuss briefly (i) the nature of CFIUS and its process, (ii) its performance, and (iii) some thoughts on CFIUS reform.

CFIUS plays a critical role in protecting U.S. national security. I recognize there are gaps in the current system that must be addressed, but I would also counsel that CFIUS's objective is to protect legitimate national security interests while promoting foreign investment, and thus CFIUS should not be used as an economic, protectionist, or overly broad tool.

The most important aspect of CFIUS is to understand what it is trying to achieve: ensure national security while promoting foreign investment. These words come directly from the legislation that created CFIUS and has guided it for the last 30 years. When experts raise concerns about national security issues that may have recently become more prominent and recommend that the best—and sometimes only—tool to address those concerns is CFIUS, my view is to evaluate those recommendations against what CFIUS was designed to achieve.

Roughly 7 million American workers, or about 6 percent of total U.S. private-sector workers, are employed directly through foreign direct investment (FDI). These jobs are higher paying: providing average compensation per worker 24 percent higher than U.S. private-sector wages. These jobs are disproportionally in the manufacturing sector: 20 percent of all manufacturing employment is due to FDI. And, according to a recent Reuters analysis—two-thirds of the manufacturing jobs created from 2010 to 2014 can be attributed to foreign direct investment.

In short, FDI is in the national interest of the United States. However, we should not be complacent. While the U.S. remains the largest destination for FDI, our share of attracting such investment has fallen about 40 percent in the past 16 years.[1]

Last, I want to note how this could be used against U.S. companies overseas. The United States has always been the leader in defining "national security" in a reasonable and fair way. I would remind the Committee that any actions we take are likely to be copied and used by other countries, potentially to the detriment of U.S. interests abroad.

CFIUS Evolution

CFIUS is an interagency committee established by Executive Order in 1975 with the Secretary of the Treasury as its chair. Its central purpose at that time was to monitor foreign direct investment in the United States. In 1988, driven by concerns regarding growing Japanese investment in the United States, Congress enacted the Exon–Florio amendment that expanded these powers significantly, including (i) giving CFIUS the responsibility to investigate foreign acquisitions of companies engaged in business in the United States, and (ii) providing the President the ability to suspend or prohibit a covered transaction that, in the President's judgment, threatens the national security and existing laws are not adequate or appropriate to address the threat.[2] In 2007, following concerns that had been raised over a Middle Eastern investment in U.S. port facilities, Congress amended and further

[1] United Nations Conference on Trade and Development (UNCTAD) World Investment Report 2017.

[2] To be precise, the President delegated the investigative functions to CFIUS by Executive Order.

strengthened CFIUS through the Foreign Investment and National Security Act (FINSA).

A new Executive Order directing CFIUS followed in early 2008 and new regulations implementing FINSA were issued later that year. The key reforms resulting from those efforts include:

- Increasing accountability in the executive branch as Senate-confirmed officials now must certify that CFIUS has completed its work on each transaction;
- Broadening the factors that CFIUS may consider in terms of investigating cross-border M&A transactions, particularly in areas such as critical technology, energy, and critical infrastructure;
- Raising the certification bar for cases in which the acquirer is a State-controlled entity;
- Increasing CFIUS interaction with Congress;
- Providing for a more formal role for the intelligence community; and
- Clarifying CFIUS criteria for evaluating whether an acquirer is obtaining control of a U.S. business.

CFIUS Process

CFIUS is chaired by Treasury and is comprised of the Departments of Commerce, Defense, Energy, Homeland Security, Justice, and State as well as the Office of the U.S. Trade Representative and the Office of Science and Technology Policy. In addition, the Intelligence Community under the leadership of the DNI and the Department of Labor serve as nonvoting members of CFIUS.[3]

Parties submit their transactions to CFIUS for review on a voluntary basis, although CFIUS has the authority to compel a filing if necessary. The statute prescribes strict timelines for CFIUS's review, but parties are encouraged to pre-file with CFIUS to provide the Government with an opportunity to begin its analysis before the "clock starts ticking."

CFIUS officials are obligated by law, and subject to the possibility of criminal or civil penalties, not to disclose information regarding transactions. The rationale behind this rule is to protect both proprietary and intelligence information.

Once a transaction has been filed, CFIUS first determines whether it has jurisdiction to review the transaction—that is, does it involve foreign control of a U.S. business in interstate commerce—and, if it does, CFIUS then undertakes a three-part evaluation:

1. Does the acquirer pose a threat to national security? This analysis is led by the Intelligence Community.
2. Is national security made more vulnerable by virtue of the acquisition of the U.S. assets? This analysis tends to be driven by the CFIUS agency with applicable subject-matter expertise.
3. Do the consequences of permitting the threat and vulnerabilities to be combined through a specific transaction risk impairing national security?

CFIUS investigates these questions in the first 30 days after it accepts the filing. If at the end of those 30 days, CFIUS is not satisfied or in most transactions where the acquirer is State-controlled, then CFIUS will undertake a second-stage investigation that lasts up to an additional 45 days.

The process, the timelines, the composition of CFIUS, the protection of information, and the reforms of 2007/08 have all been designed by Congress and respective Administrations to protect national security and to do so in the context of maintaining the United States' long-standing policy openness to investment. In addition, knowing that some transactions may raise national security issues, Congress has expressly authorized CFIUS to enter into mitigation agreements with the transaction parties to address those concerns. There are many different types of methods of mitigating a transaction. Examples include establishing special security procedures at facilities that can be verified by the Government, implementing certain passivity mechanisms, or even forcing a company to divest specific assets. In short, these mitigation agreements impose measures on the parties that address national security risks.

These mitigation agreements are the pressure valve that enables CFIUS to find solutions to more difficult transactions—to welcome foreign investment and protect national security.

[3] Several offices in the Executive Office of the President also serve as observers of CFIUS.

If at the end of that 75-day period, CFIUS cannot make a decision or recommends that a transaction should be prohibited—then the matter is referred to the President who has 15 days to make a decision. Only the President has the ability to block a transaction.

In the past 27 years, the President has prohibited or unwound only three transactions. The primary reason that such activity by the President is so rare is that most transactions do not pose a national security risk or risks can be mitigated through diligent work by CFIUS. The other reason is corporate concern about reputational risk. When the President makes a formal decision on a transaction, that decision is made public. Companies that believe the President could prohibit their transaction are understandably reluctant to be subject to a public rejection. Accordingly, most companies will withdraw from the CFIUS process and abandon their transaction.

How CFIUS Has Performed

Since FINSA was enacted 10 years ago, CFIUS—in my opinion—has performed in an exceptionally professional and thoughtful manner. Congress and the American people should be proud of how well the group of individuals across the Government have carried out their duties. Their scrutiny of cases is thorough; they have protected national security; they have protected information as well as anyone in the U.S. Government; and they have preserved the reputation of the United States as open to investment from around the world. CFIUS in many respects has been a model not only within our Government but also for other countries; various nations are now considering how they can emulate the U.S. process.

That said, there is little question that the investment landscape has changed substantially in those 10 years. By far, the most important change has been the rise of China as a direct investor in the United States. Ten years ago, CFIUS would review just one or two transactions a year that had involved a Chinese acquirer—today, it is literally dozens and dozens of transactions every year. While I believe we should welcome Chinese investment and that each transaction should be judged on its own merits, these transactions have more complex financial structures, sometimes are more opaque, and come from a country where the State plays a much larger role in the economy. Often, these factors and others, raise the threats to national security. I know that fellow panelist Jim Lewis is focusing his remarks on Chinese investment and the threats it raises so I will not elaborate further.

The other development is the concern that technology is being transferred that could make our national security more vulnerable. I know that Kevin Wolf is an expert on export control laws so I'll let him elaborate on the importance of these developments.

CFIUS Reform

As for me, these changes in the investment landscape as well as the fact that it has been 10 years since CFIUS was reformed suggest that a close, sober evaluation by Congress, by the GAO, and by the Administration is in order. As with any analysis, it is best to think of any potential reforms in terms of benefits and costs, including intended and unintended consequences.

I would have three starting points beyond a cost/benefit analysis:

First, I want to note the importance of providing appropriate resources to both Treasury and other agencies for CFIUS cases. The CFIUS process is currently under stress because of a significant increase in cases, without a commensurate increase in resources. While I strongly believe that we should set good policy on the merits, we also need to provide adequate resources to effectively carry out those policies.

CFIUS reviewed over 170 transactions last year, which is the highest number since CFIUS was strengthened 10 years ago. As mentioned earlier, there is a much larger proportion of cases originating from China and that are structurally more complex. In 2017, my understanding is that CFIUS is on pace to investigate a much higher number than in 2016. There is little question in my mind that the individuals doing their jobs are under too much strain—they need more resources before we consider how to increase their work load.

I am very concerned that a significant expansion of CFIUS will overwhelm the system and significantly impact its effectiveness and ability to function. So while resources are not the issue on the table today, I do not think you can separate them from the policy if you want the system to function efficiently and effectively.

Second, as part of the new FINSA law of 2007, this Committee added an Assistant Secretary of Treasury to oversee CFIUS. The Trump administration has nominated a highly qualified individual in Heath Tarbert. This Committee approved him with near unanimous support roughly 4 months ago. Why he has not been confirmed is a mystery to me, but at a time when CFIUS is under as much strain as

it has ever been and when Congress is considering reforms that would expand CFIUS—it is past time to confirm the individual with the most direct responsibility for overseeing the system.

Third, as we consider reforming CFIUS, we should adopt a set of guiding principles to ensure that the United States both safeguards its national security and remains the destination of choice for investment:

- Minimize the opportunity for politicizing transactions.
- Keep CFIUS narrowly focused on national security and resist the impulse to use it for broader economic policy goals.
- Ensure accountability of the executive branch for protecting national security while welcoming foreign investment.
  - This means that the executive branch should find solutions by "working a problem" and use its authority to craft appropriate mitigation measures, which may mean additional resources—maybe paid by fees from the filing parties—for monitoring and verification.
  - It also means providing filing parties an opportunity to "make their case" directly to Senate-confirmed individuals so that parties to transactions are not faced with the situation where staff-level officials are deadlocked or uncommunicative and the next step is a decision by the President.
- Maintain CFIUS's focus on—and review should be triggered only by—foreign mergers and acquisitions of U.S. businesses, and not broaden the scope to sweep in thousands of commercial or licensing transactions.
- Increase scrutiny over State-controlled acquirers, including the possibility of making the filing of such transactions mandatory.

Thank you and I'm happy to field any questions.

PREPARED STATEMENT OF KEVIN J. WOLF

PARTNER, AKIN GUMP STRAUSS HAUER & FELD LLP, AND FORMER ASSISTANT SECRETARY FOR EXPORT ADMINISTRATION, DEPARTMENT OF COMMERCE

SEPTEMBER 14, 2017

Chairman Crapo, Ranking Member Brown, and other distinguished Members of the Committee. Thank you for convening this hearing and for inviting me to testify on this important national security topic.

I was last before this Committee in January 2010 for my confirmation hearing to be the Assistant Secretary of Commerce for Export Administration, a position I held until January 20, 2017. In that role, I worked closely with my colleagues within Commerce and many other agencies in shepherding the U.S. export control system. I was also a Commerce representative to the Committee on Foreign Investment in the United States.

Although I am now a partner with Akin Gump Strauss Hauer & Feld LLP, the views I express today are my own. I am not advocating for or against any potential changes to CFIUS or its legislation on behalf of another. Rather, I am here to answer your questions from the perspective of someone who has been both a Government policymaker and a practitioner for nearly 25 years in these critical and complex national security areas. I am happy to help however you see fit.

My fellow panelists have already described well the content and scope of CFIUS, so I will get straight to my main point, which is that the CFIUS and export control systems complement each other. CFIUS has the authority to control the transfer of technology of national security concerns, but only if there is a covered transaction, however defined. The export control rules regulate the transfer of specific types of technology of national security concerns regardless of whether there is a covered transaction. This means that if concerns arise about specific or general types of technology—whether as part of a CFIUS review or from any other source—then the focus, I respectfully submit, should be on controlling the technology at issue to the destinations of concern.

The export control system is already well developed and flexible enough to address exactly this issue. Yes, it can be complex, but its national security functions are not limited by the need for a transaction. Moreover, the system is designed to constantly evolve as new threats are identified, new technologies of concern are discovered, and wide-spread commercialization makes existing controls unnecessary or impossible to implement.

The most effective export controls are those that are multilateral—those that our allies and other countries also impose for common objectives. Unilateral controls—those that only one country imposes—are generally counterproductive because they create incentives for non-U.S. companies to develop the technology outside of U.S. control. The imposition of unilateral controls, however, can be an effective short-term technique for regulating the export of technology—at any stage of its development—that is newly discovered to be sensitive in general or with respect to a specific destination.

The Export Administration Regulations, implemented by the Commerce Department's Bureau of Industry and Security, have the authority to impose such controls in coordination with other departments, primarily Defense and State. The descriptions of the technology can be as broad or narrow as the national security requires. The descriptions are generally connected to physical commodities, but do not need to be. The controls can be tailored to specific countries and to nationals of those countries. Law enforcement tools can be used with respect to domestic transactions when there is a foreign party using a U.S. company as a front. Using the export control process is also an excellent check on unintended consequences because it forces policymakers to describe clearly the information to be controlled. We can discuss the details of these tools and how they fit into the multilateral control regimes and the CFIUS process later as you like.

Although I cannot discuss specific cases, I can say that other types of national security issues created by foreign direct investment include primarily those that (i) have colocation issues (e.g., acquisitions next to military facilities); (ii) create espionage risks, (iii) could reduce the benefit of Defense Department technology investments; (iv) reveal personal identifying information of concern; (v) create security of supply issues for the Defense Department, or (vi) create potential exposure for critical infrastructure, such as with the telecommunications or power grids.

In my experience, the existing CFIUS structure, authorities, and internal procedures generally allowed for the resolution of these issues quite well. The Treasury Department was an excellent honest broker and well-facilitated consensus conclusions—often after lengthy interagency discussion and always with the terrific support from the intelligence community. The agencies were always respectful of the need for a whole-of-Government decision that took into account the particular equities and expertise of the other agencies. The career staff were and remain talented, dedicated public servants.

This last point is key. Given the increase in filings, and the increase in more complex cases, the staff was being stretched thin when I was there, and I expect they are even more stretched now. They need help. They need more resources, particularly with respect to those involved in monitoring mitigation agreements and studying transactions. I make this polite suggestion not only for their benefit but for the sake of our national security. I also make the suggestion for our economic security so that the U.S. remains known as a country that welcomes foreign direct investment with the minimum necessary and quickest possible safe-harbor review burden.

Thus, when considering changes to CFIUS to address apparent gaps in national security controls associated with foreign direct investment, the questions I would ask are (i) whether the statutory authority already exists to address the issue through a regulatory or process change; (ii) whether another area of law, such as trade remedies or export controls, could address the issue more directly and without collateral consequences on other investments; or (iii) whether the solution lies in more resources to the agencies. If the answer to these questions is "no," then that is the sweet spot for consideration of change to CFIUS legislation.

For each possible change in CFIUS's scope, however, it is vital to weigh the costs. For example, if there is even a small expansion in the scope of CFIUS's review authority, then some companies may be less willing to invest in the United States with the actual or perceived extra burden and time involved in closing a transaction, particularly if there is not a significant expansion in staff. With every expansion in scope, there will be a corresponding and exponential expansion in burdens and costs generally—more regulations lead to more words, lead to more analyses of those words in novel fact patterns, lead to more filings, lead to more reviews, lead to more mitigation agreements, and on and on. Also, if the legislation becomes too prescriptive, then it may limit the ability of the Administration and staff to resolve novel national security issues in a creative way. There were many such situations over the course of the last seven years that I suspect could not have been contemplated by the original drafters of the legislation and the regulations.

On export control and CFIUS topics, I have a 3-minute, a 30-minute, and a 3-hour version. So, I will stop here with these general opening comments and look forward to answering your questions. Thank you again for spending the time to think through this complex and important national security issue.

PREPARED STATEMENT OF JAMES A. LEWIS

SENIOR VICE PRESIDENT, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES

SEPTEMBER 14, 2017

I thank the Committee for this opportunity to testify. The Department of Treasury's Committee on Foreign Investment (CFIUS) is one of the most important tools for protecting national security while also creating the conditions that enable a strong economy and an advanced technological base. CFIUS is one of three activities that protect national security related technology and the defense industrial base along with export controls and Federal investment in research and development (R&D). The CFIUS Committee has done well, but the growing volume of cases, increased complexity of acquisition transactions, and China's industrial policies pose an increasing challenge to the CFIUS process.

The U.S. created the CFIUS process to regulate foreign acquisitions of American companies in response to concerns that strategic industries were being lost to foreign competitors. The goal is to maintain an open investment environment while mitigating risk to national security. CFIUS's authorities were updated in 2007 by the Foreign Investment and National Security Act (FINSA), which expanded the Committee's remit to include homeland security, created timelines for review, and gave the President the authority to reopen and reexamine already completed transactions (known as an "Evergreen" provision). FINSA is now 10 years old and faces challenges created by a changing global economic environment.

The most important of these challenges comes from China. China is a strategic competitor who seeks way to circumvent CFIUS protections. China's industrial policies are the greatest challenge for CFIUS. The laws, policies, and regulations that were adequate in the past, whether for export control or for foreign investment, must be reviewed and reconsidered to manage the challenge America faces from China's managed economy. China's goal is to end its dependence on foreign technology and overtake the U.S., as it has overtaken other Nations.[1] This is not a military conflict, but it has deep implications for American security and for the prospects of an international system based on the rule of law and democratic norms. The fundamental issue for the U.S. and other Western Nations is how to respond to a managed economy with a well-financed strategy to create domestic industries intended to displace foreign suppliers.

Although it is a member of the World Trade Organization (WTO), China does not follow WTO rules. Its public justification for this is that China is still a developing economy and should not be held strictly accountable, but this is nonsense for the world's second largest economy. Compare the treatment of U.S. companies in China to Chinese companies in the United States. When Alibaba built a data center in Seattle, it was not forced to do this as a junior partner in a joint venture, nor was it forced to provide source code, but U.S. companies in China face these requirements. There are other countries that want to challenge the global institutions created by the U.S. and it allies after 1945, chief among them Russia, but the Russian economy is in steady decline and while Russia is dangerous in many areas, it is not an economic competitor.

One reason that China has gotten away with this for so long is that many companies have been ambivalent about pushing back. They fear retribution from China—a reasonable concern, since China is not shy about retaliating against critics—and many do not believe the United States will take action to support them against such retribution—also a reasonable concern. China is a huge market that companies are reluctant to risk, but as the consequences of China's industrial policies become clearer, company attitudes have changed and there is growing concern about unfair competition from the Chinese State.

If China followed international practices, its decisions to invest in domestic industries would be unobjectionable. There would be potentially profound effects on the global economy, but competition is the nature of the market. But China has not hesitated to extract concessions or block foreign competition in order to advance its own firms. China's 5-year plans lay out the strategic economic and technological goals that China will pursue and fund. These have had mixed success in the past, but a steady, well-funded pursuit of its economic and technological goals is one of the hallmarks of Chinese policy. China is pulling ahead because it has a strategy to build a high-tech economy and is willing to spend heavily and consistently to achieve this. We do not always want to take Chinese propaganda announcing tech-

[1] My colleague Scott Kennedy's research initiative "Made in China 2025" explores this at greater length.

nological success at face value, but China commits to research and investment programs for decades, while our spending is often limited to fits and starts.

China's announcement of an indigenously produced commercial airliner illustrates Beijing's intent to "move up the value chain," build industries, and displace Western firms. China's Soviet-supplied aircraft factories made shoddy aircraft. When China opened its market, Western firms rushed to sell aircraft. Part of the requirement for market access was coproduction, where Chinese companies worked with Western aircraft firms to make parts for Western commercial aircraft. Coproduction, over 20 years, taught Chinese companies essential production know-how, and the quality of Chinese aircraft has improved markedly. Most of this transfer did not involve IP theft. However, the Chinese Government will be tempted to use subsidies, pressure domestic airlines to buy the new Chinese plane, and barriers to foreign companies to give their manufactures an edge in China and in the global market. These practices are not uncommon as Beijing seeks to promote its domestic companies.

Semiconductors are another key industry for China and a major concern for CFIUS. Since the 1960s, the United States has been the leader in semiconductor manufacturing. A strong semiconductor sector is crucial for growth in key high tech industries and will grow more important as more devices are connected to the internet. Semiconductors enable a broad a range of industries and serves a foundational role for critical civilian and military digital technologies. Persistent Chinese efforts to acquire semiconductor technology, combined with changes in the industry, could create risks for the U.S. and opportunities for potential attackers. In the last few years, there have been a number of efforts by Chinese companies with links to the Government to buy Western semiconductor firms, using a multi-billion-dollar acquisition fund created by the Chinese Government. While the CFIUS process has been successful in blocking many of these efforts, China's policy to end its reliance on foreign semiconductors manufacturers by creating its own companies has not changed and there will be continued pressure.

Chinese policy seeks to extract technologies from Western companies; use subsidies and nontariff barriers to competition to build national champions; and then create a protected domestic market for these champions to give them an advantage as they compete globally. Huawei is the best example of a now globally dominant Chinese company built along these lines, but there are others. A senior Chinese official once remarked that if China had not blocked Google from the China market, there would be no Baidu. Various strategies are employed, using barriers to trade, security regulations, procurement mandates, acquisitions (both licit and illicit) of foreign technology, and through strategic investments in or acquisition of foreign firms. In addition, companies from the U.S. and other Western Nations have found themselves under pressure to make long-term concessions in technology transfer in exchange for market access.

Intellectual property (IP) theft is no longer the most important problem. It is easy to overstate the cost of commercial cyber-espionage. While China's policy has been to acquire Western IP from the start of the opening of its market, and while the high point of IP theft came from cyber-espionage between 2000 and 2015 (more a reflection of our lax defenses than of Chinese skill), the situation has changed considerably. Most of the estimates of the cost of Chinese commercial espionage, however, are exaggerated. A country could steal "$600 billion" in IP and not gain $600 billion in value if it is unable to turn the stolen IP into commercially valuable products. It does little good to steal IP if you do not have the expertise to use it, and until recently, this was true for China's espionage in advanced technology. What has changed in the last decades is that in many cases, China has the money and the skill to use much of the IP it has acquired licitly or illicitly. In other cases, China has realized that acquiring "know-hows" is more important than acquiring IP, and has turned to the purchase of Western companies as a key part of its new industrial policies.

Because of past technology transfers through joint ventures and coproduction, and in part because of heavy, sustained Government investment in science and research, China has developed its own innovation capabilities. In some technology areas, China may even be the world leader. This is a good thing for the global market and competition, and it should help spur a rethinking of America's relaxed approach when it comes to technology and innovation. What is not good is the Chinese Government's policy of using unfair business practices to give Chinese companies an edge in marketing their innovations.

In the worst case, stolen IP means that the victim company faces a new competitor. In China, this new competitor may have access to Government subsidies or benefit from a protected domestic market built with nontariff barriers to hobble foreign competition. Subsidized Chinese companies have an immense advantage operating from a closed domestic market and selling to an open international market.

Confronting China over these practices is long overdue, but the central issue is not IP theft but the unfair treatment of U.S. companies in China. The word that China fears is reciprocity—that they should be treated in the United States the way American companies are treated in China.

Concern over technology transfer has been an element of the U.S.–China relationship for decades, but China's growing wealth and sophistication poses a new kind of challenge U.S. regulation and policy. Moreover, China's strategies for acquiring technology and, perhaps, for circumventing FINSA, are relatively agile and attempt to take advantage of this policy gap. The long-term viability of China's managed economy model is an open question, but in the near term, it creates new risks for U.S. companies and for national security.

One question for this hearing is whether the existing tools to manage risk are adequate. These include export controls and foreign investment reviews. Another question is whether a defensive strategy that seeks to block Chinese acquisitions is enough. The answer is both cases is that there is room for improvement. Improving the ability to compete and to create new products in the United States is an essential complement of maintaining U.S. national security and leadership in technology.

We can review the question of the effectiveness of existing policy tools like CFIUS by looking at some of the ideas for CFIUS reform. The incentive for this review is that China appears to have looked for ways around FINSA regulations. This needs to be addressed by expanding the scope of covered transactions, by providing the Committee with additional flexibility for review in difficult cases, by moving from a transactional focus to better identify technology and business trends that create risk, finding ways to cooperate with foreign partners, and by ensuring it has the resources and information needed to timely decisions.

Some recommendations, such as expanding CFIUS's jurisdiction to review transactions that do not result in foreign control of a company but still allow access to technology, or expanding CFIUS authority to review overseas joint ventures, are better handled by export controls. The same is true for having CFIUS create lists of critical technology. The Departments of Defense, Commerce, and State already maintain such lists for export control purposes and while in some cases these lists need to be updated to focus on new and truly crucial technologies, another list is unnecessary.

Similarly, while it may be helpful to the CFIUS committee to have access to lists that identify countries of concern and broader technology trends, these are competencies already found in the National Intelligence Council (NIC), which already has a CFIUS support group and is required by FINSA to review CFIUS applications. The NIC would require additional resources if these tasks were added to its portfolio, but one important goal for change should be to expand CFIUS's current transactional focus.

FINSA gives the NIC a statutory role in the CFIUS process, but it does not have a "vote" on the committee. This is appropriate and should not change, both because of our long-standing principle of not giving intelligence agencies a role in policymaking and because the Departments of Defense and Justice, who are member of the intelligence community (IC), already protect IC equities in the CFIUS process.

CFIUS already has an implicit policy of greater scrutiny of transactions involving Chinese State Owned Enterprises (SOEs). These transactions already face significant hurdles, but it may be worth considering more explicit policies targeting SOEs.

Adding new Cabinet agencies that do not have a national security as a primary mission to the CFIUS committee would be inadvisable. The net effect would be to complicate a process and dilute its focus on national security. Twelve years ago, the French Government blocked the acquisition of the yogurt maker Danone (known in the U.S. as Dannon) by an American company to protect a national champion. This sounds and was ridiculous. We do not want to find ourselves in a similar situation, nor would it be advisable to make the CFIUS process more complicated. This applies to the question of mandatory filing as well. One authority provided by FINSA was the ability of the President to return to any foreign acquisition and reverse it. This "evergreen" provision creates a powerful incentive for filing.

The most difficult issue in considering how to expand the scope of covered transactions is whether to expand CFIUS authorities to cover "Greenfield" investments. This is a difficult issue because many entrepreneurs, researcher and companies welcome Chinese investment in advanced technology. American companies maintain many research facilities in China. Finding a way to better grasp the potential risks of Chines greenfield divestment would require knowing the extent to which the source of Chinese investment was actually Beijing, ensuring that export control regulations are being observed, and giving CFIUS the scope to intervene if considered necessary for national security.

The U.S. would also benefit from a more formal cooperative mechanism. Informal cooperation exists now but this could be strengthened. Japan has adopted new regulations on "inward investment" and the European Union is drafting regulation to provide guidance to its members. All of them are motivated by the same challenge (although they do not say it publicly), that challenge being China's industrial policies. There is a good opportunity now to increase formal information sharing and cooperation in these matters to ensure that if an acquisition is denied on one country that others are aware of the denial and the reasons for it.

The decision to locate CFIUS in the Treasury Department was made to show that the goal is to encourage foreign investment while mitigating any risk to national security. This decision remains sound. It would not be useful to impose a "net benefit" or "reciprocity" test on foreign investment. These considerations are best left to the market, which takes these factors into account in its pricing mechanisms. The goal in any measure to strengthen CFIUS should be keep this open investment environment.

U.S. efforts to get China to follow global norms on technology, trade, and investment is long overdue, but it will not work without a strategy on how to move ahead in technology. The United States has innate advantages, with the strongest scientific base in the world, leading technology companies, and an innovative culture that others find difficult to match. Strengthening and revitalizing the partnership among companies, universities, and Government can reignite U.S. innovation, but it will require a willingness to invest seriously in growth.

Reports that the Trump administration will challenge China over unfair trade practices are good news, but this needs to be accompanied by policies to accelerate the creation of new goods and services in the U.S. Innovation has become a buzzword and everyone is for it. Innovation means creating new products and services, either by improving existing products or by taking advantage of scientific discoveries. Companies spend heavily on developing new products, but very little on developing new ideas. A lack of support for research limits American innovation and economic growth.

Everyone agrees that innovation is essential for America prosperity and security, but America lives in a post-innovation environment of its own making. The Nation that is coasting on the science investments of the Cold War, and underinvestment in research slows growth in income and productivity. For developed economies, innovation is the best way to grow, by finding better ways to use existing resources to produce goods and services. There are many reasons why productivity growth in the United States is flat, but underinvestment in scientific research is one of them, and this creates a self-imposed disadvantage in military and economic competition with China.

The innovation ecosystem is complex, interconnected, and global, but it is "pay-to-play." Restoring U.S. strength in innovation requires investment, both by encouraging private sector investment and by Government spending in those areas, like basic research, where private sector spending is likely to be insufficient. China has allocated billions of dollars for investment for research in and acquisitions of advanced technologies that are key to future economic growth, including semiconductors, 5G telephony, artificial intelligence, and super computers. The United States allocates millions for the same efforts, meaning we are being outspent a thousand to one. We do not want to take media hyperbole about a war over AI or supercomputing too seriously, but we also do not want to watch as others pass us.

There are other areas where policy changed could improve American innovation and economic performance. The recommendations of the International Monetary Fund for the U.S. economy include tax reform, less regulation, increased infrastructure spending, deficit reduction, educational improvements, and improved trade agreements. These can be contentious issues, but a decision to match China in investment for science and technology should not face the same debate.

It is important not to exaggerate China's strength. It faces immense problems in Government debt, life-threatening pollution, mismanagement, and corruption, but under its current leaders, it intends to displace the United States and building globally dominant high tech industries is a part of this strategy. China's leaders are practical, however, and its behavior can be changed, however, if the U.S. develops a coherent strategy in cooperation with key allies. CFIUS is not the only tool we can use in this, but it is one of the most important. I thank the Committee for the opportunity to testify and look forward to any questions.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR BROWN FROM CLAY LOWERY

Q.1. In light of recent news that 143 million Americans' personal information held by Equifax was hacked, and past incidents, like the OPM breach, in which millions of Federal employees' personal information was obtained by a foreign State, it seems to me that protecting Americans from cyber-related threats is more important than ever.

In your experience, if a foreign company that may have ties to a foreign Government is trying to acquire a U.S. company that has access to the personal data of millions of Americans, what national security concerns CFIUS would consider? How would CFIUS be able to mitigate those concerns?

A.1. When investigating a foreign direct investment (FDI), CFIUS examines (i) the threat of the acquirer, including its relationship to its home Government and (ii) the vulnerability of the asset being purchased. Increasingly, a key vulnerability for CFIUS to consider is the accumulation of substantial personally identifiable data. In most cases, CFIUS should generally be able to mitigate such concerns if they present a risk to national security. In fact, I would argue CFIUS has the obligation to try to find mitigation in such cases in order to meet its dual mandate: protect national security and promote foreign investment. In cases when the national security risks cannot be mitigated, CFIUS should, if necessary, recommend to the President that he block the transaction.

Q.2. As I mentioned in my opening statement, I think we need to keep a close watch on how much of the research capabilities in agriculture, particularly R&D relating to seeds, is owned by our adversaries. I believe additional oversight of our country's agricultural assets is critical to protecting our Nation's food supply. Do you believe that agriculture and food security are important to U.S. national security? In the case of CFIUS reviews of foreign acquisitions of agricultural assets for national security risks, is USDA appropriately included in the process?

A.2. I do think food security issues can rise to the level of being national security risks and transactions may need to be reviewed by CFIUS. CFIUS has had the ability to bring appropriate expertise throughout the Government, when necessary. In my experience, USDA has been brought into CFIUS transactions when necessary and appropriate. I would, however, suggest caution with regards to the proposal to make USDA a full member of CFIUS, primarily because the vast bulk of current transactions that go through CFIUS have little to do with USDA expertise and could be a poor allocation of scarce resources.

Q.3. In your testimony and at the hearing, you suggest that CFIUS could use more resources. If its resources were increased, how could those resources be most effectively used to better protect national security? Should it be allocated to monitoring M&A activity, reviews, investigations, mitigation, or something else?

A.3. CFIUS has been overloaded for the past couple of years and this has harmed its ability to conduct its investigations in an efficient and thorough manner. While having more resources for miti-

gation monitoring is probably necessary, this could be outsourced to trusted private sector service firms. The investigation and disposition of transactions, however, must be done by the Government and this seems to be the more immediate need.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM CLAY LOWERY

Q.1. Last year, due to increasing pressure from Venezuela's economic crisis, PdVSA, Venezuela's State-owned oil company pledged 49.9 percent of its shares in U.S. oil company Citgo to Russia's Government-owned oil company, Rosneft. Citgo is owned by PdVSA, and it operates pipelines and oil refineries throughout the U.S. It is my understanding that Rosneft may have also acquired additional ownership shares of PdVSA on the open market, which could bring their ownership potential to more than 50 percent. Respected market analysts have predicted that PdVSA could default on its debt to Rosneft in the near future. If such a default were to occur, Rosneft would then acquire at least a 49.9 percent ownership stake in Citgo.

If PdVSA defaults on its debt, Rosneft would acquire, at a minimum, a near-majority ownership stake in Citgo, which has 48 petroleum product terminals, three refineries in Texas, Louisiana, and Illinois, and nine pipelines throughout the United States. In your opinion, would such an acquisition generate national security concerns?

In your opinion, should CFIUS review any acquisition of Citgo by Rosneft?

Are there any statutory limits that constrain CFIUS's authority to review foreign acquisitions of U.S.-based companies that are owned by foreign companies, as would be the case if Rosneft were to acquire Citgo?

A.1. It is hard for me to comment on this transaction because I do not have any insight into the specifics. In general, however, under the regulations (see Section 800.303 and Section 800.304), CFIUS may find a convertible debt instrument to be an instance of a "covered" transaction as defined in the regulations.

Q.2. To my knowledge, CFIUS does not have a process requiring members to recuse themselves from a review if they have conflicts with a particular transaction.

Would it concern you if members of the CFIUS had prior employment engagements, personal financial holdings, or other interests that served to impede their ability to objectively review transactions? In such cases, do you believe that CFIUS members should recuse themselves?

In your opinion, should CFIUS establish a recusal process governing member participation in the event of potential conflicts?

A.2. CFIUS is essentially a committee of individual agencies in which the Treasury Department chairs. It is not an established bureau or other legal entity of the Treasury Department. The ethics requirements and regulations of each agency are applicable to the employees of those agencies so members should be recusing themselves when appropriate under current law. In my experience, indi-

viduals within CFIUS recused themselves from transactions based—I believe—on the ethics rules and commitments that they had with their respective agencies. During my time at CFIUS, a number of officials from different agencies did recuse themselves from transactions, even in cases where the connection to the purchasing or targeted firm was tenuous.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR BROWN FROM KEVIN J. WOLF

Q.1. In light of recent news that 143 million Americans' personal information held by Equifax was hacked, and past incidents, like the OPM breach, in which millions of Federal employees' personal information was obtained by a foreign State, it seems to me that protecting Americans from cyber-related threats is more important than ever.

In your experience, if a foreign company that may have ties to a foreign Government is trying to acquire a U.S. company that has access to the personal data of millions of Americans, what national security concerns CFIUS would consider? How would CFIUS be able to mitigate those concerns?

A.1. I agree that foreign Government access to or control over PII of U.S. persons, particularly Government employees, can present national security concerns warranting CFIUS mitigation or other action. If, for example, as part of its espionage activities directed against the United States, a foreign Government were to acquire large quantities of PII about U.S. Government employees, it could mine such data for compromising or embarrassing personal information that could be used to coerce employees to engage in activities contrary to the interests of the United States. Examples of such information could be indications of a child's drug problem, extra-marital affairs, gambling problems, or large financial debts. Often people would like to keep such personal information confidential. A foreign Government could trade on this general desire to motivate such employees to engage in illegal or unethical activities in exchange for a promise to not release the comprising information. In my experience, CFIUS has been able to mitigate such issues. Although the applicable laws prohibit me from referring to any particular case, there are, in general, ways of mitigating such concerns. For example, CFIUS could require as a condition for clearance that a U.S. company be created and then managed and controlled by U.S. citizens. This would ensure U.S. person control over all U.S. person PII involved in the transaction. The foreign buyer would still receive financial gain from the transaction and engage in other activities unrelated to the PII, but would not have the ability to access the PII because of the U.S. person intermediary that was established. Although every transaction is different in terms of risk and financial considerations, other mitigation efforts could include audits of how the PII is being secured.

Q.2. Which agency, or agencies, are best equipped to identify threats from the transfer of critical technology, dual-use technology or early stage technology know-how, intellectual property theft and espionage, and cyberthreats, to name a few?

A.2. No one agency is, could, or should be solely responsible for identifying such technology and know-how. The technologies are too varied. Issues warranting technology control range, for example, from bird flu information to Artificial Intelligence software to robotics technology to advanced semiconductor production technology. There are hundreds of other examples. Different agencies have different equities and expertise, which makes them better able to identify more precisely technologies and threats of particular concern.

The Commerce Department's Bureau of Industry and Security (BIS) is, however, the best single agency to lead and coordinate efforts to identify and control such technologies. Indeed, the primary purpose for its existence and the regulations it administers—the Export Administration Regulations (EAR)—is to be responsible for such efforts. It has a staff of experts in most areas of technology, a licensing system to regulate the control of dual-use and commercial technologies of concern, policy staff to revise and update the controls, and, unlike any other export control agency, its own enforcement officials.

The list of dual-use and commercial technologies, which include know-how, that are now controlled for export is the Commerce Control List (CCL). See: *https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl.* It is a lengthy, complex list that is the result of decades of interagency and allied efforts to identify dual-use and commercial technologies that warrant control for national security, foreign policy or other reasons. The list primarily implements controls agreed to with our multilateral regime partners to regulate the flow of commercial technologies and other items that also have military, nuclear, biological/toxicological, and missile applications. It also contains some unilateral controls on items of particular concern to the United States, such as commercial satellites and related technology. It is relatively easy to update and can be revised without the need for new legislation.

The difficult part is identifying new technologies of concern, which is particularly challenging given the fast evolution of commercial technologies. (This issue is a large part of what is motivating consideration of whether to expand the scope of CFIUS reviews.) During the Obama administration, Commerce worked closely with the Defense Department, State Department, and other departments to substantially revise and update the list of military and space items warranting control. This effort, which affected hundreds of thousands of military and space items, took all available extra time of hundreds of U.S. Government experts to complete over the course of 7 years. Indeed, we only published our final military and space reform regulations in the weeks prior to the end of the Administration.

This reform effort was done on top of the existing and generally well-run interagency effort to update annually the existing lists of items controlled by the multilateral export control regimes. Regardless of what happens with the FIRRMA bill, I strongly believe that Congress should ask of, and provide support to, a massive Administration effort to identify the emerging critical technologies of concern that are not now controlled but should be. No one knows precisely what these technologies are, but BIS exists to lead such an

interagency and whole-of-Government effort to identify and control them. There is no need to create whole new systems or agencies to do exactly what BIS is already specially designed to do. BIS and the agencies it works with will, however, need additional resources to create the regular process for researching, analyzing, and defining novel technologies identified in FIRRMA that are of concern. They are not as easy to identify and describe clearly as technology for use in traditional military, nuclear, biological/toxicological, or missile applications.

With respect to the second part of your question, BIS is not the right agency to lead efforts to stem the theft of intellectual property, acts of espionage, or cyberthreats. Although BIS can certainly provide support to such efforts in several ways, such issues are better led by the Departments of Justice and Homeland Security.

Q.3. If a foreign company is engaged in any of these activities and is acquiring a U.S. firm, will CFIUS consider this as part of the review or investigation?

A.3. CFIUS indeed considers export control, IP theft, espionage, and cyber-issues when deciding whether to approve, mitigate, or block a proposed transaction. If another area of law can address the concern, such as export controls, then CFIUS does not act. If another area of law cannot, then CFIUS factors the threat into its analysis of what action it should take.

Q.4. Are there areas were CFIUS should play a larger role or have additional authority to address national security threats?

A.4. Yes. CFIUS should have more authority to: (1) control real estate transactions near sensitive military or other Government facilities; (2) share information with allies as part of its or common considerations of transactions, taking into account business proprietary and classified information sensitivities; and (3) address changes in existing relationships, such as through bankruptcies, that would create national security concerns. More importantly, CFIUS needs massively more funding and staffing to review a significant increase in covered transactions—and covered transactions that are more complex. The agencies can barely handle the workload they have now, which harms both national and economic security because of the uncertainty and delay it injects into the system. CFIUS also needs more resources in various departments to research and investigate covered transactions that are not filed with the committee.

Q.5. As I mentioned in my opening statement, I think we need to keep a close watch on how much of the research capabilities in agriculture, particularly R&D relating to seeds, is owned by our adversaries. I believe additional oversight of our country's agricultural assets is critical to protecting our Nation's food supply. Do you believe that agriculture and food security are important to U.S. national security? In the case of CFIUS reviews of foreign acquisitions of agricultural assets for national security risks, is USDA appropriately included in the process?

A.5. Yes. Without commenting on any particular case, acquisitions in the agricultural sector generally do not create national security threats. It is conceivable that a large enough one or one with a hos-

tile buyer though could present national security issues. This is why CFIUS has the authority to—and indeed does invite—agencies not normally part of CFIUS to participate if they have particular equities in the matter. In my experience, USDA and other similar agencies are routinely invited to participate in cases involving agriculture or food security, and their expertise is given great weight by the committee as part of the CFIUS review process.

Q.6. In your testimony and at the hearing, you suggest that CFIUS could use more resources. If its resources were increased, how could those resources be most effectively used to better protect national security? Should it be allocated to monitoring M&A activity, reviews, investigations, mitigation, or something else?

A.6. Yes. CFIUS needs help in all these areas. Each of the agencies, particularly the economic agencies need more people with business and national security backgrounds reviewing transactions that occur but are not filed. They need an ever-growing number of people to be involved in mitigation arrangements. Without such staff, mitigation will not be considered an option and the committee will effectively be forced to recommend a block rather than a resource-consuming mitigation arrangement. Every agency needs more subject matter experts in business and the technologies at issue. Now, the staff are taken from existing resources. As hiring freezes and budget cuts delay the recruiting of new staff, the problems compound. As the cases become more complex and more cases go to investigation, more staff are needed. Treasury and the other departments can give you a better assessment of resource needs, but, in my Government and private sector experience, resources for a significant number of new career officials is needed even without an expansion of CFIUS' scope. If it is expanded, it will take a significantly larger allocation and recruiting effort to get the staff needed to handle the hundreds or thousands of new cases that would come in.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM KEVIN J. WOLF

Q.1. Last year, due to increasing pressure from Venezuela's economic crisis, PdVSA, Venezuela's State-owned oil company pledged 49.9 percent of its shares in U.S. oil company Citgo to Russia's Government-owned oil company, Rosneft. Citgo is owned by PdVSA, and it operates pipelines and oil refineries throughout the U.S. It is my understanding that Rosneft may have also acquired additional ownership shares of PdVSA on the open market, which could bring their ownership potential to more than 50 percent. Respected market analysts have predicted that PdVSA could default on its debt to Rosneft in the near future. If such a default were to occur, Rosneft would then acquire at least a 49.9 percent ownership stake in Citgo.

If PdVSA defaults on its debt, Rosneft would acquire, at a minimum, a near-majority ownership stake in Citgo, which has 48 petroleum product terminals, three refineries in Texas, Louisiana, and Illinois, and nine pipelines throughout the United States. In your opinion, would such an acquisition generate national security concerns?

A.1. I do not know enough about the financial arrangements to be able to opine. My experience with complex cases such as this is that they require a significant amount of analysis and detail before coming to a conclusion that there are no unresolved national security risks.

Q.2. In your opinion, should CFIUS review any acquisition of Citgo by Rosneft?

A.2. I do not know, but, based on the information provided, it seems as there would be foreign ownership or control of a U.S. business.

Q.3. Are there any statutory limits that constrain CFIUS's authority to review foreign acquisitions of U.S.-based companies that are owned by foreign companies, as would be the case if Rosneft were to acquire Citgo?

A.3. I do not believe so, but would need to research the issue to be certain.

Q.4. To my knowledge, CFIUS does not have a process requiring members to recuse themselves from a review if they have conflicts with a particular transaction.

Would it concern you if members of the CFIUS had prior employment engagements, personal financial holdings, or other interests that served to impede their ability to objectively review transactions? In such cases, do you believe that CFIUS members should recuse themselves?

A.4. Yes, I would be concerned. The question describes a conflict of interest. Yes, if such conflicts exist, they should recuse themselves from the matter before the committee. If such a person refused to recuse himself or herself, I would speak up and ask that deliberations stop until the conflict issue was resolved.

Q.5. In your opinion, should CFIUS establish a recusal process governing member participation in the event of potential conflicts?

A.5. Although the idea is worth discussing, it is probably more efficient for the individual members to work with the ethics counsel at the departments for which they work to ensure their understanding of and compliance with applicable ethics rules. CFIUS is a committee; it is not a stand-alone agency. Thus, it does not have the infrastructure of a regular bureau, agency, or department to provide support to the members. Also, conflicts for Government officials do not potentially arise only in CFIUS matters, but also in many other aspects of their day-to-day work. Thus, it makes more sense for ethics education and compliance to be a focus of the employee's department. That said, your question suggests the existence of an issue that I do not know about. A reasonable response by the Treasury department CFIUS leaders if there is a possible issue would be to remind the staff and political members of the committee of their ethics obligations and that they should work with their department's counsel to understand the scope of their obligations.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR BROWN FROM JAMES A. LEWIS

Q.1. In light of recent news that 143 million Americans' personal information held by Equifax was hacked, and past incidents, like the OPM breach, in which millions of Federal employees' personal information was obtained by a foreign State, it seems to me that protecting Americans from cyber-related threats is more important than ever.

In your experience, if a foreign company that may have ties to a foreign Government is trying to acquire a U.S. company that has access to the personal data of millions of Americans, what national security concerns CFIUS would consider? How would CFIUS be able to mitigate those concerns?

A.1. I have recently written a CSIS Commentary on the risks of foreign access to data through the acquisition of American companies. Here is the link: *https://www.csis.org/analysis/understanding-ant-big-data-and-cfius*.

The gist of the essay is that CFIUS was created to protect the defense industrial base; homeland security and critical infrastructure were added by the FINSA reforms of 2007; now it is time to add access to data as a consideration. Legislation is not necessary to do this, but adding language on data to legislation would send a clear signal.

Q.2. As I mentioned in my opening statement, I think we need to keep a close watch on how much of the research capabilities in agriculture, particularly R&D relating to seeds, is owned by our adversaries. I believe additional oversight of our country's agricultural assets is critical to protecting our Nation's food supply. Do you believe that agriculture and food security are important to U.S. national security? In the case of CFIUS reviews of foreign acquisitions of agricultural assets for national security risks, is USDA appropriately included in the process?

A.2. That probability is very low that nations seeking to use force or coercion against the U.S. does will exploit food as a vulnerability. The one area where consideration of agriculture may have merit is in the acquisition of advanced research or genetic manipulation techniques. CFIUS, in these cases, could consult with USDA to consider the risk from the potential loss of intellectual property.

Q.3. In your testimony and at the hearing, you suggest that CFIUS could use more resources. If its resources were increased, how could those resources be most effectively used to better protect national security? Should it be allocated to monitoring M&A activity, reviews, investigations, mitigation, or something else?

A.3. Better tracking of M&A activity in the U.S. and abroad, including trends in research and development that could lead to new companies or products, would be useful, as would additional resources to the Intelligence Community entity that supports CFIUS (which I occasionally advise). Monitoring of risk-mitigation agreements are best performed by the Defense Security Service (DSS) and an expanded workload would require more resources.

RESPONSES TO WRITTEN QUESTIONS OF SENATOR MENENDEZ FROM JAMES A. LEWIS

Q.1. Last year, due to increasing pressure from Venezuela's economic crisis, PdVSA, Venezuela's State-owned oil company pledged 49.9 percent of its shares in U.S. oil company Citgo to Russia's Government-owned oil company, Rosneft. Citgo is owned by PdVSA, and it operates pipelines and oil refineries throughout the U.S. It is my understanding that Rosneft may have also acquired additional ownership shares of PdVSA on the open market, which could bring their ownership potential to more than 50 percent. Respected market analysts have predicted that PdVSA could default on its debt to Rosneft in the near future. If such a default were to occur, Rosneft would then acquire at least a 49.9 percent ownership stake in Citgo.

If PdVSA defaults on its debt, Rosneft would acquire, at a minimum, a near-majority ownership stake in Citgo, which has 48 petroleum product terminals, three refineries in Texas, Louisiana, and Illinois, and nine pipelines throughout the United States. In your opinion, would such an acquisition generate national security concerns?

In your opinion, should CFIUS review any acquisition of Citgo by Rosneft?

A.1. CFIUS should review this acquisition.

Q.2. Are there any statutory limits that constrain CFIUS's authority to review foreign acquisitions of U.S.-based companies that are owned by foreign companies, as would be the case if Rosneft were to acquire Citgo?

A.2. I do not believe there are limitations if some link to the U.S. can be demonstrated. The legislation proposed by Senator Cornyn would help make clear that CFIUS has the authority to review such transactions.

Q.3. To my knowledge, CFIUS does not have a process requiring members to recuse themselves from a review if they have conflicts with a particular transaction.

Would it concern you if members of the CFIUS had prior employment engagements, personal financial holdings, or other interests that served to impede their ability to objectively review transactions? In such cases, do you believe that CFIUS members should recuse themselves?

In your opinion, should CFIUS establish a recusal process governing member participation in the event of potential conflicts?

A.3. CFIUS members represent agencies and do not act in their individual capacity. Agency positions go through an internal clearance process, and the CFIUS process itself works against self-interest. If an individual representative has a conflict of interest, he or she would normally be replaced by another individual from the agency in question, but in general, what is being presented is an agency view.

ADDITIONAL MATERIAL SUPPLIED FOR THE RECORD

STATEMENT SUBMITTED BY THE RAIL SECURITY ALLIANCE

TESTIMONY OF

THE RAIL SECURITY ALLIANCE

BEFORE THE

COMMITTEE ON BANKING, HOUSING AND URBAN AFFAIRS

UNITED STATES SENATE

AT A HEARING ENTITLED,

"EXAMINING THE COMMITTEE ON

FOREIGN INVESTMENT IN THE UNITED STATES"

SEPTEMBER 14, 2017

1341 G St. NW 6th Floor| Washington, DC 20005 | 202. 466. 8700

Introduction

The Rail Security Alliance (RSA), a collaborative of American freight rail manufacturers, suppliers and other interests, appreciates the opportunity to submit testimony to the Senate Banking, Housing, and Urban Affairs to highlight the urgent need for reforms to the Committee on Foreign Investment in the United States (CFIUS). As the Committee is aware, CFIUS has long served as an important tool for protecting U.S. national security interests from being compromised by foreign investments. However, the evolution of digital technologies, increased use of murky financing by foreign investors, and a changing international landscape since the last CFIUS update in 2007, among other things, suggest that the CFIUS is very much in need of an overhaul, as it is often ill-equipped to deal with these new risks to economic and national security.

China and Chinese state-owned enterprises have particularly, and troublingly, exploited these gaps in the CFIUS process to strategically entrench itself in the U.S. freight rail manufacturing sector. Allowing China to continue to target and do harm to the stability of U.S. freight rail manufacturing not only threatens roughly 65,000 American jobs,[1] but also has the potential to severely compromise our economic and national security. Freight rail is a core component of U.S. critical infrastructure, according to the Department of Homeland Security.[2] With nearly 140,000 miles of railroad covering the United States, freight rail regularly transports sensitive materials such as oil and nuclear waste that are integral to American defense and economic infrastructure. Yet freight manufacturing – which offers Chinese interests an opportunity to offload excess capacity of both freight supplies as well as steel and other raw materials – has increasingly drawn Chinese government investment activity in the United States. Today, Chinese state-owned interests are using circuitous and anti-competitive tactics to build freight rail manufacturing capabilities in the U.S. market that are undermining U.S. industry and raising dire concerns about the economic security of the United States. However, despite the intent of Congress when it first established CFIUS over 40 years ago, the CFIUS process as we know it is not equipped to address these urgent challenges.

As Congress examines possible reforms to CFIUS to address these gaps, we ask the Committee to consider these critical facts:

- China is strategically targeting the U.S. freight rail manufacturing sector, first with aggressive and anticompetitive early moves into U.S. transit rail that have nabbed four U.S. metropolitan transit contracts thus far, and largely through anticompetitive under-bidding practices.

- With China's government picking up U.S. transit rail contracts, the Chinese are now using their rail manufacturing capabilities to take on the U.S. freight manufacturing sector.

---

[1] Oxford Economics, *Will We Derail US Freight Rolling Stock Production?*, May 2017, at 5.
[2] Department of Homeland Security, *Transportation Systems Sector Overview*, July 6, 2017. https://www.dhs.gov/transportation-systems-sector

- This activity is a pattern for China's state-owned rail sector: Over the last nine years, it has systematically wiped out the entire freight rail manufacturing capability in Australia. Without proper government oversight, the same thing could all-too-easily occur in the U.S. market.

- The upshot of such a catastrophe would be felt not only by the U.S. manufacturing sector: Forcing America's industrial, military, and other government interests to rely significantly or wholly on Chinese government-made freight rail cars raises grave security concerns.

- CFIUS has thus far failed to recognize these concerns or been able to address the implications of having the Chinese government closely involved in a core sector of our nation's infrastructure.

China's CRRC Targets U.S. Freight Rail

The "Made in China 2025" initiative, a key component of China's 13th Five-Year plan,[3] identifies the rail manufacturing sector as a top target for Chinese expansion and has driven strategic investment and financing activities of the China Railroad Rolling Stock Corporation (CRRC) in third-country markets and the United States. CRRC is wholly owned by the Government of China and it has 90 percent of China's domestic market for production of rail locomotives, bullet trains, passenger trains and metro vehicles.[4] In 2015, CRRC reported revenues of more than $37 billion[5] — significantly outpacing the entire U.S. railcar market, which had $22 billion of output during the same year.[6] According to Chinese state media, CRRC plans to increase overseas sales to $15 billion by 2020, about double the level of export orders in 2014,[7] and the U.S. market is a prime target.

The dangers to allowing CRRC's anticompetitive actions are evident in Australia, whose rail manufacturing sector CRRC entered in 2008. In less than 10 years, CRRC effectively decimated the sector, undoing the other four manufacturers in that country, which left only CRRC standing.[8] CRRC leveraged financing from its own government to help customers acquire its product at costs well below the market. Today, almost no meaningful Australian freight rolling stock manufacturing exists[9] – CRRC's Australia footprint is almost exclusively that of an assembler of Chinese-made parts and a financier of purchases from CRRC.

---

[3] U.S.-China Economic and Security Review Commission, *2016 Report to Congress*, November 2016, at 100.
[4] Langi Chiang, *China's largest train maker CRRC Corp announces 12.2 billion yuan in contracts*, South China Morning REPORT, July 23, 2015.
[5] Macquarie Research, *CRRC Corp Ltd: Too big to roll too fast*, May 20, 2016, at 3.
[6] Oxford Economics, *Will We Derail US Freight Rolling Stock Production?*, May 2017, at 24.
[7] Brenda Goh, *China Trainmaker CRRC to build more plants abroad in expansion plan: China Daily*, REUTERS, Dec. 5, 2016, http://www.reuters.com/article/us-crrc-expansion-idUSKBN13U0EJ.
[8] *Id.*
[9] *Id.* at 15-16.

In the United States, we have since 2015 witnessed CRRC establish rail assembly operations in three states, along with additional research and bidding operations in three others. By beginning with a business strategy to take market share in the U.S. transit rail manufacturing sector and deploying near-limitless financing from its home government to help lower the below-market bids for new U.S. metropolitan transit projects, CRRC has quickly established itself as an unbeatable force in U.S. transit rail competition.

Several recent cases involving CRRC bids for new transit rail projects serve as compelling examples:

- CRRC bid $567 million – roughly half the next highest bid (from Bombardier, a company with a longstanding U.S. manufacturing workforce and footprint) – to win the contract with the MBTA in Boston in 2014.[10]

- In 2016, CRRC won a contract to provide transit rail for the Chicago's CTA, bidding $226 million less than the next-highest bidder.[11]

- In early 2017, CRRC bid $137.5 million for a contract with SEPTA in Philadelphia, underbidding the next-largest bidder by $34 million.[12]

- In March 2017, CRRC finalized a contract with the Los Angeles County Metropolitan Transportation Authority for its transit rail system that could be worth up to $647 million,[13] reportedly leveraging below-market financing to enable them to undercut other bidders.

Faced with the outcomes of these anticompetitive tactics, transit rail manufacturers in the U.S. market are feeling the pinch and many have already begun to downsize U.S. manufacturing facilities and workforces,[14] with the prospects of more workforce reductions to come. Anticipating the opportunity to unseat other manufacturers here and take advantage of the opportunity that these U.S. job reductions are likely to create, CRRC most recently announced

---

[10] Bonnie Cao, *After Winning MBTA Contract, China Trainmaker CRRC Plans American Expansion*, Boston Globe, Sept. 11, 2015. https://www.bostonglobe.com/business/2015/09/11/after-winning-mbta-contract-china-trainmaker-crrc-plans-american-expansion/jnS1kU7uHWFGR9gjWmDEjM/story.html

[11] Corilyn Shropshire, *First Step to New CTA Rail Cars: Build the Factory in Chicago*, Chicago Tribune, Mar. 16, 2017. http://www.chicagotribune.com/business/ct-cta-new-railcar-plant-0316-biz-20170315-story.html

[12] Jason Laughlin, *Mass.-Based Company with Chinese Backing Beats Local Group for SEPTA Car Contract*, The Philadelphia Inquirer, Mar. 21, 2017. http://www.philly.com/philly/business/transportation/Mass-based-company-with-Chinese-backing-beats-out-local-group-for-SEPTA-car-contract.html

[13] Keith Barrow, *Los Angeles Orders CRRC Metro Cars*, International Railway Journal, Mar. 24, 2017. http://www.railjournal.com/index.php/north-america/los-angeles-orders-crrc-metro-cars.html

[14] See *UPDATE: GE closing 3 former Alstom plants in Chattanooga*, WRCB, June 21, 2016,http://www.wrcbtv.com/story/32156061/update-ge-closing-3-former-alstom-plants-in-chattanooga; *GE making layoffs at Salem plant*," WDBJ7, Mar. 24, 2017, http://www.wdbj7.com/content/news/GE-making-layoffs-at-Salem-plant-417044683.html.

that it is developing a 204,000-square foot plant in Springfield, Massachusetts, where it will assemble railcar components shipped from China to the United States.[15]

CRRC: A Case Study for CFIUS Reform

In 2016, CRRC announced a joint venture with Majestic Legend Holdings Limited and Vertex Rail Technology to create a new railcar manufacturing enterprise, Vertex Rail Corporation. This initial formation appeared to be structured as a greenfield investment, avoiding a CFIUS review, though this is mostly optical, as the company is effectively a way to enable the Chinese government investment in a subsidiary of Vertex Rail Technology. Public reports from Vertex's general counsel indicated that ownership would transfer once the company produced several hundred freight cars. Due to this takeover by the Chinese government, 55 Members of the House and 42 Senators raised concerns about this transaction and urged CFIUS to investigate. Nevertheless, Vertex announced in late 2016 that CFIUS would allow the deal to move forward. Given CRRC's existing stronghold in U.S. transit rail, the Vertex deal now provides CRRC with the opportunity to rapidly expand into the freight rail sector where additional national security risks come into play.

Implications for National Security

Unlike the U.S. maritime shipping industry, whose security is protected by the 100-year-old Jones Act – a measure that requires vessels transporting goods between U.S. ports to be U.S.-built and majority U.S.-owned – freight rail in America has been left comparatively unprotected. Yet the Department of Homeland Security (DHS) deems the U.S. rail sector as part of the nation's critical infrastructure,[16] noting that 140,000 rail miles enable U.S. freight rail to run through every major American city and every military base in the nation. Freight rail transports not only military freight and industrial products, but also nuclear material and hazardous chemicals that can be safely and effectively transported only by rail. There are very real concerns, DHS has noted, about freight rail vulnerability, including through cyber-attack. As DHS reported in 2010,

> *With the merger of information system technology and transportation infrastructure, railroad operations have become increasingly reliant on information systems and communications technologies. Rail companies have made growing use of onboard-computers, local area networks, automated equipment identifiers, global positioning system (GPS) tracking, automatic reporting of work orders to headquarters, car scheduling and train order systems, and two-way wireless communications. . .. Nearly all . . . rail cars are tagged with automatic*

---

[15] Jim Kinney, *CRRC MA Springfield plant has deal to build subway cars for Los Angeles*, MASSLIVE, Dec. 22, 2016, http://www.masslive.com/business-news/index.ssf/2016/12/crrc_plans_final_assembly_of_los_angeles.html.

[16] Presidential Policy Directive 21 (PPD-21) identifies 16 critical infrastructure sectors, including "Transportation Systems." The Department of Homeland Security defines "Freight Rail" as one of the seven key subsectors. *See generally*, PPD-21, *Critical Infrastructure Security and Resilience*, Feb. 12, 2013, https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil and *Transportation Systems Sector*, Dep't of Homeland Sec., Mar. 25, 2013, http://www.dhs.gov/transportation-systems-sector.

> *identification transponders, which automatically record and report car location as it passes a wayside detector. . .. The railroad's growing dependence on these centralized monitoring and control systems, including Centralized Traffic Control networks, prompts concerns of possible cyber-attacks upon these systems.*[17]

That assessment, written seven years ago, did not account for substantially more complex digital capabilities that have since evolved, or are in development, for U.S. freight rail cars and freight train operations. Yet the assessment underscores the clear danger of a foreign country, and particularly the Government of China and its state-owned enterprises, having undue control of freight manufacturing in the U.S. market.

Already, there are reports of Chinese manufacturers investigating the production of their own "telematics" technology to allow the monitoring and control of their freight cars.[18] Needless to say, as China's CRRC becomes more dominant as a U.S. rail manufacturer, there are urgent questions we must answer regarding whether a growing presence of – and reliance on –freight cars from the major state-owned Chinese rail enterprise could compromise the security and safety of industrial, military, and other U.S. freight shipments.

Recommendations

This hearing is an important first step to amending CFIUS to enable the U.S. Government to tackle this pressing challenge. As Congress debates this issue, we recommend the following updates be made to CFIUS:

- Expand the Committee's jurisdiction to cover greenfield investments where an investor is a foreign sovereign, state owned enterprise or is financed by such a party.
- Expanded definition of "control by a foreign government" to include the access of the buyer to below-market loans and other financing directly or indirectly from government sources.
- Systematically increased scrutiny of investments by from certain countries that pose a significant threat to the United States.
- Greater review of transactions where the company being purchased or invested in is an industry that supports the manufacturing of critical infrastructure.

Conclusion

We appreciate the Committee's interest in addressing these issues. The strategic targeting of our nation's infrastructure by the Government of China and its state-owned enterprises poses a fundamental threat not only to the economic and security of the United States, but to our country's standing as a global power. Addressing these concerns will not follow any single

---

[17] Department of Homeland Security, Transportation Systems Sector-Specific Plan: An Annex to the National Infrastructure Protection Plan (2010), at 285.

[18] *China plans 'smart trains' to take on global rail companies*, CHINA DAILY, March 10, 2016, http://english.chinamil.com.cn/news-channels/2016-03/10/content_6952271_2.htm.

solution, but we believe reforms to the CFIUS process are an essential part of protecting U.S. infrastructure from being compromised by foreign influence. To that end, we support efforts being led by Senator Cornyn to pursue needed changes to the CFIUS law, as well as other similar efforts to bolster the Administration's ability to track and protect U.S. economic interests relative to investment activity by SOEs in the rail manufacturing sector.

Thank you again for the opportunity to submit testimony and the members of RSA look forward to hearing the solutions put forward by Congress to address these threats.

LETTER SUBMITTED TO THE TRUMP ADMINISTRATION ON CHINESE EQUITY CAPS FINANCIAL SERVICES SECTOR

United States Senate
WASHINGTON, DC 20510

September 5, 2017

The Honorable Wilbur Ross
Secretary of Commerce
1401 Constitution Ave., NW
Washington, D.C. 20230

The Honorable Robert E. Lighthizer
United States Trade Representative
600 17th St., NW
Washington, D.C. 20508

The Honorable Steven Mnuchin
Secretary of the Treasury
1500 Pennsylvania Ave., NW
Washington, D.C. 20220

The Honorable Gary Cohn
Director of the National Economic Council
1600 Pennsylvania Ave., NW
Washington, D.C. 20500

Dear Secretary Ross, Secretary Mnuchin, Ambassador Lighthizer, and Director Cohn:

As the Trump Administration continues to review our nation's economic relationship with China as part of the U.S.-China Comprehensive Economic Dialogue (CED), we ask that you continue to address Chinese trade and investment barriers that harm U.S. financial institutions and their ability to grow the American economy.

U.S. financial services providers, including those in securities, banking, and insurance, face significant restrictions in the Chinese market that limit their investment and market access. China prohibits certain types of foreign financial services companies from establishing wholly-owned operations, requiring them instead to establish securities joint ventures subject to a 49 percent foreign equity cap. While the current cap that applies to securities firms reflects an increase from 33 percent, which China agreed to in 2012, U.S. companies are still required to partner with local Chinese entities that retain a majority interest in the joint venture. The life insurance foreign equity cap has not been raised from 50 percent since it was put in place in 2001, when China joined the World Trade Organization (WTO).

Such restrictions effectively block U.S. financial companies from owning and controlling their investments as they do in almost every other market in which they operate. They also harm U.S. companies in other sectors of the economy, like manufacturing, that rely on the scale, scope, and expertise of U.S. financial services providers to compete with Chinese competitors.

By contrast, Chinese financial services companies face few, if any, barriers to entry when doing business in the U.S., other than meeting prudential requirements set by Congress and our financial regulators for all financial sector participants on a non-discriminatory basis.

We understand that the Chinese have indicated a willingness to address financial services equity caps in the context of a bilateral investment treaty (BIT). While we applaud this development, we ask that the Administration prioritize work through the CED to seek a more timely solution to this problem and garner a commitment from China to allow U.S. financial services companies to own 100 percent of their Chinese operations. The Administration should continue to negotiate for the elimination of these barriers to entry so that U.S. institutions will have the same opportunities to do business in China that Chinese institutions have in the U.S. Doing so will level the playing field

between the U.S. and China, promote domestic economic growth, and ensure the protection of U.S. economic interests abroad. Thank you for your consideration of this important matter.

Sincerely,

Tim Scott
United States Senate

Tom Cotton
United States Senate

Dean Heller
United States Senate

Thom Tillis
United States Senate

Mike Crapo
United States Senate

John Cornyn
United States Senate

David Perdue
United States Senate

Rob Portman
United States Senate

Bill Cassidy, M.D.
United States Senate

Johnny Isakson
United States Senate

M. Michael Rounds
United States Senate

John Thune
United States Senate

Steve Daines
United States Senate

Richard C. Shelby
United States Senate

John Kennedy
United States Senate

Pat Toomey
United States Senate

Pre-Decisional Draft 1.0--For Discussion Purposes Only

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.

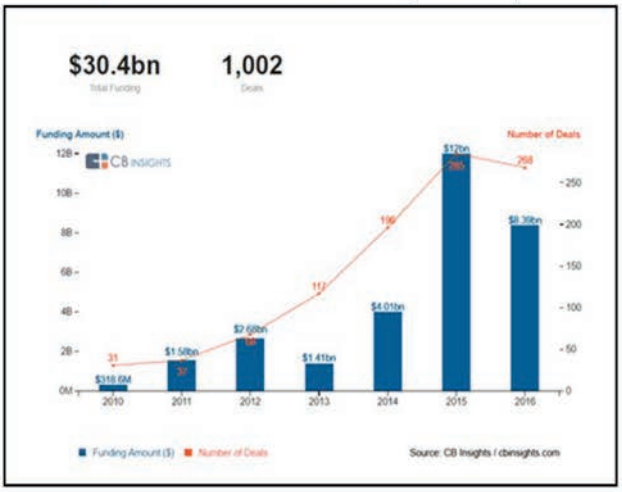
[14] "Xi Sets Targets for China's Science, Technology Progress" *Xinhua* (2016, May 30). Retrieved at http://www.xinhuanet.com

[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]

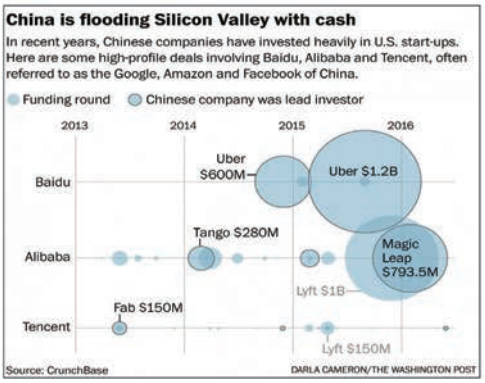
---

[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.tpinternational.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 Times* (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: PROTECTING CRITICAL TECHNOLOGIES

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: RESTRICT CHINA'S INVESTMENTS IN CRITICAL TECHNOLOGIES & EXPAND OUR NATIONAL TECHNOLOGY STRATEGY

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.

1. Data collection & analysis capability. 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.

2. Consider a lead agency for a new U.S. government China policy. 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: China Investment in Critical Technologies
Appendix 2: Select Chinese Venture Deals in 2016
Appendix 3: Case Studies of Chinese Venture Capital Firms: Sinovation and Hax
Appendix 4: Chinese Government-Backed Funds in Silicon Valley
Appendix 5: Chinese Economic and Technology Goals
Appendix 6: China's Mega Projects
Appendix 7: McKinsey Study on Industries Where China Leads in Innovation
Appendix 8: Largest Chinese Cyber Attacks
Appendix 9: U.S. Events with Chinese Sponsorship
Appendix 10: Private Sector Largely Unaware of China's Technology Transfer Threat
Appendix 11: Strengths and Weaknesses of CFIUS Process
Appendix 12: Consultations

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

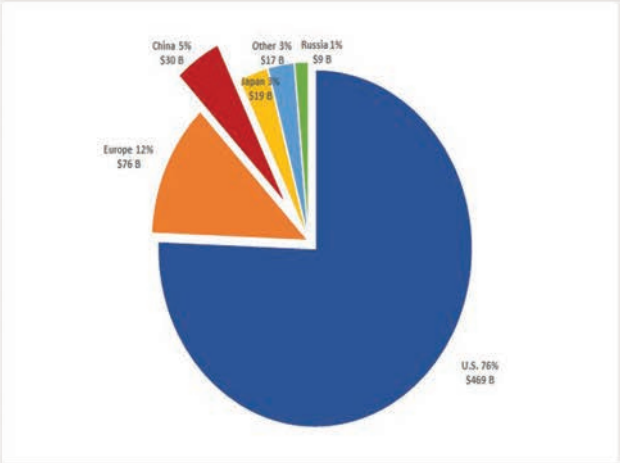


Chart 3: Chinese Investment in U.S. Artificial Intelligence Companies, 2010 - 2016

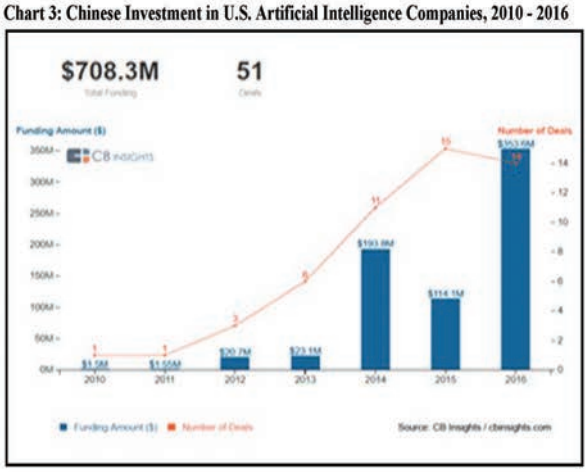


Chart 4: Chinese Investment in U.S. Robotics Companies, 2010 - 2016

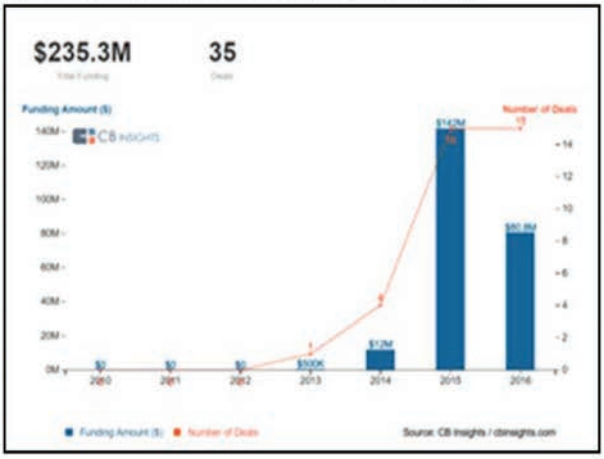


Chart 5: Chinese Investment in U.S. AR/VR Companies, 2010 - 2016

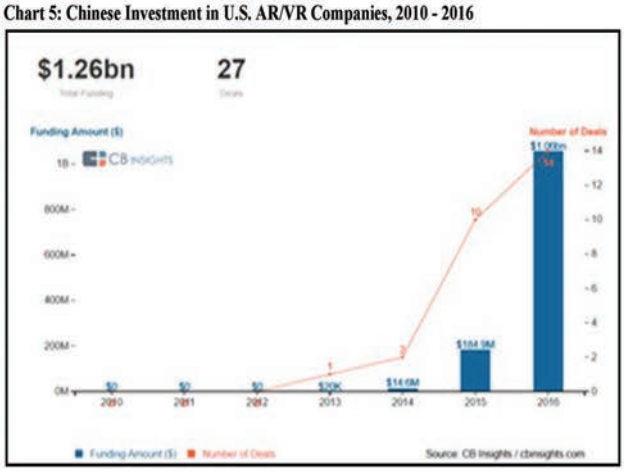
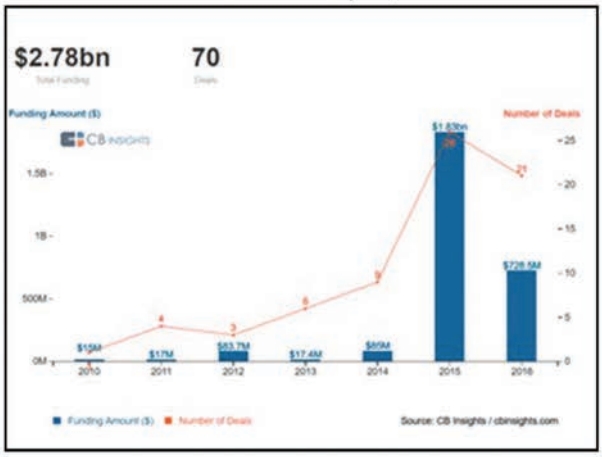


Chart 6: Chinese Investment in U.S. FinTech Companies, 2010 - 2016



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/haxdr8r#/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

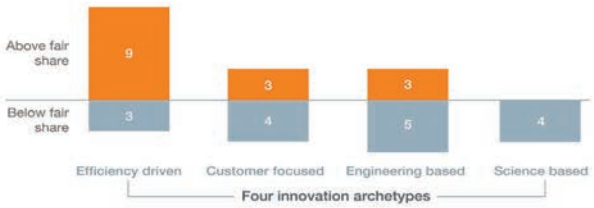
To assess the comparative innovation capability between China and the U.S., McKinsey recently analyzed in what industries China was developing an innovation lead and in what industries China is lagging.[107]

- 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

CONSULTATIONS

INTERVIEWS w/ OFFICIALS FROM POLICY, ACADEMIC AND INVESTMENT ECOSYSTEM

U.S. Government

Economic Departments, Agencies, and Councils

- Department of the Treasury
- Department of Commerce
- USTR
- National Economic Council
- Department of Energy

National Security Departments, Agencies, and Councils

- Department of Defense (JS; Net Assessment; DARPA)
- Department of State
- Department of Justice/FBI
- Department of Homeland Security
- Central Intelligence Agency
- Open Source Center
- Office of the Director of National Intelligence
- National Security Council
- Office of Science and Technology Policy

Presidential Boards and Congressional Commissions

- President's Intelligence Advisory Board
- U.S. - China Economic and Security Review Commission

Venture Capital and Financial Community

- Focus Ventures
- Kleiner Perkins
- Norwest Ventures
- Sutter Hill Ventures
- Translink Capital
- In-Q-Tel
- Silicon Valley Bank
- Cisco Ventures
- National Venture Capital Association
- Robotics Hub

Legal and Consulting Firms

- Chertoff Group
- Scowcroft Group
- Wessel Group
- Kelley Drye & Warren
- Covington and Burling
- Steptoe and Johnson
- Chain Security
- Wiley Rein
- Accenture
- Skadden Arps
- Defense Group, Inc.
- Squirrel Werkz

Academic and Research Institutions

- Stanford University
- Georgetown University
- George Washington University
- Center for Strategic and International Studies
- National Intelligence University
- RAND Corporation
- Institute for Defense Analysis
- Center for New American Security
- Heritage Foundation
- Harvard Business School
- University of California--San Diego

Other Industry Groups / Associations

- Semiconductor Industry Assn.
- U.S. Chamber of Commerce
- Institute for the Study of War

Authors

- William Hannas
- James Mulvenon

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.

Byrner, 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.