S. HRG. 116–564

CHINA: CHALLENGES FOR U.S. COMMERCE

HEARING

BEFORE THE

SUBCOMMITTEE ON SECURITY

OF THE

COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION UNITED STATES SENATE

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

MARCH 7, 2019

Printed for the use of the Committee on Commerce, Science, and Transportation

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

U.S. GOVERNMENT PUBLISHING OFFICE

52–567 PDF WASHINGTON : 2023

SENATE COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION

ONE HUNDRED SIXTEENTH CONGRESS

FIRST SESSION

ROGER WICKER, Mississippi, *Chairman*

JOHN THUNE, South Dakota
ROY BLUNT, Missouri
TED CRUZ, Texas
DEB FISCHER, Nebraska
JERRY MORAN, Kansas
DAN SULLIVAN, Alaska
CORY GARDNER, Colorado
MARSHA BLACKBURN, Tennessee
SHELLEY MOORE CAPITO, West Virginia
MIKE LEE, Utah
RON JOHNSON, Wisconsin
TODD YOUNG, Indiana
RICK SCOTT, Florida

MARIA CANTWELL, Washington, *Ranking*
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, Connecticut
BRIAN SCHATZ, Hawaii
EDWARD MARKEY, Massachusetts
TOM UDALL, New Mexico
GARY PETERS, Michigan
TAMMY BALDWIN, Wisconsin
TAMMY DUCKWORTH, Illinois
JON TESTER, Montana
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

JOHN KEAST, *Staff Director*
CRYSTAL TULLY, *Deputy Staff Director*
STEVEN WALL, *General Counsel*
KIM LIPSKY, *Democratic Staff Director*
CHRIS DAY, *Democratic Deputy Staff Director*
RENAE BLACK, *Senior Counsel*

SUBCOMMITTEE ON SECURITY

DAN SULLIVAN, Alaska, *Chairman*
ROY BLUNT, Missouri
TED CRUZ, Texas,
DEB FISCHER, Nebraska
MARSHA BLACKBURN, Tennessee
MIKE LEE, Utah
RON JOHNSON, Wisconsin
TODD YOUNG, Indiana
RICK SCOTT, Florida

EDWARD MARKEY, Massachusetts, *Ranking*
AMY KLOBUCHAR, Minnesota
RICHARD BLUMENTHAL, *Connecticut*
BRIAN SCHATZ, Hawaii
TOM UDALL, New Mexico
TAMMY DUCKWORTH, Illinois
KYRSTEN SINEMA, Arizona
JACKY ROSEN, Nevada

CONTENTS

WITNESSES

APPENDIX

CHINA: CHALLENGES FOR U.S. COMMERCE

THURSDAY, MARCH 7, 2019

U.S. SENATE,
SUBCOMMITTEE ON SECURITY,
COMMITTEE ON COMMERCE, SCIENCE, AND TRANSPORTATION,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:02 a.m. in room SD–562, Dirksen Senate Office Building, Hon. Dan Sullivan, Chairman of the Subcommittee, presiding.

Present: Senators Sullivan [presiding], Markey, Blunt, Fischer, Blackburn, Wicker, Klobuchar, Blumenthal, and Rosen.

OPENING STATEMENT OF HON. DAN SULLIVAN, U.S. SENATOR FROM ALASKA

Senator SULLIVAN. Good morning. The Subcommittee on Economics and Security of the Commerce Committee will now come to order.

This is our inaugural meeting of the newly created Subcommittee on Economics and Security, and I want to commend Chairman Wicker on his leadership in creating this subcommittee to provide a venue in Congress to focus on the nexus between commerce, economic issues, and security, and his constant focus to bolster national security and the economic competitiveness of the United States.

I'm very honored to be named as the Subcommittee Chair and I am excited to be serving with my good friend, Senator Markey, as the Subcommittee's Ranking Member.

Senator Markey has a long and accomplished career and history of public service, including his work in the House on homeland security, to close gaps in our Nation's defenses, and I look forward to working with you, Senator Markey, and the members of this Subcommittee on these important issues.

Be forewarned, we will be a very active subcommittee. There is a lot of territory and ground to cover and the Ranking Member and I have already had a number of good discussions on where we want to begin.

So where are we beginning? Well, there's no more relevant issue today in terms of the effect on our economy and our security than the strategic challenge posed by the rise of China and its subsequent retrenchment into authoritarianism and rejection of international norms and standards, which in many ways has helped so much with their own rise and lifting millions and millions of their citizens out of poverty.

The stakes are high. China is now the largest U.S. merchandise trading partner, biggest source of imports, and largest destination market for U.S. exports, outside of North America.

The bilateral relationship supports approximately one million jobs in the United States. Even in places like my great state, the great state of Alaska, China has quickly eclipsed other long-established trading partners to become our largest trading partner.

China remains a critical market for American companies and our economic and commercial ties have long been the underpinning of the relationship between our two nations. If steps are not taken by China and soon to address some of the concerns we are going to raise today, this relationship could be needlessly at risk.

While it has been suggested during the Trump Administration's ongoing trade discussions with the Chinese that they are receptive to offsetting the trade imbalance by increasing purchases of American goods, like farm products or LNG, it is imperative that the Chinese also commit to structural changes in their economy.

Those changes would include the curbing of industrial subsidies, state-owned enterprises, the bolstering of intellectual property protection, and an end to forced technology transfers, which the Chinese deny they do but we all know they do do. Also, the issue of officially sanctioned corruption globally is another issue that they need to address.

Additionally, when the United States supported China's entry into the World Trade Organization in late 2001, the expectations were that China would lower its trade barriers and follow WTO trade practices, including respecting intellectual property rights, promoting basic safety standards for exports, and not subjecting imports to illegal non-tariff barriers. China has not kept these commitments.

I saw this up close many, many years ago when I was a staffer on the National Security Council staff working for Condoleeza Rice and President George W. Bush. In a meeting I attended in the Oval Office in 2003, then Vice Premier Madam Wu Yi told the President of the United States that it was in China's interest to address the intellectual property theft that often occurs between our two countries and she would personally take steps to make sure this happened. That meeting was over 16 years ago and the IPR theft problem between the United States and China is actually worse.

President Obama also tried to stem these blatantly unfair trade practices but Beijing has not honored the "common understanding" reached between President Obama and Xi Jinping on curbing cyber hacking of government and corporate data for economic gain.

The U.S. Trade Representative estimates that Chinese theft of American intellectual property costs the U.S. economy as much as $600 billion per year, not to mention thousands of American jobs.

From foreign equity restrictions with joint venture requirements to intellectual property theft, China is pursuing its narrow economic interests in ways that contradict and undermine the global trading system, practices and a system that has fostered decades of global growth and stability and allowed China its own strong economic rise.

The Trump Administration should be commended for its reorientation of the U.S.-China relationship under its current trade nego-

tiations. The United States must insist that the bilateral trade relationship with China be defined by something understood by every American citizen: reciprocity and fairness, reciprocity and fairness.

For too long, the U.S. has accepted unfulfilled Chinese promises of greater market access even as we open our economy to Chinese companies. A demand for fairness and reciprocity should not undermine China's success as market principles would work toward long-term stabilization and state-directed economic growth can produce massive over-capacity and mountains of debt.

To put it bluntly, the United States is suffering from a decades-long promise fatigue with China. We get commitments from China, they make promises, and then they don't keep them. In order to move forward, great countries need to keep their words.

It is my hope that this hearing will inform us on some of the challenges to U.S. commerce and our current relationship with China as it relates to China's harmful practices stemming from industrial policy, intellectual property theft, forced technology transfer, cyber espionage, and many other practices.

With that, I want to thank all of our witnesses for being here today, and I now recognize the Ranking Member for any opening statement that he may have.

Senator Markey.

STATEMENT OF HON. EDWARD MARKEY,
U.S. SENATOR FROM MASSACHUSETTS

Senator MARKEY. Thank you, Mr. Chairman, very much, and thank you for your role in helping to create this very important subcommittee, the Security Subcommittee.

I think that it's time for us to have this special focus and I thank you for your leadership on this issue and I'm looking forward to partnering with you——

Senator SULLIVAN. Me, too.

Senator MARKEY.—and I, like you, want to thank Senator Wicker and Senator Cantwell for their conversations in creating this subcommittee. I think it gives us a focus that is going to be very important on issues that loom large in the 21st Century but need this specific attention because for over a century, America has enjoyed the largest, most dynamic economy in the world, consistently dominating global markets and leading the world economic order.

Our unrivaled economic production and innovation economy has made us the most prosperous nation on earth. The economic dominance has also enabled the United States to be the world's lone remaining super power. It helped us build and lead a rules-based international order that creates a level playing field for all and broadly encourages countries to aspire to America's ideals of democracy and individual liberties.

Regrettably, there are unprecedented challenges to our commercial might and to this rules-based international order, as Senator Sullivan and I are going to be focusing upon those issues.

Through a series of coordinated and concerted actions, China has launched a comprehensive and well-executed plan to dominate key high-tech industries, like 5G, telecommunications networks, artificial intelligence, and advanced manufacturing.

China's goal is to dominate these high-tech fields within the next 30 years so that they may gain a massive economic, military, and intelligence edge for decades to come, and here is the Chinese game plan.

One, direct subsidies, hundreds of billions of dollars of direct subsidies, low-interest loans, and tax breaks to Chinese industries, two, foreign investments and acquisitions, investing and acquiring foreign companies to gain access to advanced technologies, and three, forced transfer agreements forcing foreign companies wishing to invest or conduct business in China to share intellectual property and technology secrets with the Chinese Government.

These efforts pose a threat to our country's economic welfare and our national security.

In 2018, U.S. intelligence agencies stated that the Pentagon is facing an unprecedented threat to its technological and industrial base as a result of Chinese recruitment of foreign scientists, intellectual property theft, and targeted acquisitions of American companies.

The Office of U.S. Trade Representative recently issued a report highlighting China's unfair trade practices, noting not only the country's opaque regulatory system but also its poor record of adhering to its transparency obligations as a World Trade Organization member.

If we are to retain our role as a global leader committed to international norms, we have to confront this challenge head on and that's why I am so excited to explore what policy tools are at our disposal to combat these threats. Tools such as leveraging the World Trade Organization to challenge unfair Chinese industrial policies, restricting Chinese firms' ability to conduct business in the United States if they pose a threat to commerce and security, applying tailored trade restrictions to protect domestic industries threatened by unfair Chinese trade practices.

But to be clear, tariffs and tweets alone are not sufficient to address these threats to commerce nor is any bilateral deal that does not address the underlying structural problems in our economic relationship. We must be willing to make the domestic investments needed to ensure our workers, our manufacturers, and our innovators have the tools and resources they need to compete in this globalized economy.

Closing the trillion dollar backlog in infrastructure investments, investing in education and human capital development, building an intellectual bridge that transitions the workforce to the 21st Century economy and providing robust funding for science and research and development programs to help ensure America remains the world's preeminent innovation incubator.

So I'm excited to learn more from this all-star group of witnesses which have assembled here today, Mr. Chairman, and I thank you for holding this hearing. This is an incredible kick-off to a new era in this committee's history, but I think it's much needed, and again I congratulate you on this first day.

Senator SULLIVAN. Great. Thank you, Senator Markey, and as hopefully you can see, this is going to be a very strong bipartisan endeavor. I think this is an area on so many of these issues where

there is a lot of bipartisan interest and bipartisan support. So we're excited about that.

Well, I want to welcome our witnesses and some of whom I've had the opportunity to work with previously. Let me begin from left to right.

We have Mr. Daniel Rosen, who is a Partner at the Rhodium Group; Mr. Jonathan Kallmer, Executive Vice President of Policy Information Technology of the Information Technology Industry Council; Ms. Samm Sacks, Cybersecurity Policy Fellow and China Digital Economy Fellow, New America; and the Honorable Eric Rosenbach, Co-Director, Belfer Center for Science and International Affairs, at Harvard Kennedy School or, as Senator Markey would say, Hahvid Kennedy School.

Mr. Rosen,——

Senator MARKEY. By the way, that's coming from a Harvard graduate.

[Laughter.]

Senator SULLIVAN. That's where I learned this.

Mr. Rosen, you have five minutes to deliver an oral statement. A longer written statement will be included in the record. The floor is yours.

STATEMENT OF DANIEL H. ROSEN, PARTNER, RHODIUM GROUP

Mr. ROSEN. Thank you, Chairman Sullivan, Ranking Member Markey, and Members of the Subcommittee. I appreciate the opportunity to offer my views.

I approach the question based on 26 years evaluating China's economy, the prospects for U.S.-China relations, and the interests of American firms since starting my career after finishing the MSF Program at Georgetown with somebody else in the room in 1992.

I'll offer a high-level picture of China's economic practices leading to the present concerns we're talking about and I can elaborate all that in the discussion.

After starting reform and opening in 1978, China generally converged with the liberal economic practices champion by the United States, not due to pressure but because market economics simply worked better. This was in the U.S. strategic and commercial interests.

More recently, this convergence has slowed and in some cases reversed and given China's size and global footprint, that is a challenge for U.S. welfare and for other market economies, regardless of why it's happening.

While the right American policy response to these trends is not yet clear, there is now a consensus that status quo approaches must evolve. Not all challenges to the United States are maligned and the United States should in principle welcome those that accompany the betterment of one-fifth of humanity.

Our concern arises therefore not from competition per se but from the implications if a $13 trillion China today uses non-market solutions to its problems and because China is around the world now as a trader, investor, and development financier, the non-market choices it makes at home will affect conditions globally.

American engagement never rested on China becoming a market economy overnight but on China endeavoring to liberalize for its own reasons and Beijing did do that after 1978.

Concern today is not that China never tried to converge with our way of doing things but that their progress has stalled. From 2012 to 2018, the Xi era, Beijing attempted to deleverage its interbank credit markets twice, open the equity markets, empower independent boards of directors at state enterprises, achieve currency internationalization, and open the capital account. All of these economic reform moves led to many crises and were reversed.

The shadow over U.S.-China economic engagement therefore comes not because China refused to reform but because it couldn't manage to do so.

China's non-convergence with market approaches has consequences for others. We depend for our vitality on things that China's current policy choices will disrupt. I mentioned three: the financial system, rules-based pro-competitive regimes, and the sanctity of private intellectual property rights protection.

Nations that do not share the same fealty to these elements simply cannot be as engaged or interoperable with us as nations that do. This is a simple reality.

First, while Chinese authorities say they can be neutral in regulating capital access for state and non-state firms alike, the reality is that separate but equal is inherently unequal in Chinese capital markets today.

This insulates many Chinese firms from the diligence demanded of their private foreign competitors, giving them an advantage. Local government fiscal outlays and national and sub-national subsidies, as the Ranking Member noted, also distort conditions profoundly.

Second, for market systems, even-handed Rule of Law is essential, including competition policy. China today is trying to mix political guidance with commercial logic in ways that simply distort markets.

I can point to the Rhodium Group ASPI China Dashboard showing that foreign firms seeking merger review in China are six times more likely to get hauled in for review than purely Chinese parties trying to do a tie-up.

Third, and the rest of the panel is going to deal with this extensively, innovation drives modern economies, especially higher-income levels, and China's previous promises in the 2003 era and also more recently to marketize innovation have not matched up with action.

It's hard to project what the total costs of China choosing to pursue non-market models are will be for the United States, let alone to try to predict the costs for things that are hard to quantify, like our national security and our resilience.

I can talk to you more about the efforts we make as economists to try to do a better job evaluating that, but I want to just finish in 10 seconds and maybe 30 more if I can weigh on the schedule to point to three principles that I'm going to suggest for how we respond rather than absolutely specific policies. I think principle at this point is most important.

First of all, our responses for now should be provisional. They should be reversible, depending on whether China takes note of the dangers of its non-market policies right now and reverts back to a market course.

Second, our responses should be selective. Where there are national security risks or risks to our system, we must address them, but, by and large, the United States can still say yes to most Chinese manufacturing and direct investment in the United States without having to forego the benefits of that interaction in the name of our security.

And third, even to the extent we do disengage with China to some extent, should we reach that conclusion, there's a way in which we can do that peacefully with peaceful disengagement being the keyword. That is to say, without malice, with the hope that China finds its way back to the kinds of liberal ideas, small "l," that have worked so well in the advanced economies over the past century.

A final point I'll make, of course, is that openness is the wellspring of our national security and we must never forget that. Our dynamism, our exposure to ideas and practices around the world ultimately make us stronger, and there will be a large cost to us economically and otherwise to the extent we need to close doors and so we need to be very mindful about how we do that.

Thank you very much, and I look forward to the conversation.

[The prepared statement of Mr. Rosen follows:]

PREPARED STATEMENT OF DANIEL H. ROSEN, PARTNER, RHODIUM GROUP

Chairman Sullivan, Ranking Member Markey and Members of the Subcommittee, I appreciate the opportunity to offer my views at this hearing on challenges for U.S. commerce presented by China's marketplace practices. I approach this question based on 26 years of professional work evaluating the nature of China's economy, the prospects for US-China economic relations, and the interests of American firms pursuing commercial opportunities. Following eight years in the think tank sector and time in government, I established what is today Rhodium Group—a private research partnership—to conduct this analysis, where 16 researchers are presently involved in the effort.

Today I wish to offer a high-level picture of the arc of China's economic practices and priorities leading up to the present concerns. Each of the broad characterizations I offer is underpinned by a body of research which I would be pleased to elaborate in discussion, or in follow-up with you or your staff.

Background

After the start of its self-described "reform and opening" era in 1978, China generally converged—though with fits, starts and exceptions—with the liberal economic approaches championed by the United States. It did so not due to foreign pressure, but because market economics was more productive. Support for this evolution was in the United States' strategic and commercial interest. In recent years, however, this convergence has slowed and in some areas reversed. With its size and global footprint, a China pursuing a non-market oriented path—regardless of motive—will be a concern for U.S. economic welfare, and for other market economies. While the right American policy response to these trends is not yet clear, there is a consensus that status-quo approaches must evolve.

Structural Divergence

As China recovered from a state of epic impoverishment in 1978 to a normal level of development, it was bound to present a trial to the United States and the world. Since Nixon went to China the Nation's population has risen by 60 percent to 1.4 billion, and per capita incomes rose 75-fold in nominal terms: accommodating the demand and supply consequences of that was naturally a challenge. Not all challenges are malign, and the United States should welcome those that accompany the betterment of one-fifth of humanity, and the related commercial competition that

was bound to bring. The real concern arises not from competition per se, but from the implications if a $13 trillion China decides to revert to non-market solutions to managing its economy. And because China now seeks to project economic presence around the world as a trader, financial investor, commercial director investor and development finance purveyor, the non-market incentives China uses to shape its economy at home will spill over and affect economic conditions around the world.

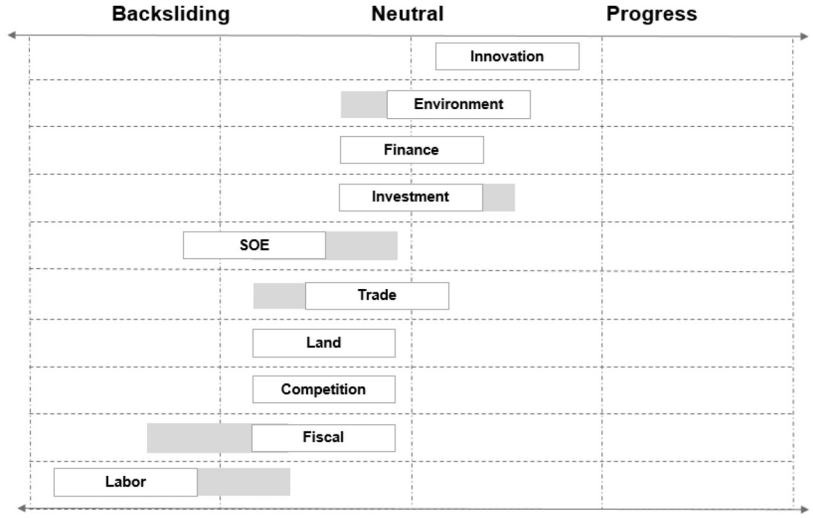
The American bet on engagement with China never rested on China becoming a market economy overnight, but on evidence that China believed its interests were served by marketization in the long-term, and, thus, that with patience (and transitional mechanisms) we would naturally converge. This depended on China endeavoring to liberalize its economy, not on pressure from American trade negotiators. Two hundred years of American foreign policy experience had taught that only China would change China. Twenty years of observation from the start of rapprochement to Deng Xiaoping's recommitment to market reform in 1992 made clear that China, and the Communist Party, was serious about change.

Concern for U.S. economic interests today stems from indications that China's drive to converge with the liberal international economic order has stalled. Xi Jinping began his tenure with a broad economic reform plan—the *Sixty Decisions*—and he endorsed a series of reform initiatives in his first term. From 2012 to 2018 Beijing attempted to deleverage the interbank credit markets (twice), open the equity markets, empower independent boards of directors at state enterprises, achieve currency internationalization, and open the capital account. All of these economic reform moves led to mini-crises and were reversed (arguably the second credit deleveraging is still underway). The shadow over US-China economic engagement comes not so much because China refused to reform but because it couldn't manage it.

Regardless of etiology, China's non-convergence with market approaches to resource allocation and regulating competition (see Figure 1) has consequences for others, including the United States. We depend for our vitality on structural conditions that China's current policy choices will disrupt. There are myriad pieces of a liberal market foundation, but three that are paramount are the financial system, rules-based pro-competitive regimes, and the sanctity of private intellectual property protection. Nations that do not share the same fealty to these elements cannot be as engaged or interoperable as nations that do.

Figure I. Net Assessment: Winter 2019 China Dashboard

Quarterly movement in IO areas



Source: Asia Society Policy Institute, Rhodium Group.

First, China's financial system serves the interests of borrowing firms with favored access to credit more than consumers or savers. While Chinese authorities assert that they can be neutral in regulating capital market access for state and non-state firms alike, the reality so far is that this separate but equal approach is inher-

ently unequal. The mushrooming volume and cost of capital have insulated many Chinese firms from the same diligence demanded of their private foreign competitors, giving them an advantage. This is true even when Chinese rates for credit are higher than foreign rates, as debt service ratios don't matter if new money to pay off old loans is always made available. In addition to capital market conditions, local government fiscal outlays and abundant national and sub-national subsidies also distort capital allocation conditions.

Second, for a market-oriented system to function, even-handed rule of law is essential. For commercial interests competition policy is a crucial aspect of this. China is today mixing political guidance with commercial considerations in corporate governance, in ways prone to change market outcomes at home and abroad. The Rhodium Group-Asia Society China Dashboard shows, for instance, that foreign firms pursuing a merger in China are about five times as likely to face Chinese government review than solely Chinese merger are. Asymmetries in trade and investment market access for foreign firms in China relative to Chinese firms abroad are an important part of uneven legal conditions. This distorts market outcomes and generally serves the interests of firms in China at the expense of Chinese consumers and foreign producers including those from the United States. China is not the only nation with border barriers to commerce higher than those maintained by the United States, and American consumers benefit from imports regardless of trade barrier differences. But at China's scale and weight in marginal global growth these distortions, like financial subsidies, can quickly put firms in other nations out of business, and thus present predatory outcomes or otherwise harm efficiency. China's international initiatives including the Belt and Road program are extending the consequences of the Chinese model worldwide.

Third, innovation drives modern economies, especially at higher income levels. In their 2013 reform program, China's leaders pledged to improve the innovation environment in China through greater emphasis on market forces. They called for "market-based technology innovation mechanisms" and said "the market is to play a key part in determining innovation programs and allocation of funds and assessing results, and administrative dominance is to be abolished." But eighteen months later *Made in China 2025* was launched, a 10-year strategic plan for achieving new levels of innovation in emerging sectors. The plan emphasized central planning, setting performance targets for domestic content and domestic control of intellectual property in critical industries. A related implementation plan set benchmarks for global market share for Chinese firms. This industrial policy approach to innovation, infused with hundreds of billions of dollars in support, will distort conditions in the innovation ecosystems of other nations, including the United States, and precipitated the aggressive 2018 U.S. Section 301 Investigation, which concluded that China's technology push was unreasonable, discriminatory and a burden on U.S. commerce.

Impacts and Options

It is impossible to confidently project the economic cost of China choosing to pursue a non-market model for the United States or U.S. manufacturing, let alone for qualitative variables such as national security or resilience. This is turn impedes cost-benefit assessment of policy options for our response. Do tariffs work? In some ways, but by depriving us of cost-efficient intermediate inputs they also diminish our export competitiveness. What is the price of disengagement? It depends on how much erosion in the value of American intellectual property if we do not respond to technology policies abroad, not on a steady-state projection of U.S. conditions. And meanwhile, if China continues to put political guidance above efficiency in the economy a financial crisis is almost inevitable, changing our China concerns from those associated with a strengthening competitor to those wrapped up in a flailing one.

The concerning features of the Chinese system described above would be present and require our attention even if China were staying the course on reform. If that were the case, the questions would be *what degree* of statism would China keep, what would it slough off, and how long would it take. Most nations, including the United States, employ some state involvement in the economy, including in the allocation of finance (Fannie Mae), tipping the competitive playing field in some industries (electric power—Tennessee Valley Authority) and promoting innovation (Sematech). The question of degree and ground rules—whether there is an overarching commitment to the primacy of market and consumer orientation—is key. And the mix is not eternal, as present debates over the role of industrial policy in the United States and other advanced economies shows. But if instead of convergence with advanced economy norms where the state plays a limited economic role Beijing claims to have an alternative, state-guided model that requires other nations

to accommodate its non-market preferences, then past assumptions about the course of engagement with China will be outdated. China has the sovereign right to choose the system it thinks best for itself, but to draw on an old saying, its freedom to swing its fist stops where our nose begins.

What to Do: Provisional, Partial, Peaceful

We are at the beginning of a national conversation—better still, an international conversation among like-minded liberal colleagues—about policy responses to new directions in China's evolution, not at the end. There are not yet refined answers. However principles to guide policy thinking are emerging.

First, our responses should be provisional. Unless everything we think we know about the relative efficiency and dynamism of free markets over state-controlled markets is wrong, the present Chinese policy turn will be a dead-end, and we will see either a diminishing threat or a reversion to market orientation in the future. Indeed, one can argue that China is already showing signs of an economic stall. Anticipating this, American policy should be built for adaptability. Any disengagement we pursue should be reversible, and our ability to reengage should be protected.

Second, our response should be partial and selective, whether in the short-term or the long-term. Where there are national security risks from commerce, or interaction threatens to disrupt the healthy functioning of our market ecosystem, we must be prepared to stand apart; but in much of our economic exchange these concerns are not present or can be mitigated. *The United States can say yes to Chinese manufactured goods and direct investment most of the time.* Blocking these flows would be gratuitous and serve no strategic purpose. Rather than plan only for all or nothing scenarios, we should build a sliding scale of engagement that fits with the likely mixed-bag that China will present—a nation somewhere in the middle between advanced economy norms and statism.

A third normative principle is for our stance on commercial interaction with China, even if emphasizing disengagement, to be *peaceful,* not just on liberal moral grounds, but for realpolitik reasons. Putting politics above economic efficiency will not work in China today, just as it failed to work in the past. When a reckoning occurs, the Chinese people will either blame bad ideas at home or hostile foreign forces abroad. It is the American interest that they correctly make the domestic diagnosis, and that when the time comes to engage in convergence again there is a foundation of goodwill between us not a sour recollection of bellicosity. If China chooses to pursue a non-market solution to its problems we can be self-protective and counsel caution to others, while at the same time avoiding malice.

Concluding Thought: Danger of Overprotection

Openness is a wellspring of American national security. In responding to concerns about China it is imperative that we preserve that asset as much as possible. Our welfare will take a hit from sliding our engagement scale in the direction of caution, at least in the short-term. Our ability to offset that cost is uncertain. We will need to enact domestic policies to replace inputs from China, adjust our trade to embrace replacement imports from other nations, and write-off many investments made in the past. There are real centers of innovation leadership in China too, and disengagement will deprive us of those. The quicker and more extensively we choose to part ways with China in areas of high-tech concern, the more urgently we need to return to responsible leadership of the advanced economy caucus. Economic protectionism has often been disguised as national security through history, and when firms reduce competition with fear-mongering our security is diminished. As we consider strategies to mitigate consequences of China's economy for our interests, we must take care to do no harm to what makes us strong in the first place.

Senator SULLIVAN. Thank you, Mr. Rosen.

Mr. Kallmer.

STATEMENT OF JOSH KALLMER, EXECUTIVE VICE PRESIDENT OF POLICY, INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI)

Mr. KALLMER. Chairman Sullivan, Ranking Member Markey, Members of the Subcommittee, thank you for inviting me to discuss this critically important topic.

My name is Josh Kallmer, and I'm the Executive Vice President for Policy at the Information Technology Industry Council or ITI.

ITI is a collection of 64 of the world's most innovative companies, representing the entire spectrum of the technology sector. Every one of our companies operates globally with the vast majority doing business in China.

We have a keen interest in this subject and we commend the Administration in working to close the deal with China that could address many of the challenges of doing business there.

I also have a personal perspective on this matter. Several years ago, I served as Deputy Assistant U.S. Trade Representative for Investment, where I was responsible for negotiating treaties to secure additional market access for U.S. companies and for representing USTR on the Committee on Foreign Investment in the United States or CFIUS and that was the context in which I had the privilege to work with you, Mr. Chairman.

As you can imagine, China was a frequent topic of my work. Let me say at the outset that our organization and the companies we represent recognize and respect the national security considerations at play here. The U.S. Government has no more solemn and important responsibility than to protect the Nation's security and we're committed to working with Congress, the executive branch, and the entire stakeholder community to address these challenges consistent with that imperative.

So I'd like to make three broad points today. The first is that tech companies face significant challenges doing business in China. For years, China has abused the privilege of being a member of the international trading system, pursuing a tapestry of policies and practices that favor Chinese companies and support the Chinese state.

China's conduct has been particularly egregious in the technology sector where it coerces foreign companies into disclosing proprietary technology, subsidizes the domestic manufacturing of many products, enacts unique domestic standards without meaningful participation from foreign companies, and restricts cross-border data flows.

My second point is that it's nevertheless important that companies continue to do business in China. Despite the challenges, U.S. business engagement in China strengthens America economically and technologically and thereby contributes to its security and its leadership.

China is an important and growing market for U.S. technology exports. Being able to sell products and services to a fifth of the world's population allows U.S. tech companies to create jobs and expand R&D investment in the U.S., which allows the United States to retain its technological edge.

Doing business in China also helps U.S. firms avoid ceding global markets to their Chinese competitors. Customers of services, such as cloud computing, whether they're Chinese, German, Brazilian, or otherwise, want services that are available globally.

If U.S. companies cannot provide cloud services to multinational customers who do business in China and around the world, Chinese firms will and furthermore, while China frequently violates its trade commitments, continued business engagement helps prevent it from flouting international norms much more substantially.

By pressing for increased market access, participation in standard-setting, and fairer treatment overall, U.S. companies help keep a spotlight on Chinese practices that preclude it from rewriting the rules of trade.

Finally, to address these challenges, we need to have a strong multidimensional partnership between companies and policymakers. Government and industry must work together to address China's conduct. Neither alone can address the challenges.

Companies understand how data moves and therefore how to mitigate risks to networks and operations. Policymakers understand how to assess security risks and how to seek changes in other countries' behavior, and we see three specific ways of doing so that I suspect we'll discuss today.

First, the tech industry welcomes the Administration's efforts to redefine the bilateral economic relationship with China and we're eager to see an agreement that meaningfully addresses its policies and practices and in that regard, Mr. Chairman, Mr. Ranking Member, I couldn't agree more with the idea that the agreement has to address the structural problems in China's market.

We look forward to supporting the Administration in working to ensure that once an agreement is reached, China abides by every single commitment that it makes.

Second, we need to ensure that the U.S. Government has the tools to address security risks effectively without impeding the innovation that supports U.S. technological leadership.

We strongly supported the development of last year's FIRRMA legislation to improve the CFIUS process and we're working actively with the Administration to modernize the export control system under the Export Control Reform Act.

We also work closely with the U.S. Government through our leadership position in the Department of Homeland Security's ICT Supply Chain Risk Management Task Force.

Finally, we need to invest in America's future to ensure that its companies and workers are as competitive as possible. That means investing in research and development in areas such as AI, 5G, enhancing STEM education, improving physical and digital infrastructure, and pursuing economic policies that allow the United States' world-class companies, entrepreneurs, and workers to compete with anyone in the world.

So I'll wrap up my opening remarks there, but let me thank you again for having me, and I'd be happy to take your questions.

[The prepared statement of Mr. Kallmer follows:]

PREPARED STATEMENT OF JOSH KALLMER, EXECUTIVE VICE PRESIDENT OF POLICY, INFORMATION TECHNOLOGY INDUSTRY COUNCIL (ITI)

Introduction

Members of the Committee, thank you for inviting me to testify today.

The Information Technology Industry Council (ITI) represents 64 of the world's leading information and communications technology (ICT) companies. We are the global voice of the tech sector and the premier advocate and thought leader in the United States and around the world for the ICT industry. ITI's member companies are comprised of leading technology and innovation companies from all corners of the ICT sector, including hardware, software, digital services, semiconductor, network equipment, Internet companies, and companies using technology to fundamentally evolve their businesses. Trade issues are critical to our members, and China is always a subject of much concern and interest.

Today's hearing is particularly timely, as China, trade, and security issues garner significant attention from the administration and Congress. Media attention and the potential for conflating these issues make it even more important to clarify and address these complex subjects. China's blatant disregard for international norms governing free trade and market access has been well-established and must be addressed. China's role and impact on the global economy is as complex as it is important, however, and its relationship with the United States is by nature both competitive and cooperative.

China has a well-established record of shifting the playing field in its favor—whether it is creating conditions for technology transfer through forced partnerships with Chinese companies; establishing ambiguous and intrusive security review regimes; or circumventing U.S. export controls laws, these unfair practices not only create an unfair economic advantage but may also, in some cases, pose a national security risk. Numerous policymakers have voiced concern regarding the security implications of China's practices. ITI members take security very seriously, including taking measures to ensure protection of their networks, customer data, IP, and threats to national security. ITI has demonstrated this commitment through our active engagement with policymakers on a number of issues, including the Committee on Foreign Investment in the U.S. (CFIUS) and export controls reform, and we welcome the opportunity to work with policymakers on the issues before us today.

While we must address China's problematic policies and practices, that is only half of the equation. The U.S. Government must also rebalance its approach to strengthening the U.S. economy and the capacity for innovation in the United States. To that end, we encourage the U.S. Government to invest in education and skills training and basic research and development, and to foster the growth of emerging technologies in the United States.

Regardless of whether China plays by the rules or not, it will continue to improve in technological development, innovation, and growth. We are no longer in a situation in which China makes technological gains simply by virtue of stealing U.S. technology. Therefore, efforts to wall the U.S. off from competition with China will not solve the problem. The United States must be prepared to compete.

In my testimony, I will outline some of the challenges that our companies face as well as what we can do about it, why the Chinese market is so important, and how we can ensure that the United States continues to foster an environment that gives the best and brightest individuals the necessary tools to develop tomorrow's most innovative technology.

Key Problems Foreign Tech Companies Face from China

Our companies face real and persistent challenges in the Chinese market, including data localization requirements, cloud services restrictions, and intrusive and undefined security review regimes that may lead to exposure of source code and other intellectual property.

Over the last decade, China has made a concerted effort not only to address legitimate cybersecurity and privacy concerns of Chinese citizens and companies but also to foster a protected space for domestic companies to gain an unfair market advantage. As the Office of the United States Trade Representative (USTR) laid out in its comprehensive Section 301 investigation findings report, China has created a tapestry of laws, regulations, standards, and practices that collectively advantage Chinese companies and create conditions for direct and indirect tech transfer.

Despite this clearly strategic approach to boost Chinese innovation and indigenous technology, the Chinese government is not a monolith. Infighting, discord, and pressure from Chinese leadership for agencies to issue regulations and demonstrate enforcement has added another layer of uncertainty and unpredictability to the Chinese market. Following passage of China's 2016 Cybersecurity Law, the tech sector has seen an unprecedented onslaught of implementing regulations, notices, measures, and standards drafted by numerous agencies within the Chinese bureaucracy, often contradicting one another. For example, the information technology standards body known as TC 260 released 110 standards for comment between November 2016 and December 2017 alone, followed by another 53 standards in 2018—accounting for two-thirds of all standards that TC 260 has released for public comment. While these standards are often classified as voluntary, they may become de facto mandatory standards, making the short comment windows even more critical. These hastily enacted regulations also allow enforcement agencies to both interpret obligations unevenly and, potentially, target foreign companies.

Broad and Ambiguous Security Review Regimes

While the Chinese government has for the most part been careful not to explicitly outline requirements for transfers of technology, source code, or other IP, the ambi-

guity and uncertainty surrounding China's numerous "security review regimes" create conditions ripe for coercion of companies to expose valuable intellectual property. For example, the Cybersecurity Law requires that companies subject themselves to intrusive security reviews for products and infrastructure to qualify as "secure and controllable." While the meaning of this term is ambiguous, the provision favors domestic companies and products as inherently more secure and is, in effect, a thinly-veiled attempt to encourage consumers to "buy domestic." Specifically, *the Cross-Border Data Transfer Measures* outline highly intrusive procedures, including background investigations of network suppliers and inspections of corporate offices.

Implicit and Explicit Technology Transfer Requirements

Chinese requirements outlined in various laws and regulations—including those that require firms to locate production or facilities in China and establish a joint venture (JV) with a Chinese partner in order to operate in China—can put their valuable technology and other intellectual property at risk. Disclosure of sensitive information can be forced through a contract (*e.g.,* JV, partnership), direct pressure from local or central governments, or governmental review or certification mechanisms. While there is nothing inherently wrong with voluntary JVs and partnerships, they become problematic when they are forced on foreign parties and when regulations stipulate either that the Chinese partner must maintain majority control of the JV or that only a Chinese company may obtain required product licenses.[1]

China has made its technology transfer objectives clear through its national strategy to promote indigenous innovation, *Made in China 2025.* The strategy explicitly promotes the transfer of technology as a means of advancing technological capability, competitiveness, and strategic emerging industries. Further, it outlines a wide-ranging effort to employ funding and the investment of significant government resources in support of key industries. While the Chinese government intended *Made in China 2025* as a means of setting aspirational goals for a domestic audience, it has nonetheless fostered an environment that makes forced technology transfer more likely and may yield overcapacity in targeted sectors. These factors create real competitiveness risks for companies and can significantly distort market supply and demand.

Restrictions on Foreign Cloud Service Providers

China's restrictions on U.S. cloud services providers (CSPs) exemplify the lack of fairness in the U.S.-China trade relationship. Foreign companies face written and unwritten requirements that do not allow foreign companies to obtain licenses to operate without a Chinese partner; force U.S. CSPs to surrender use of their brand names; and require companies to hand over operation and control of their businesses to Chinese companies in order to do business in the Chinese market. Chinese cloud services providers operating in the United States are subject to *none* of these restrictions.

Data Localization Requirements

Cross-border data flows are essential to digital trade. In 2016, over 53 percent of total U.S. service exports relied on cross-border data flows.[2] Data flows are also important for purposes of network protection, as companies rely on real-time exchanges of information across borders to identify and "patch" vulnerabilities and receive timely system and software updates. Despite numerous efforts by the U.S. tech sector to explain that data localization does not enhance—and may diminish—data security, China continues to publish new and troubling laws, regulations, and standards that require the storage of data in China. For example, China's Cybersecurity Law and other regulations seriously harm many U.S. exporters by restricting cross-border data flows and requiring firms to store and process data in China. Draft regulations—including *the Cross-Border Data Transfer Measures* and *the Critical Information Infrastructure Protection Regulatio*n (both implementing regulations of the Cybersecurity Law) contain numerous provisions that would force companies to localize certain data in China and create undue and expensive impediments to transferring business information out of China in a timely manner.

---

[1] See *Law of the People's Republic of China on Chinese-Foreign Joint Ventures; Provisions on Administration of Foreign-Invested Telecommunications Enterprises; The People's Republic of China Foreign Investment Catalogue 2017*

[2] "Cross-Border Data Flows, the Internet and What is Means for U.S. and EU Trade and Investment" (Brookings, *https://www.brookings.edu/blog/up-front/2014/10/21/cross-border-data-flows-the-internet-and-what-it-means-for-u-s-and-eu-trade-and-investment/*).

China's Standards Development

Chinese standards work and implementation of the 2017 revision of the *Standardization Law* presents a unique set of challenges, as China aims to codify the standards-development process in China.

The Law includes problematic elements such as unclear public disclosure requirements that may reveal business-sensitive information. Implementing policies of the Law, such as the *Pioneer Standards Program,* incentivize public disclosure of standards that companies use in their products. Disclosure is not mandatory, yet companies that do not disclose standards will not be recognized as standards "pioneers," which may influence consumer purchasing preferences and also renders the product ineligible to compete for government procurement contracts.

ITI supports industry-led, consensus-based international standards development, which fosters an environment in which standards are market-driven and only adopted if they benefit current technology and consumers. However, China and other nations have utilized "country-unique" standards as a policy tool to establish market access barriers and give domestic companies a competitive advantage. Given the size and influence of China's market, these national standards may influence regional trends and product development. China's exclusion or strict limitations on the participation of foreign companies in standards development bodies means that Chinese standards are developed in way that weakens interoperability and the global standards system. ITI urges Congress and the Administration to promote and strengthen the standards development process worldwide to ensure that development is fully consistent with international norms and the World Trade Organization (WTO).

China's reliance on a top-down model to promote its standards does not mean that the U.S. Government should take a similar approach. While China may propose many more standards in international standards organizations, the market should ultimately choose the most appropriate standard for consumers and the current technology. Regardless of quantity, a robust industry-led international standards development process leads to adoption of the most appropriate standard. In this regard, there is no "first mover advantage" that would give China an advantage in the development of 5G or technologies related to AI. The best way to counter China's growing influence in international standards bodies is to work within and support the international standards system. The U.S. Government can assist by promoting reliance on international standards and by investing in research and development, which will allow U.S.-based companies to continue to innovate and lead in the market.

Why Do Companies Stay in the Chinese Market?

While the Chinese market presents clear risks and impediments for foreign companies, its size and impact on the global supply chain cannot be ignored. In 2018 alone, the U.S. exported nearly $21 billion worth of ICT goods to China.[3] China is the third largest market for U.S. services exports in Asia and accounts for nearly a quarter of the global consumer market. These customers operate not only in China but also globally—and they demand products and services that operate globally. If U.S. companies leave the Chinese market, they effectively forfeit much more than the Chinese market to Chinese companies. Customers—particularly those that depend on enterprise services such as cloud computing—will seek companies that provide services in all markets in which they operate.

From both an economic and technological advantage perspective, it is not in the interest of U.S. companies, consumers, or the government to cede market share to Chinese companies. Put simply, if companies want to compete for global consumers and continue to be at the forefront of emerging technology development they must compete with Chinese companies in China and abroad.

What the U.S. Government Can Do

ITI appreciates that the U.S. Government recognizes China has instituted problematic tech policies and practices and that the administration has taken steps to address it, including USTR's Section 301 investigation and subsequent report. We routinely hear from policymakers regarding both economic and security concerns related to China, including current and future American economic competitiveness. The tools that the U.S. Government uses to address these issues, however, must be tailored and strategic to avoid causing unnecessary harm to U.S. competitiveness and innovation—which are key to the Uniteds States' economic *and* national security. I'd like to outline a few basic tenets below.

[3] "U.S. GDP was $20.89 trillion in the fourth quarter of 2018" (Bureau of Economic Analysis, *https://www.bea.gov/news/2019/initial-gross-domestic-product-4th-quarter-and-annual-2018*).

Assess Potential Security Problems from Both a Private and Public Sector Perspective

ITI respects and acknowledges national security concerns. We advocate for and work with policymakers to develop thoughtful and tailored policy approaches that consider: the problem or threat from both a public sector and private sector perspective; whether and to what extent a threat can be mitigated; and how to limit adverse or unintended effects on companies' ability to operate, compete, and innovate. It is important to recognize that the public sector often has information and political insights that the private sector does not and vice versa. While the U.S. Government has visibility into many security threats, it relies on the private sector to tell it what is happening on its networks and the steps that should be taken to mitigate risks.

While policymakers are rightly concerned about safeguarding American companies' innovations in emerging technology fields such as artificial intelligence (AI) and 5G, it is important to ensure that such safeguards do not hamstring companies' ability to develop the very technologies that the U.S. Government values for purposes of economic growth and national security. The tech sector can help in this assessment of future impacts.

The consequences of security policy to tech companies will have significant ripple effects. ITI encourages Congress and the administration to engage with the private sector on these important issues and work together to develop a strategic and coordinated approach to the potential threats and challenges posed by China and others.

Compete with China and Invest in America's Future

Preventing China from stealing technology alone will not help us achieve our goals. The U.S. Government must invest in America's future. This means investing in research and development, education, science and technology, artificial intelligence (AI), and digital infrastructure. Strengthening the business environment, the Nation's human resources, and incentivizing innovation are all key to generating sustainable economic prosperity.

If the U.S. is to preserve its technological edge, it must be prepared to step up and compete with China. Regardless of whether China plays by the rules or not, Chinese inventors, entrepreneurs, and businesses will continue innovating and will close the technological gap between the U.S. and China. While a level playing field is of course important, it is vital that the U.S. Government continue to commit to serious investments in technology to ensure American competitiveness and economic growth. China is making a concerted, strategic effort to invest and plan for its economic and technological future. The clock is running out for the U.S. Government to take action. Where the private sector in the U.S. is making significant progress in advancing the next generation of technologies and investing heavily in cutting-edge research, the U.S. Government can and should do more to support innovation.

With the world's largest and increasingly educated population, China had 4.7 million STEM graduates in 2016. To put that in perspective, that means half of China's nearly 8 million graduates are focusing on STEM, while in the U.S. less than a third—roughly 568,000 of America's 2 million graduates—major in STEM. The U.S. has invested less and less in R&D spending, where in 2016 R&D constituted about 2.7 percent of GDP.[4] China is catching up quickly with an expenditure of 2 percent of its GDP going to R&D.[5] In 2017, China accounted for 48 percent of the total global investment in artificial intelligence startup funding, while the U.S. accounted for 38 percent. In monetary terms, China invested $7.3 billion in artificial intelligence while the U.S. invested $5.77 billion.

China is also on track to outpace the United States in other areas. For example, according to a 2018 International Data Corporation report, the U.S. will spend $22 billion on smart city development this year. China is close behind with projected spending at $21 billion. As of 2015, there were 1,000 smart city pilot plans in the works worldwide, 500 of which were located in China. While 66 percent of U.S. cities are adopting smart city technologies, China's test bed for smart cities is the largest in the world.

These are just a few examples. The bottom line is that the United States is failing itself by not seriously investing in our country's technological and economic future.

Conclusion

China poses serious challenges to the tech sector. We must address these challenges aggressively yet strategically and with an eye to future ramifications for the economy and technological competitiveness. We also can neither ignore nor deny the

[4] "How much does your country invest in R&D" (UNESCO Institute for Statistics, *http://uis.unesco.org/apps/visualisations/research-and-development-spending/).*

[5] Ibid.

significant role China plays in the global economy as a key piece of the global supply chain, supplier of products and components, an innovative competitor, and a vital market for U.S. goods and services, and it would be a disservice to downplay the need to invest in U.S. companies' ability to compete with an increasingly innovative and technologically advanced China. With the right approach, we can address these serious challenges in a way that benefits the United States' economic and national security.

On behalf of all ITI members, I thank you for having me before the Committee today and commend you for your interest in examining the various challenges that China poses to the tech sector. We stand ready to work with you to address these challenges. I look forward to answering your questions.

Senator SULLIVAN. Thank you, Mr. Kallmer.

Ms. Sacks, the floor is yours.

STATEMENT OF SAMM SACKS, CYBERSECURITY POLICY AND CHINA DIGITAL ECONOMY FELLOW, NEW AMERICA

Ms. SACKS. Chairman Sullivan, Ranking Member Markey, and Members of the Subcommittee, thank you for the opportunity to testify today, and I, too, am very excited to talk about the tools we have at our disposal.

My research focuses on information and communication technology policies in China. I have worked on Chinese tech policy issues for over a decade, both with the national security community as well as the private sector and now in a research capacity.

The United States and China are now locked in a growing conflict with technology and cybersecurity at the center. The decisions made by U.S. policymakers now will have consequences for years to come.

While much attention is paid to the role played by joint ventures and China's industrial policy in tech transfer and IP theft, I will focus on three related issues but issues that have gotten less attention where I think there is an opportunity right now for action.

I will discuss the challenges posed by standards, data transfer, and emerging technology norms. First, standards. Since 2015, China has issued over 300 cybersecurity standards. I've translated and analyzed these standards in a report from last year and will be happy to discuss that in more detail in follow-on questions.

These standards pose three main issues to U.S. commerce. First, the Chinese Government can use standards to pressure companies to undergo invasive product reviews where sensitive information and source code may be exposed as part of verification and testing.

Second, they may create a competitive advantage for Chinese companies if regulators deem Chinese companies to be superior, and third, to comply with some standards, foreign firms may need to redesign products for the China market in ways that are fundamentally incompatible with the global standard system.

Another major issue for U.S. companies in China, as my colleague, Mr. Kallmer, has mentioned, is cross-border data transfers. Depending on how China's cybersecurity law is implemented, the government could require certain kinds of data to be stored within Mainland China and require security approvals for cross-border data transfer.

A third challenge is the Chinese Government's efforts to shape the norms for the use of emerging technologies. The Chinese leadership was not at the table in shaping the rules for the global

Internet and now they want to ensure that that does not happen in transformative technologies.

When it comes to issues, like AI ethics, safety, and privacy, the rules do not yet exist in China or in the rest of the world. There are some troubling indications when it comes to the Community Party's vision for the use of technology.

For example, reports say that in Xinjian, the government is detaining large numbers, upwards of hundreds of thousands to one million Muslims, and using a range of technologies in that process.

So on all of these fronts, right now, the U.S. has a window for achieving meaningful change that should not be squandered.

I have five recommendations. First, adopt a small yard/high fence approach. This is a phrase used by the former Secretary of Defense Robert Gates and it essentially means be selective about what technologies are vital to national security but be aggressive in protecting them. Overreach in the form of blanket bans, unwinding global supply chains, and discrimination against individuals is not the answer.

Second, make targeted demands of China in trade talks. As China's standards regime is still taking shape, the Chinese Government should commit to revise those standards that pressure U.S. companies to disclose source code, encryption keys, and sensitive information. On data, Beijing should commit to allow more commercial data to exit the country.

Third, work with China on setting norms for emerging technologies. The U.S. benefits from exchange and cooperation with Chinese practitioners and scholars. There are grave risks to losing visibility and insight into China's approach on these matters.

In parallel, the U.S. should coordinate with allies and partners to create international pressure on Beijing. Multilateral pressure has been effective in the past.

Last, we cannot just play defense. We must play offense. The United States must invest in its own R&D, its infrastructure, its STEM education, because China will not abandon its technological aspirations. We must be able to compete in our own right.

Thank you very much, and I look forward to your questions.

[The prepared statement of Ms. Sacks follows:]

PREPARED STATEMENT OF SAMM SACKS, CYBERSECURITY POLICY AND CHINA DIGITAL ECONOMY FELLOW, NEW AMERICA

Chairman Sullivan, Ranking Member Markey, and Members of the Subcommittee, I appreciate the opportunity to testify on the challenges China presents to U.S. commerce.

I am a Cybersecurity Policy and China Digital Economy Fellow at New America. New America is a nonpartisan think tank dedicated to the mission of realizing our Nation's highest ideals through confronting challenges caused by rapid technological and social change.

My research focuses on information and communication technology (ICT) policies in China and the U.S.-China technology relationship. I have worked on Chinese technology and cyber issues for over a decade, not only with the U.S. government, where I focused on the national security implications of technology transfer and dual-use technology, but also with the private sector, looking at China's complex and rapidly evolving regulatory environment.

This hearing could not come at a more critical moment. The United States and China are locked in a deepening conflict with technology and cybersecurity at the center. It is arguably the most significant period in the bilateral trade and investment relationship in the last four decades. The decisions made by U.S. policymakers

during this window will have consequences for U.S. national security, competitiveness, innovation, technological leadership, and norms for years to come.

China's Technology Challenge

In his testimony last week before the House Ways and Means Committee, Ambassador Lighthizer testified that technology transfer, failure to protect intellectual property (IP), large subsidies, and cyber theft of commercial secrets present major problems for the U.S. economy.[1] While much attention is paid to the role played by joint ventures (JVs) and China's industrial policy, I will focus here on three related issues that get less attention than they deserve and where there is an opportunity right now for action: standards, data flows, and emerging technology norms and governance.

While I will focus my comments on the ICT space, these challenges are not limited to companies in the technology industry. They also matter for all sectors that rely on ICT infrastructure, data, and digital platforms—including manufacturing, finance, energy, retail, healthcare, etc.

1. Market Access, IP, and Technology Transfer

The administration of President Xi Jinping is doubling down on plans to reduce reliance on foreign suppliers in what are deemed "core technologies."[2] These efforts coincide with Beijing's rapid build-out of the most comprehensive cybersecurity legal and regulatory regime of any government in the world. An interlocking system of laws, regulations, and standards create a maze of rules spanning data, online content, and critical infrastructure. While the Cybersecurity Law is the centerpiece of this system, far less understood are the hundreds of cybersecurity standards accompanying it, which in practice are vital for actually doing business on the ground.

These standards contribute to making China an increasingly difficult market for foreign firms to operate in. There are three main challenges posed by the standards regime:[3]

- *First, the Chinese government can use standards to pressure companies to undergo invasive product reviews where sensitive information and source code (even if not explicitly required) may be exposed as part of verification and testing.* This includes, for example, the security assessment process for products such as central processing units, operating systems, and office software suites. As part of the assessment, suppliers need to submit verification materials including product IP, source code, and design and development documents. China's Standardization Law (which took effect in January 2018) may require public disclosure of what are called "enterprise standards," referring to a company's proprietary product and service specifications, according to BSA's Special 301 Submission.[4]
- *Second, Chinese standards also create a competitive advantage for Chinese companies.* Chinese companies may not have the same concerns foreign companies do about providing sensitive information to the government as a condition of meeting the standards. Chinese regulators may also deem Chinese companies as being more secure under the vague criteria contained in the standards simply because they are local and therefore perceived to be more "secure and controllable" and without influence from foreign governments.
- *Third, to comply with some standards, foreign firms may need to redesign products for the China market where they are not compatible with international standards.* This is not only costly, but also creates interoperability issues with global markets.

Beijing uses vague language in standards, like in many Chinese laws and regulations, to avoid issues, such as World Trade Organization (WTO) challenges, while allowing the government maximum flexibility and discretion to apply onerous provisions when it sees fit. Internationally Beijing must disclose required standards to

---

[1] Robert Lighthizer, "Opening Statement of USTR Robert Lighthizer to the House Ways and Means Committee," February 27, 2019, *https://ustr.gov/about-us/policy-offices/press-office/press-releases/2019/february/opening-statement-ustr-robert.*

[2] Paul Triolo, Graham Webster, Lorand Laskai, and Katharin Tai, "Xi Jinping Puts 'Indigenous Innovation' and 'Core Technologies' at the Center of Development Priorities," *DigiChina,* New America, May 2, 2018, *https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/.*

[3] Samm Sacks and Manyi Kathy Li, "How Chinese Cybersecurity Standards Impact Doing Business in China," *CSIS Briefs,* Center for Strategic & International Studies, August 2 2018, *https://www.csis.org/analysis/how-chinese-cybersecurity-standards-impact-doing-business-china.*

[4] BSA / The Software Alliance, "Special 301 Submission," February 8, 2018, *https://www.bsa.org/~/media/Files/Policy/Trade/BSA2018Special301.pdf.*

the WTO. However, in 2017 the government downgraded over 1,000 Chinese standards submitted to the WTO from required national standards to recommendations.[5]

Although officially most standards are deemed "recommended," in practice many may often be required to do business in China. This is the case when standards are listed as procurement requirements for government or state-owned enterprises. Beyond government customers, some Chinese customers may not buy from vendors who lack a certification associated with certain standards. There have been cases in which customer deals do not go through because a product lacks a certain certification.

Many more standards are likely to come, as Beijing is still only in the early stages of a national effort to build out its cybersecurity standards regime. Many existing standards are still only in draft form.

For more details on China's cybersecurity standards regime, please see the report I wrote in my previous position at the Center for Strategic & International Studies.[6] The report includes our translation and analysis of more than 300 standards dating back to 2015, when the Cybersecurity Law drafting process began.

2. Data Localization

Restrictions on cross-border data flows represent one of the top problems for U.S. companies in China. According to Article 37 of China's Cybersecurity Law: "Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China."[7] Depending on how it is implemented, this provision could require certain kinds of data to be stored within mainland China and require security approvals for cross-border data transfer.

The Chinese government is still defining "personal information" and "important data," as well as what sectors fall under "critical information infrastructure" (CII), under separate measures still in draft form,[8] but there are concerns that the scope could be vast and ambiguous.[9]

As the government finalizes these draft requirements amid much internal debate, it is important to keep in mind that there are also competing voices in China advocating for more alignment with international practices. Key players in China's private sector have argued that cutting off cross-border data flows will hurt the country's global economic goals; in fact, one of the main reasons why Beijing has yet to finalize the cross-border data flow measures is that there has been so much pushback from Chinese industry seeking global markets.

3. Leadership in Technology Norms and Governance

Artificial intelligence (AI), the Internet of Things (IoT), and the collection and use of the data involved present new challenges when it comes to technology norms and governance. The rules do not yet exist when it comes to complex questions related to ethics, safety, privacy, and discrimination.

Chinese scholars, practitioners, and the government are beginning to grapple with these challenges in often positive ways. There is a growing field of public conversations and legal scholarship in China devoted to topics ranging from the right to con-

---

[5] "396-xiang Qiangzhixing Guojia Biaozhun Feizhi 1077-xiang Qiangzhixing Guojia Biaozhun Zhuanhua" [396 Mandatory National Standards Abolished, 1077 National Standards Transformed], Ministry of Commerce of the People's Republic of China, April 1, 2017, *http://chinawto.mofcom.gov.cn/article/i/ac/201704/20170402545384.shtml.*

[6] Sacks and Li, "How Chinese Cybersecurity Standards Impact Doing Business in China."

[7] A translation of China's Cybersecurity Law is available at: *https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/*.

[8] "Measures on Security Assessment of Cross-border Transfer of Personal Information & Important Data (Draft for comment)" and separate standard Information Security Technology—Guidelines for Data Cross-Border Transfer Security Assessment (draft for comment) together are meant to flesh out technical guidelines assessing cross-border data transfers. LINK See also Samm Sacks, Paul Triolo, and Graham Webster, "Beyond the Worst-Case Assumptions on China's Cybersecurity Law," *DigiChina,* New America, October 13, 2017, *https://www.newamerica.org/cybersecurity-initiative/blog/beyond-worst-case-assumptions-chinas-cybersecurity-law/*

[9] According to the latest publicly available draft, all "network operators" will be subject to assessments before exporting data out of China. In practice, this could mean anyone who owns and operates an IT network. Industry sources report the government may have walked this back recently to focus just on CII operators, but there is still tremendous regulatory uncertainty given that the definition of CII itself is up in the air. The May 27, 2017, version gives a sweeping definition of "important data," spanning that which can "influence or harm the government, state, military, economy, culture, society, technology, information . . . and other national security matters."

test algorithmic decisions to bias and discrimination in AI—similar questions under discussion among leading AI thinkers in the United States.[10]

Last year, China took a major step in asserting leadership in AI governance by hosting a major international AI standards meeting in Beijing and publishing an AI standards white paper that underlined the need for rules of the road when it comes to AI ethics, privacy, and safety.[11] Chinese authorities see this as a way to take a leading role in international governance, reflecting long-standing concerns that Chinese representatives were not at the table to help set the rules of the game for the global Internet. The Chinese government wants to make sure that this does not happen with the next generation of transformative technology, now that China has become a technology power with a sizeable market and leading technology companies.

With AI governance still in its early stages, it is too early to know what approach China will take; however, in some areas there are very troubling indications when it comes to the Communist Party's vision for the use of technology.

Reputable reports say that in Xinjiang, the government is detaining large numbers of Muslims and using a range of technologies in the process. Biometric scans, facial recognition, devices that scan smartphones for encrypted chats, and high-tech big data monitoring systems are enabling the mass surveillance and incarceration of Uighurs and other citizens, with estimates ranging from hundreds of thousands to as many as one million people affected.[12]

It is not clear whether the Chinese government plans to expand the model for how technology is being used by security services in Xinjiang to other parts of China, but we cannot ignore that possibility that it could in the future.

There is tremendous uncertainty in China and the rest of the world about how to shape rules and norms around new technologies in ways that will bring benefits to humanity. China aspires to play a leading role in this conversation in ways that will have ramifications for U.S. companies doing business in China, and, more broadly, for the formation of global governance frameworks for the use of technology.

Recommendations for U.S. Policy Toward China

As Ambassador Lighthizer testified last week, the U.S. government is engaged in "very intense, extremely serious, and very specific negotiation with China on crucial structural issues."[13] This presents a window for achieving meaningful change that should not be squandered.

I have five recommendations:

1. *Adopt a "small yard, high fence" approach.* The question is how to address the challenges posed by China in a way that does not undermine ourselves in the process. In a recent article for *Foreign Affairs,* my colleague Lorand Laskai and I argue for an approach based on what the former Secretary of Defense Robert Gates called "small yard, high fence." This means being selective about what technologies are vital to U.S. national security, but being aggressive in protecting them.[14]

   Overreach in the form of blanket bans, unwinding global supply chains, and discrimination based on national origin is not the answer. Tools like the Committee on Foreign Investment in the United States (CFIUS), export controls, and law enforcement are designed to be used as scalpels, not blunt instruments.

   Overreach has costs for U.S. security, competitiveness, and innovation. As my New America colleague Graham Webster writes for *MIT Technology Review,* there may be greater harm to U.S. interests in viewing China's technological

[10] I recently participated in a Track 2 dialogue on privacy with Berkeley Law and Peking University Law. The link to the public portion of the conference is available here: *https://www.law.berkeley.edu/research/bclt/bcltevents/2019-privacy-and-cybersecurity-law-developments/agenda/.*

[11] Jeff Ding, Paul Triolo, and Samm Sacks, "Chinese Interests Take a Big Seat at the AI Governance Table," *DigiChina,* New America, June 20, 2018, *https://www.newamerica.org/cybersecurity-initiative/digichina/blog/chinese-interests-take-big-seat-ai-governance-table/.*

[12] Josh Chin and Clemente Burge, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life," *The Wall Street Journal,* December 19, 2018, *https://www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355.*

[13] Lighthizer, "Opening Statement of USTR Robert Lighthizer to the House Ways and Means Committee."

[14] Lorand Laskai and Samm Sacks, "The Right Way to Protect America's Innovation Advantage," *Foreign Affairs,* October 23, 2018, *https://www.foreignaffairs.com/articles/2018–10–23/right-way-protect-americas-innovation-advantage.*

ambitions as an existential struggle between two competing blocs.[15] That is because the United States and China belong to an interconnected system when it comes to research, development, and manufacturing. Innovation by American companies is fueled by access to the Chinese market. The leading semiconductor manufacturers make substantial profits in China. They then plow a major portion of those profits back into R&D in order to stay competitive in emerging technologies like 5G.

Unlike the Cold War space race with the Soviet Union, the line between U.S. and Chinese technological development is not as clear as the political border between the two countries. Today, government scientists have been replaced by international corporations and diffuse global networks of entrepreneurs, researchers, and venture capitalists.[16]

Innovation flows both ways across the Pacific. China is emerging as an AI powerhouse, with Chinese start-ups excelling in several areas, including computer vision, speech recognition, and machine translation. If U.S. companies are to have any chance of keeping up, they will need access to Chinese research, talent, and expertise.

2. *Targeted demands in China trade talks.* As U.S. and Chinese negotiators work to complete a trade deal, the U.S. side should structure its demands of Beijing to focus on the following issues which will have significant effect on the ability of U.S. companies to do business in China. By prioritizing the following three issues, the U.S. side may have a shot at achieving more than just a cosmetic deal with Beijing. These do not require that Beijing dismantle state capitalism or abandon its technological ambitions, but they could result in meaningful changes for doing business in China:

   a. *Standards:* Since China's standards regime is still taking shape, this is an area upon which the United States should press Beijing. The Chinese government should commit to revise regulations and standards that pressure U.S. companies to disclose source code, encryption keys, and other sensitive information such as proprietary product specifications in exchange for market access. Any government reviews should be conducted in a non-arbitrary and transparent manner, and include international third-party accredited bodies.[17]

   b. *Data Flows:* Beijing has yet to finalize the scope of what kind of data must be stored locally under the pending definition of critical information infrastructure. Beijing should commit to allow more commercial data to exit the country without undergoing opaque and arbitrary security audits. The final version of the relevant regulations on the issue should spell this scope out in clear terms. Beijing should also sign onto the Asia-Pacific Economic Cooperation's (APEC's) Cross Border Privacy Rules System (CBPRs)[18] to facilitate cross-border data transfers with the United States. Since Beijing is concerned with new U.S. restrictions on U.S. citizen data under the expanded CFIUS regime, the U.S. side should agree to its own security reviews involving access to U.S. citizen data in a narrow fashion.

   c. *IP Theft:* On IP theft, Beijing should commit to impose criminal penalties, including jail time (not just fines) against individuals as a deterrent against IP theft. It also should agree to put in place measures that protect confidential business information during government review processes, including a dispute channel to address conflicts of interest and the types of information requested, according to the U.S. China Business Council.[19]

      Robust verification measures should be put in place to backstop commitments made by Beijing. China did not live up to its commitments not to conduct cyber industrial espionage under the 2015 Xi-Obama cyber agreement. A compliance monitoring system focused specifically on IP and tech transfer should be used to scrutinize practices, procedures, and systems of violators.

---

[15] Graham Webster, "The U.S. and China Aren't in a Cold War, So Stop Calling it That," *MIT Technology Review,* December 19, 2018, *https://www.technologyreview.com/s/612602/the-us-and-china-arent-in-a-cold-war-so-stop-calling-it-that/*.

[16] Laskai and Sacks, "The Right Way to Protect America's Innovation Advantage."

[17] BSA / The Software Alliance, "Special 301 Submission."

[18] See: *http://cbprs.org/*.

[19] US-China Business Council, "US-China Business Council Statement on Section 301 Report," March 22, 2018, *https://www.uschina.org/media/press/us-china-business-council-statement-section-301-report.*

3. Work with China on setting norms for emerging technologies. As governments around the world grapple with how to set norms and shape governance for emerging technologies, the United States benefits from cooperation and exchange with Chinese officials, companies, and policy thinkers. There are risks to losing visibility and insight into what China is doing on this front. It is in the U.S. interest to work with China to set rules on AI ethics and safety. Joint research and other partnerships provide this lens and channel.
4. *Coordinate with allies and partners to create international pressure on Beijing.* Multilateral pressure has proven successful in the past. For example, in 2009 a coalition including the United States, Japan, and Europe combined efforts to pressure the Chinese government to suspend a requirement that screening software ("Green Dam Youth Escort") with surveillance capabilities be installed on computers sold in China. The United States should build upon the alliance structures that have been successful since the end of World War II. Unilateral action will not only compel China to retaliate against U.S. companies; it will make Beijing double down on the very structural problems we want to address, feeding Beijing's own narrative about cybersecurity governance.
5. The United States must play offense by investing in its own R&D, infrastructure, STEM education, and a capital market that rewards investment. China will continue to invest in closing the technology gap with the United States regardless of our actions, so the United States must be able to compete through its own technological and economic leadership.

Senator SULLIVAN. Thank you, Ms. Sacks.

And next we have the Honorable Eric Rosenbach.

STATEMENT OF HON. ERIC ROSENBACH, CO-DIRECTOR, BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, HARVARD KENNEDY SCHOOL, FORMER DOD CHIEF OF STAFF; FORMER ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY

Mr. ROSENBACH. Thank you, Mr. Chairman, Ranking Member. A pleasure to see you, Mr. Chairman, after working with you to get the brigade in Alaska, and Ranking Member, Senator Markey, thank you for everything you do for Massachusetts and your recent visit to the Kennedy School.

This is the Information Age and information is now the world's most consequential and contested geopolitical resource. The world's most profitable businesses have understood for years that data is the new oil.

Political operatives and, unfortunately, foreign intelligence operatives, as well, have shown that data-driven social media is the key to influencing public opinion.

Leading researchers in the area of artificial intelligence know that good data, not just algorithms, will allow companies and nations to gain a competitive edge.

In the 1990s, America's supremacy in information technologies and the Internet seemed unassailable. Unfortunately, as the importance of information as a geopolitical resource has waxed, U.S. dominance has waned. That's why this hearing is so important.

China is moving very quickly into the Information Age with a strategic approach that bolsters their national interests. The United States, on the other hand, seems to be standing by, beholden by large tech companies focused primarily on connecting more people to generate more data to ensure more clicks on advertising links.

In the absence of a national strategy to protect Americans' data, promote competitiveness of American firms, and secure our infor-

mation and technology infrastructure, the U.S. risks ceding its leadership role in the Information Age.

As you heard over the past decade, China's pursued a national strategy to challenge U.S. global leadership in the Information Age. There are two things in particular that I'd like to hit on.

First, one of the best-known Chinese national champions is Huawei, now the largest telecom producer in the world. The significant resources that Huawei derives from the backing of the Chinese Government puts American and European telecom firms at a clear disadvantage and this comes in particular when it comes to developing and deploying some of the technology necessary for the next generation of broadband networks. Clearly, allowing Huawei equipment into the U.S. 5G backbone would be a grave national security concern.

The Chinese Government has also devoted significant military intelligence capabilities to stealing the data and intellectual property needed to fulfill the ambitious goals established by President Xi's Made in China 2025 Plan.

The PLA was responsible for the hacks and theft of hundreds of millions of Americans' data from the Office of Personnel Management, Marriott, Anthem Health, and Equifax. Although the PLA undoubtedly used this information for intelligence purposes, it's also highly likely that this high-quality data has been used to help the government-sponsored development of Chinese AI capabilities.

The Committee's well versed in this issue, but I'd be happy to discuss more about my experience based in the Pentagon negotiating with the Chinese on issues of intellectual property theft.

So that leads us to what should we do. Clearly, many of China's actions are unfair in a modern global economy, but the United States and Congress in particular also need to internalize an important point. This is not about China. This is about America. This is not a partisan issue. We control our own destiny and we can outcompete any nation in the world if we unite and focus on a few key areas of policy and law.

Here are some that I recommend. First, we need to promote the competitiveness of American firms and the most important place to start is by passing a national data security and privacy law.

As you heard, information is and will be the Nation's most important strategic resource in the next century, yet American companies are left to deal with competing and often contradictory requirements. In particular this impacts early young innovative firms trying to figure out how to navigate the Information Age.

We should ensure regulation supports the competitiveness of American firms and critical sectors and Broadband 5G in particular. The U.S. Government and the FTC in particular should be sure that regulations designed to protect consumers and competition don't inadvertently undermine the competitiveness of American firms and promote the success of national champions, like Huawei.

The U.S. needs to win the race for talent. The U.S. has excelled by prizing and nurturing openness, creativity, and innovation. Simply put, we will not out-compete the Chinese unless we ensure that more highly skilled workers are able to obtain H1B visas.

We need to continue to limit foreign ownership of key information sectors and provide CFIASs with additional human resources. Congress should be encouraging action of reforming CFIAS now and needs to ensure that CFIAS has the human resources to make this law implementable.

Finally, I believe very strongly the U.S. needs to deter actions to steal our national resources by defending America's interests in cyberspace. This starts with publicly attributing attacks that raise the cost to adversaries. This has proven effective in the past. We should continue to do this regularly.

Furthermore, we need to develop precise and legal offensive cyber operations that change the current dynamic of America simply sitting back and absorbing the blows of China's actions. Good defenses are important but defense alone will not mitigate the threat of these attacks.

At this time, I would like to submit the rest of my statement for the record and look forward to your questions.

Senator SULLIVAN. Without objection.

[The prepared statement of Mr. Rosenbach follows:]

PREPARED STATEMENT OF HON. ERIC ROSENBACH, CO-DIRECTOR, BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS, HARVARD KENNEDY SCHOOL, FORMER DOD CHIEF OF STAFF; FORMER ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY

Chairman Sullivan, Ranking Member Markey, other distinguished members of the Subcommittee on security, thank you for calling this important hearing on "China's Challenges to U.S. Commerce" and for the invitation to testify today.

This hearing is important: China is moving very quickly into the Information Age with a strategic approach that bolsters their national interests. The United States, on the other hand, seems to be standing by, beholden to large technology companies focused primarily on connecting more people to generate more data to further bolster their profits. In the absence of a national strategy to protect Americans' data, promote the competitiveness of American firms, and secure our information and technology infrastructure assets, the U.S. risks ceding its leadership role in the future economic, military, and political landscapes.

The Information Age

This is the Information Age. And information is now the world's most consequential and contested geopolitical resource. The world's most profitable businesses have understood for years that data is the "new oil." Political operatives—and, unfortunately, foreign intelligence operatives as well—have shown over the past two presidential elections that data-driven social media is the key to influencing public opinion. Leading researchers in the area of artificial intelligence know that good data, not just algorithms, will allow companies, and nations, to gain a competitive edge.

Data-driven innovation is not only disrupting economies and societies; it is reshaping relations between nations, and there is no better example than the US-China relationship. The pursuit of information power—involving states' ability to acquire, refine, protect, and use information to advance their interests—is changing strategic priorities. In the current US-China trade negotiations, for example, IP theft and state-support for tech companies is on the table next to soybean and automobile tariffs. American policymakers are questioning a long-standing tenet of the U.S. economic system: openness to foreign investment. In short, the pursuit of information power is altering strategic and economic relations between nations.

In the 1990s, America's supremacy in information technologies and the Internet seemed unassailable. Unfortunately, as the importance of information as a geopolitical resource has waxed, U.S. dominance has waned. States with authoritarian forms of government—and China in particular—first recognized the strategic importance of information, and have adapted their national laws and policies accordingly. America's economic competitors believe they are locked in a zero-sum competition to create, collect, buy or steal data, and to develop the talent and technology to convert it into strategic advantage.

Data held by both corporate and government entities has more strategic value than ever before because of its importance in developing artificial intelligence. A technical wunderkind is no longer as critical to writing a good AI learning algorithm; instead, what developers most require are troves of high-quality data to train and optimize algorithms over time. As a result, states have a strong interest in developing, accessing or stealing commercial, private and government data necessary to train and optimize AI algorithms.

Indian Prime Minister Narendra Modi, for example, believes that "whoever acquires and controls" data will attain "hegemony." In his recent book *AI Superpowers,* venture capitalist Kai-Fu Lee predicts that China's widening lead in artificial intelligence will not only ensure the "economic balance of power tilts in China's favor," but will tilt "political influence and 'soft power,' towards China," and cement its "cultural and ideological footprint around the globe." Most developed economies now have national "artificial intelligence"strategies. None are more mercantilist than China's "Development Plan for a New Generation of Artificial Intelligence," which aims through a combination of government subsidies and incentives to push China into leading the world in AI by 2030.

The Competitive Threat from China

Over the past decade, China has pursued a national strategy to challenge the United States' global leadership in the Information Age through a conscious strategy of state-backed investment, loose consumer data privacy protections, a centralized AI and technology deployment strategy, and intelligence operations to steal crucial data and intellectual property.

The Chinese government has invested heavily in the research and development of technology that underpins supercomputing, artificial intelligence, broadband networks and big data. Those investments have resulted in genuine achievements. In 2016, for example, China unveiled the world's fastest supercomputer—and announced that it owned more of the top 500 supercomputers than any other nation in the world. Chinese firms and research institutions, nearly always supported with state funds, have made advances in artificial intelligence that some corporate leaders believe will make China the world leader in hardware-based AI.

President Xi has also advanced his nation's strategic plans by developing and supporting firms in key areas of economic power with state-sponsored loans, contracts and research and development. One of the best known of these Chinese "national champions" is Huawei, now the largest telecommunications equipment maker in the world. The significant resources Huawei derives from the backing of the Chinese government puts American and European telecommunications equipment providers at a clear disadvantage, particularly when it comes to developing and deploying some of the technology necessary for next generation broadband networks.

The Chinese government has also devoted significant military intelligence capabilities to steal the data and intellectual property needed to fulfill the ambitious goals established for President Xi's "Made in China 2025 Plan." Over the past decade, Chinese intelligence officers from the People's Liberation Army (PLA) have conducted thousands of cyberattacks against both private sector and government targets. The Chinese, for example, were almost certainly responsible for the hacks and the theft of hundreds of millions of Americans' data from the Office of Personnel Management, Marriot, Anthem Health and Equifax. Although the PLA undoubtedly used this for intelligence purposes, it's highly likely that this high-quality data was also used to help the government-sponsored development of AI capabilities.

Over the past decade, Chinese intelligence operatives have been equally aggressive in systematically stealing intellectual property and trade secrets from American organizations essential to national competitiveness. "More than 90 percent of the department's cases alleging economic espionage over the past seven years involve China," deputy attorney general Rod Rosenstein said after an indictment unsealed in December 2018.

The Obama Administration's response to these attacks was slow and initially weak, but by 2015 the Administration finally recognized the need to confront Chinese leadership with explicit attribution, sanctions and improved cyber defenses. These actions resulted in a short-term drop in Chinese cyberattacks against the US. Over the past 18 months, however, Chinese cyber operations have resumed. In the most recent annual national threat assessment, for example, Director of National Intelligence Daniel Coats said that, "China will continue to use cyber-espionage and bolster cyberattack capabilities to support [its] national security priorities." This past December, the FBI's top counterintelligence official asserted that, "Our prosperity and place in the world are at risk."

What Congress Must Do

As the Information Age advances, the United States needs to recognize that data collection and technology deployment are critical both from the perspective of economic competitiveness and national security. Looking over the horizon, adversaries will greatly increase operations to steal sensitive and valuable information in order to advance their strategic and economic advantage over the United States. Given the richness of data held by the largest companies and research centers in the tech, financial and healthcare sectors, it is highly likely that adversary intelligence services will expand their traditional targets to include corporate datasets that could be used to train AI systems and to hone information operations.

U.S. policy responses to these threats should be centered around a few guiding principles:

1. *The Information Age demands a data-centric security and economic strategy:* America needs to develop a data-focused strategy for competitiveness. From a security perspective, a network-centric approach to national security is failing. Focus on the threat of a low probability catastrophic attack on critical infrastructure networks, for example, has distracted leaders from the reality that we are not defending the Nation's most precious resource: information. Likewise, the government has done very little to prioritize the centers of gravity for an economy powered for the Information Age.
2. *The privacy of personal information is a national security and economic priority.* Policies aimed at bolstering U.S. national security and promoting U.S. economic competitiveness must go hand-in-hand with consumer protection. Authoritarian governments may ignore consumer rights in pursuit of acquiring information power, but democracies cannot. Bolstering the global competitiveness of American companies should remain a top priority, but not at the expense of allowing these companies to collect, use, and sell information without user consent or under-invest in cybersecurity measures.
3. *America needs a whole-of-government strategy to improve national competitiveness in the Information Age.* Information geopolitics cuts across all aspects of the economy, society and state security apparatus. Authoritarian governments have adopted a highly centralized, mercantilist approach to protecting, acquiring and using information. Centralization will not be the answer for democracies, but coordination must be. Unprecedented cooperation is required, across economic, social, defense, intelligence, state department and homeland security portfolios. For example, the American government can no silo regulatory decisions about information-related companies separate from foreign policy decisions on cyberspace.
4. *Even further, America needs a whole-of-nation strategy that includes coordination with the private sector.* The U.S. intelligence community needs to share threat information about foreign intelligence organizations with the social media platforms that so directly influence Americans' economic and political decision. Policymakers must be willing to work with private actors to ensure regulatory red tape does not stand in the way of innovation, and that public-private partnerships continue to create incentives to accelerate technology development. At the same time, American technology firms need to understand, and be held accountable for, their role in protecting national security interests.

These principles should be combined with forward-leaning policy action. Specifically:

- *Pass national data security and privacy legislation.* Information is and will be the Nation's most import strategic resource for the next century. Yet, even in the face of inadequate data protection practices and damaging data breaches, the U.S. continues to muddle along with a complex web of state-based and industry-specific requirements. American consumers are worse off because their data is unprotected and, in the event of a personally costly data breach, their rights and access to legal recourse are unclear. American companies are left to deal with competing and possibly contradictory requirements, in particular impacting early innovators and small businesses without the resources to navigate this complex environment.

  U.S. policymakers urgently need to pass a national law that will protect user data, reduce regulatory complexity, and spur innovation by reconciling differences in state and Federal requirements. While Europe's General Data Protection Regulation (GDPR) is by no means a perfect model and in some respects is inconsistent with other U.S. values, it has been effective at driving corporate investment in data protection. Data protection legislation passed in California

in June 2018 will need fine-tuning before taking effect in 2020, but it establishes important principles that could serve as the foundation for national legislation.

- *Promote competitiveness of American firms:* China undeniably has an advantage in data collection, by virtue of its large population and weak data privacy protection policies. While data is an important input, it is not the only determinant of competitiveness in the information age. China's authoritarian system also gives it a deployment advantage, but the U.S. can do a lot more to reduce regulatory red tape, attract top talent, and create other incentives to spur innovation.
  - ***Ensure regulation supports competitiveness of American firms in critical sectors.*** A key driver of the information age has been the exponential growth of high-speed wireless broadband infrastructure around the world. American firms are currently locked in a tight competition with Chinese powerhouses to determine who will dominate this important area. The U.S. government—and the FTC in particular—should make sure that regulations designed to protect consumers and competition don't inadvertently undermine the competitiveness of American firms relative to Chinese national champions like Huawei.
  - ***Reduce regulatory red tape to expedite deployment of next-generation broadband infrastructure.*** Nationwide 5G deployment is a massive effort requiring equipment installation and associated permits and approval processes across thousands of localities. Yet without this foundation, the U.S. risks falling behind in the next generation of wireless-enabled technologies. Policymakers must drive toward regulation that standardizes and fast-tracks local approvals, while giving local authorities the opportunity to provide implementation guidance.
  - ***Continue public-private partnerships that support advanced technology development.*** Within the framework of robust national data privacy and security laws, the U.S. government should promote more partnerships with civilian companies and academic institutions to make progress on high-priority AI initiatives. For example, the Defense Innovation Unit—Experimental (DIUx), established by DoD for this purpose, provides a model for incentivizing the private sector to develop technologies with direct national security applications.
  - ***Win the race for talent.*** The U.S. has a history of prizing and nurturing openness, creativity, and innovation. Our university system is a springboard for raw talent; our legal and government institutions allow new businesses to thrive; and our sophisticated financial system enable the best ideas to be successful. To maintain a competitive edge, the U.S. needs a foundation of policies and practices that continue to attract top talent, like the heads of AI at Apple, Facebook, Microsoft, and Google's cloud computing division, who were all born outside the US. The visa program is a good place to start—at minimum, Congress should ensure that more highly skilled workers are able to obtain H–1B visas. Policymakers should further consider special programs for students and experts in the AI and broader set of STEM fields.
- *Protect American information and infrastructure assets:* Good offense that promotes U.S. economic competitiveness must be coupled with good defense that bolsters the U.S. system against foreign attacks and takeovers.
  - ***Incentivize use of strong encryption.*** Making America the world leader in encryption technology could advance both economic and national security interests. Protecting the Nation's most important resource will require a significant expansion in the use of encryption. The nation's defense and security agencies have relied on encryption to protect its most precious secrets for many decades—DoD, in fact, is the largest user of encryption in the world. The U.S. must both clarify the legal questions around encryption and develop real incentives to promote the use and growth of encryption products and platforms that allow individuals and organizations to protect their data.
  - ***Limit foreign ownership and provide resources to support firms in key information sectors.*** Over the past decade China has systematically targeted investment in and ownership of firms developing technology, such as AI, that will drive strategic advantage in the Information Age. Congress took encouraging action by reforming and passing legislation that increased limitations and oversight of foreign ownership and involvement in data-rich sectors. This was important, but should be supplemented with new sources of incen-

tives to sustain American tech firms whose technology does not have an immediate commercial application.

- *Deter Chinese actions to steal our national resources by defending America's interests in cyberspace:* Our response to Chinese cyber-attacks that steal personal data and intellectual property has been weak, resulting in the perception by China that an attack on the American economy will not incur costs. The U.S. needs a strong national response to demonstrate that interference with American information and infrastructure assets in any manner is unacceptable. We have to raise the cost of attacks and decrease the benefits that our adversaries seek.
  - ***Publicly attribute attacks to raise costs to adversaries.*** The increased willingness of the Intelligence Community, DHS, and FBI publically to attribute Chinese cyber attacks through indictments is crucial and positive first step.
  - ***Develop precise and legal offensive cyber operations that change the current dynamic of America simply sitting back and absorbing the blows of adversarial actions.*** Good defenses are important, but defense will not alone mitigate the threat of foreign attacks. To complement defensive measures, the U.S. government, led by the Department of Defense, needs to bolster its capabilities to disrupt and degrade Chinese cyber operations before they succeed.
  - ***Improve intelligence sharing with the private sector.*** The Intelligence Community should also strive to share as much intelligence information as possible about Chinese cyber operations. In the past, the government has too often watched important intellectual property or data flow out of the country without warning impacted organizations.

Senator SULLIVAN. Well, thank you. Outstanding opening statements by each of our witnesses, and we have the Chairman of the Full Committee here and I'm just wondering if he wants to make an opening statement before we start making questions.

STATEMENT OF HON. ROGER WICKER, U.S. SENATOR FROM MISSISSIPPI

Senator WICKER. Thank you very much, Mr. Chairman, and I will not take anywhere near five minutes to make an opening statement, but I do want to say that this is the very type of hearing that I envisioned when we came up with the Subcommittee on Security.

I want to commend Chairman Sullivan and my long-time friend and colleague from the House and Senate, Senator Markey, for their leadership in this regard.

The economic relationship that the United States has had with China has been remarkable in the past few decades, but it's been a learning experience as American consumers have benefited from this and certainly as the Chinese people have benefited from it.

It has become obvious that the leadership in China has no intention of playing by international rules, that they have no concept of respecting such international principles as intellectual property rights or data privacy and so while the relationship that we have and that we're going to necessarily have with China over time presents us with great opportunities, it does present us, as the title of this subcommittee hearing indicates, with immense challenges.

So I think this is a very thing that we need to be looking at in a very good way early on in this Congress for this subcommittee to spend its time and I congratulate both of my friends for their leadership in this regard and wish you well.

Senator SULLIVAN. Well, thank you, Mr. Chairman, and I'll begin the questioning here by, you know, one of the big things we're trying to do in the Congress is really hot to work with the Administration to craft a bipartisan strategy on how to deal with these issues which are very complex.

One of the issues, and I highlighted it in my opening statement, is this issue of reciprocity. I think reciprocity is important because people certainly in our country understand it and I think in most countries they understand it. It just goes to basic fairness.

I've asked a number of keen observers of China, including Dr. Henry Kissinger, in an Armed Services hearing a couple years ago about should this be a defining feature between the United States and China. He essentially answered yes in so many words.

So I want to talk about this issue, particularly as it relates to the economic relationship. You know, I had my first trip to China as a U.S. Senator and I raised this question of reciprocity last spring on numerous fronts. Here's just an example. We all know that Chinese companies, usually backed by government subsidies or government investment funds, come to the United States and they buy, for example, you name it, movie studios, biotech companies, robotics companies, Internet companies, OK, and then the answer—and I'm not going to even ask you because we all know what the answer is.

If a U.S. company wants to go to China and buy the same kind of companies, a movie studio, a biotech company, a high-tech company, an Internet company, the answer is no. So there's no reciprocity, particularly on the investment side of the ledger.

So my question and maybe I'll start with you, Mr. Kallmer, would you be supportive of a very simple bill, maybe called the U.S.-China Reciprocity Act of 2019, that essentially says if a U.S. firm can't go over in a sector of China and buy a company, then they can't do it here? What would be wrong with that?

The American people would understand it and this is a really important point. We meet with many foreign leaders. I am very convinced that if we did something like this, the EU would, the Japanese would, the Koreans would, and all of a sudden you could have two-thirds of the global GDP of the world saying the same thing. If you don't play by the rules that we all play by, you can't invest. Pure reciprocity. It's fair. People understand it.

Would you support something like that? What would be the pros and cons of that approach?

Mr. KALLMER. Thanks for the question, Mr. Chairman. I think we would——

Senator SULLIVAN. And then comment on our allies doing it, as well, which I think they would be willing to do with U.S. leadership leading the way on this.

Mr. KALLMER. And I would actually—I wanted to comment on that in a little bit of a broader context.

I think we would certainly want to see the text of such a bill, but I think in general terms we'd be very supportive of the concept.

Senator SULLIVAN. This would be broader than the CFIAS reform we just did.

Mr. KALLMER. Absolutely, absolutely. I mean, this is a systemic issue in doing business with the Chinese. The example I used in

my opening remarks about the cloud services companies is a perfect example.

We have the best cloud services companies in the world. When they go to China, they are prevented from owning Chinese companies. They're, you know, forced to enter joint ventures. They're prevented from using their intellectual property. They're prevented from representing themselves in——

Senator SULLIVAN. But the Chinese don't have similar restrictions here.

Mr. KALLMER. Not at all, not at all.

Senator SULLIVAN. Not at all. So it's unfair. It's basically unfair.

Mr. KALLMER. It is completely unfair.

Senator SULLIVAN. Not a level playing field.

Mr. KALLMER. It is not. It is not, and you can replicate that fact pattern across different sectors of the economy and so I think we would look forward to the opportunity to work on something like that with you.

Your point about the support of allies is critical not just——

Senator SULLIVAN. Critical.

Mr. KALLMER.—in the context of something like this but in everything we do to try to influence China. The United State is still the biggest economy in the world, but we can't do it alone. This is fundamentally a global problem. Chinese practices harm German companies, Japanese companies. They impede innovation in those countries.

Senator SULLIVAN. Let me just interrupt you here.

Mr. KALLMER. Yes.

Senator SULLIVAN. Sorry. I want to ask one follow-up.

Ambassador Lighthizer's doing this a lot with the EU and Japan. They even have a group, the U.S.-Japan-EU group that's pretty much focused on these issues working together as it relates to the China challenge.

Mr. Rosen, what do you think of that idea of pure, just a pure straight-up reciprocity bill that says if you can't do it here—if we can't do it there, you can't do it here? Pretty simple, pretty easy to go home and explain to our constituents about it, and very, very fair. Why would we not want to do something like that?

Mr. ROSEN. Thank you very much, Mr. Chairman. I think first thing that can be helpful to the deliberation is that Rhodium's put together a fairly perfect database on two-way flows and it is actually still the case that the value of U.S., FDI, and China is much greater than the value of Chinese direct investment in the United States, although at the margin in recent years, the trend has been that there's been more annual Chinese flow into our economy than is possible in the other direction.

Second, some non-trivial amount of this Chinese investment coming into, say, Silicon Valley is actually Chinese companies that were started by U.S. private equity and venture capital companies. So there is some American chromosomes, if you will, in some of the money that's flowing in this direction.

That is the kind of granular stuff that's important to unpack and have staff kind of work through as you design and put together what might be a very important and useful framework and regime on reciprocity.

Moving to the question of fairness, though, for just a second, you know, it has since the 1790s, in fact, been the position of the U.S. that if other people want to bring their treasure here, that's a good thing for us, regardless of whether they accept our treasure flowing in their direction. That is to say, you know, Cuban capital flight out of that economy because of the realities there, we should accept regardless of whether they have the ability to absorb our capital outflows.

Senator SULLIVAN. Not if they're stealing the investment and then using it to buildup their own industrial base.

Mr. ROSEN. Right. So we need to take the analysis to the next level. What is the nature of the lack of reciprocity, the nature of the asymmetry and investment opportunity, and is there in fact a specific risk in a given area of technology that confers a benefit, especially in an emerging foundational technology area?

So there are many cases where I am acutely concerned about the lack of reciprocity. There are many other sectors, like real estate, where I don't really care very much and I say let the money leave China and come up on our shores.

Senator SULLIVAN. OK. Senator Markey.

Senator MARKEY. Thank you, Mr. Chairman.

This is the proper committee because this is the Committee in the 1990s that created this whole digital revolution with the laws that were passed out of this Committee. So we are the right committee. We are the Committee of expertise to now be examining the consequences. So I thank you again for bringing this focus to it.

Mr. Rosenbach, Tick Tock is a Chinese-owned app which allows users to share and view short video clips with music and it's no secret that kids and teens flock to this platform every day.

Last month, the Federal Trade Commission levied a record fine against Tick Tock for violating the Children's Online Privacy Protection Act and its Chinese company that's doing it. It's illegal, whether it's Chinese or American, but it's an indication of how the Chinese can get inside of our system.

What steps should the United States take to protect Americans from invasion of privacy that Chinese companies, like Tick Tock, are engaging in every single day?

Mr. ROSENBACH. Thank you, Senator. To start with, you know, theft of intellectual property is one thing that is horrible but doing something that would harm kids, you know, is kind of over the top, as the father of a pre-teen who would be involved in that, and so I think you need to uphold the rules and if this firm is not going to follow U.S. law and the privacy protections that are there in place to protect children, they should not be allowed to operate in the U.S. and we should find ways for them to be blocked so that kids can't access that and the app is not legal here.

Senator MARKEY. Thank you, sir. I'd like to give you—yes, Ms. Sacks.

Ms. SACKS. Under the expanded CFIAS system, access to U.S. citizens-sensitive personal data is now a consideration and I welcome that for specifically this issue.

Senator MARKEY. Thank you.

Ms. SACKS. However, I think that it needs to be narrowly tailored. Right now, it's very broad and so from the Chinese perspec-

tive, they see this as justification for their own efforts to localize data.

So as we think about access to U.S. citizen data under CFIUS, let's see if we can set a model for the Chinese in more narrowly scoping what that means.

Senator MARKEY. OK. But still we have to deal with it. It's going to happen and intensify as the years go by.

I want to follow up on the Chairman's question, just go to the Huawei issue, and our need to deal with their desire to bring their technologies and to build them into the communications networks of our country and yet just going to the reciprocity question, clearly that would never be allowable in their country in terms of allowing our companies to do the same thing.

So if you could, just expand upon that duality and what you would recommend that we establish as policies, following up on what the Chairman said, to ensure that we have some parity of treatment between the two countries, sir.

Mr. ROSENBACH. Yes, sir. I've been working in national security and telecom intelligence for almost 20 years, have followed the Huawei trajectory for the last 10. There's no way I would allow Huawei gear in the U.S. 5G backbone. It's a threat to national security and clearly they don't even play fair.

More importantly, the Chinese used Snowden as an excuse to exclude a lot of American firms from the market to raise some of these data protection boundaries that are not based on real fact or technology and are very protectionist and if they're going to do that, then I think the reciprocity principle is something that is very important to recognize.

We want our firms to be able to compete on a level playing field and U.S. tech firms will win if they can do that.

Senator MARKEY. Anyone else want to comment upon that and the Chairman's, you know, insight in terms of the lack of reciprocity? The Chinese would never allow us to have an American company go inside their networks and build these kinds of technologies into information-gathering operations. Yes, Mr. Kallmer.

Mr. KALLMER. Thanks, Ranking Member Markey. I would just add that I think there are multiple ways to view this kind of an issue.

Reciprocity and whether and how to do it is an incredibly important one, but it sort of speaks more to the economic commercial trade issues. There could be wholly separate national security considerations, such as the ones that Mr. Rosenbach identified for which the U.S. Government also needs to have tools and that is a theme that we talk about a lot. We'll probably talk about it more today, which is that from a security perspective, it's important also for the U.S. Government to clearly identify the authorities that it has or that it needs or that it has but needs to build up, to address all of these risks.

Senator MARKEY. Yes. And a lot of this hearing is really just to deal with the sinister side of cyberspace. We talk about all the benefits but there is a definite sinister side and you, Mr. Rosenbach, were talking about all of the attempts by the PLA, People's Liberation Army, to penetrate key American interests.

So could you expand upon that and whether or not you think this is a pathology? What's the smartest way to deal with that underlying pathology so that we're paradoxing them correctly?

Mr. ROSENBACH. Yes, sir. So this is something that was directed from the senior most levels of the Chinese leadership to use national intelligence agencies to steal intellectual property and pass them to state-owned industries. That's something that not only doesn't happen in the U.S., is illegal. The idea that NSA would pass secrets to Intel or Google or Microsoft, you know, is absurd. That's not fair.

Not only that, they're using that data, from my assessment, to build a new platform for AI. Data matters a lot and that's the reason you would steal these large troves of data that's clean and organized and help you further develop the algorithms of machine learning.

So it's not only a cost in the way people expect an IP, down the road I believe it's even more important and will have a bigger impact——

Senator MARKEY. And when Huawei says, oh, and we're not connected to the government at all, we're just a private sector, do you have a brief comment on that?

Mr. ROSENBACH. I don't believe it, and in some ways there will always be a nexus between telecom companies and the U.S. and the government but it's not the same. There's not the same type of relationship and if you look at the trajectory of some countries that made the mistake of putting Huawei gear in their backbone, like the U.K. and Australia, they're now in the very difficult situation of ripping it out.

I don't think the U.S. wants that. We're already a little behind on 5G. Doing something like that would put us even further behind.

Senator MARKEY. Thank you. Thank you, Mr. Chairman.

Senator SULLIVAN. Senator Fischer.

STATEMENT OF HON. DEB FISCHER,
U.S. SENATOR FROM NEBRASKA

Senator FISCHER. Thank you, Mr. Chairman.

Mr. Rosenbach, you've mentioned a couple times now about the hacking and the theft that we have seen of Americans' information. You talked about the collection of that data and it's going to feed the Chinese AI system.

I would like to ask you specific examples that you can give us about the risk that this poses to consumers and to businesses from an economic espionage perspective, please.

Mr. ROSENBACH. Some of the examples of IP theft, which might be different than just the large data theft, would be the theft of aerospace secrets, both in the commercial and the private sector. There are some pretty well-documented cases of in the chemical sector.

One that you can say is a known fact relates to Huawei itself which in a court case admitted and paid a fine for stealing the source code from Cisco that they then used to build the core routers that have made them successful down the road. That's the type of behavior that is directly harmful to U.S. firms.

The other thing is there's a cost here to the economy for these large data thefts, which means every consumer that has to deal with getting new credit cards. It seems like a small thing but anyone who was involved in Equifax knows you spent time, it's a drag on the economy, and we need to protect our data better because of that.

Senator FISCHER. You've also highlighted the need to limit foreign ownership to protect American information and infrastructure assets that we have.

I know you're aware of the efforts of the Chinese to penetrate the U.S. railcar industry. The CRRC has recently signed contracts to provide inexpensive Chinese Government-subsidized railcars to meet the several Metro Centers across the U.S. and that's a concern. That's a worry that they could install some kind of technology there that's going to provide them with surveillance of our rail and our transit interests.

Do you share those concerns, and do you believe Congress should implement some kind of additional oversight so that we do have safeguards to protect our critical infrastructure in those circumstances?

Mr. ROSENBACH. Yes, ma'am, I do. First, it just seems odd that a firm that's getting help from the Chinese Government would be able to do that and we wouldn't produce them in the U.S. if we could.

Second, your point on critical infrastructure is really important. What if there is a special sauce baked into the software that controls the networks that run these transportation modes in any transportation sector, and at a time of their choosing, the Chinese use that to hold the U.S. hostage or, in the worse case, unlikely but very critical, to conduct a cyber attack? Those are two bad things for certain.

Senator FISCHER. Thank you.

Ms. Sacks, in your testimony, you cited and you also warned against the U.S. interests viewing China's tech ambitions as a struggle between two compelling blocks.

Given the Chinese Government's trend toward country-unique policies that hinder market access, how can the United States and its allies approach imbalances that are created by China's core interests in favoring those domestic companies and can we realistically try to shape China's approach in many respects?

Ms. SACKS. Thank you. I think the key in addressing these issues is to understand the cost-benefit that comes with looking at this as a competition in which this is a zero sum game, right.

So when we talk about AI and 5G and all sorts of technologies, they don't necessarily conform neatly to national borders. Code flows between borders when we talk about the research being done with diffuse networks of sciences across countries, the open source information that is sort of the backbone of AI cutting edge research right now.

So right now under consideration is new export controls around emerging and foundational technologies and I welcome industry and others to weigh in on how do we more narrowly tailor the scope of this to take into consideration ways that we can erect bar-

riers without undermining our own competitiveness and innovation in the process.

In some ways, distinguish——

Senator FISCHER. Do you think that's realistic? Can we——

Ms. SACKS. When it comes to AI,——

Senator FISCHER.—have those barriers and not have that bilateral competitiveness?

Ms. SACKS. I think with AI, it's going to be very difficult. In some ways, it may be impossible to distinguish between the military and civilian use for some of these applications, and I agree with the assessment of ITI and my colleague, Mr. Kallmer, in that when we think about where these technologies are being used, what is essential from a military advantage? It's not just about being used or could be used by the military and there needs to be a process to understand that.

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

Senator SULLIVAN. Senator Blackburn.

STATEMENT OF HON. MARSHA BLACKBURN, U.S. SENATOR FROM TENNESSEE

Senator BLACKBURN. Thank you, Mr. Chairman. I am so pleased that Chairman Wicker established this subcommittee. I think it's so needed as we work on these issues and Mr. Markey and I've worked on these issues for a long time, as Senator Blunt was also with us over at Energy and Commerce in the House.

I think as we talk about AI, as we talk about 5G, not only are we concerned with China and how you never know where their commercial sector and their industrial complex end and begin. They really are pretty much one and the same.

And in addition to the things that you all have discussed this morning, I think we also have to look at, and, Ms. Sacks, this goes to your point to Ms. Fischer, looking at who is going to set the standards when it comes to AI, when it comes to 5G, and knowing that we're going to have to deal with the China scale and weight and intensity on this issue and Huawei specifically as we look at a lot of this and how they embed the malware and the spyware into their technology.

We don't want our allies to use it. We do not want American companies to be using this technology because of their tendency to do that. So in that context of looking at communications and the information equipment, to what extent can Chinese firms put a downward pressure on us and on our allies as we talk about what we're doing in that Armed Services sphere?

I served on Armed Services Committee and, Mr. Kallmer, I see you shaking your head, nodding your head. I'd like for you to answer and, Mr. Rosenbach, I'd like to come to you.

Mr. KALLMER. Sure. Thanks, Senator Blackburn, and the reason I'm nodding my head is because it's a terrific question that I think illustrates the importance of being really deliberate and analytical about identifying risk.

One of the points that we made throughout the FIRRMA process last year is that, in addition to nothing being more important than U.S. national security, it's critical that we observe with humility

working with our government partners who have best access to information and breakdown the various risks.

Is the risk one of a foreign company with bad intentions buying something in the United States? Is there a risk of technology outflow from the United States to some other country? Is the risk the one you identified, which is another country, such as China, having a disproportionate role in writing the rules and setting the standards?

And in that regard, it is critical that we get our arms around this whole risk set and have tools to address each of them.

Senator BLACKBURN. Well, and I would add to that, as we look at the risk set, I think the intentionality——

Mr. KALLMER. Right.

Senator BLACKBURN.—needs to be a consideration.

Mr. KALLMER. Exactly. And so the example of standards is a perfect one. It goes maybe not so much anymore, but traditionally a little bit below the radar because it's quite technical, but in a way, there's nothing more pernicious than China's approach to seeking to dominate the writing of standards, pushing that approach in——

Senator BLACKBURN. Well, they set the rules of the road if they set the standards.

Mr. Rosenbach.

Mr. ROSENBACH. I think it is important to talk about risk and the one thing to keep in mind is you need to think about risk on a decade-long at least perspective and so sometimes firms, American, European, otherwise, will make risk decisions based on a year or two or three out and that?s when they're more likely to invest in Huawei gear because they have a better deal because it's subsidized by Chinese Government and they don't think, first of all, at the national level what that can mean for a national security perspective or that 10 years down the line, they're going to be locked into something that they can't get out of and that's where it's more of the government's role to think about risk at the strategic perspective for the country and over the run of the Information Age.

Senator BLACKBURN. OK. My time is expiring. Ms. Sacks, I have a question for you. I'll submit it for the record, but I liked your analogy that you used of a small yard/high fence. I've got a question on that for you.

Mr. Rosenbach, I'm going to come back to you with something as Commerce being a market-facing agency, a couple of questions there as that relates to the integration for some of our stakeholders as we look at our military side and our commercial side.

Yield back.

Senator SULLIVAN. Senator Klobuchar.

STATEMENT OF HON. AMY KLOBUCHAR,
U.S. SENATOR FROM MINNESOTA

Senator KLOBUCHAR. Thank you very much. I don't have much of a voice. So that means I won't filibuster. Very good for you.

Mr. Kallmer, I recently led 18 Senators in a letter urging the National Security Advisor to reconsider the decision to eliminate the role of Cybersecurity Coordinator at the NSC and I'm concerned that, given the Chinese Government's commitment to cyber pro-

grams and investment in cyber capabilities, we aren't keeping pace. Could you respond to that?

Mr. KALLMER. Yes, thank you, Senator Klobuchar, and I hope you recover your voice soon.

Senator KLOBUCHAR. So do I.

Mr. KALLMER. That is a theme that has been very important to us. Our companies across the board care deeply about cybersecurity and historically have found that there's nothing more important than the U.S. Government not only having a lot of smart people thinking about it, but in having a truly coordinated approach and so whether it is having a senior role at the White House, whether it is having a senior person at the State Department, and the extent to which they are all coordinating a whole of government approach, it's critical.

In fact, the RSA conference is occurring right now in San Francisco, which I think is the world's largest cybersecurity conference. Finding ways for industry to support the U.S. Government in having that top-notch whole of government approach is a top priority.

Senator KLOBUCHAR. Right. Senator Thune and I actually have a bill that I'm leading to try to get more expertise into the government from the private sector with tours of duty. Have you thought through that?

Mr. KALLMER. We have. In fact, part of our organization focuses not just on public procurement of ICT products but also IT modernization within the government and this is a theme that we have been pushing for some time, which is to find some way to second or create opportunities for really talented cutting-edge people in the private sector to do tours of duty in the government.

Senator KLOBUCHAR. Good. Then there's kind of that non-traditional espionage with 500 million guests for Marriott and some of the other hacks that we've seen.

Maybe someone else wants to answer this. What kind of outreach, Mr. Rosenbach, do you think should be going on with the private sector?

Mr. ROSENBACH. The idea of bringing outside private sector expertise into the government is really important. During the time I was in the Pentagon as chief of staff, we started something called the Defense Digital Service in which we found ways to bring hardcore techies in for a tour of 3 years, small team, did some really phenomenal things that really improved the overall level of cybersecurity at DoD.

Anything that you could do to make that more widespread across government I think would be very helpful.

Senator KLOBUCHAR. OK. Another area, election infrastructure. A report by the Hoover Institute and the Asia Society concluded that China did not directly interfere in our 2018 elections, although we know Russia was working on it pretty hard in terms of hacking in and then, of course, Russia did a lot of other things that were very bad.

Can any of you explain the cyber capabilities of China to interfere in our elections?

Mr. ROSENBACH. Yes, ma'am. I 'm running a project at the Kennedy School called Defending Digital Democracy that's working with state and local election officials to help them protect their in-

frastructure. We had an after-action review from the 2018 elections, had 25 states come and talk about what they saw.

We shouldn't be relieved that we didn't see anything in 2018 and very clearly if the Chinese wanted to influence the U.S. in a strategic way, they have the capability to do it, either through directly attacking the election and undermining trust or through disinformation campaigns that would be done via social media.

So it's something we need to keep working on and, quite frankly, the Government needs to play a stronger role. DHS has gotten much better, but it's not fair to let the states take blows from nation state intelligence services when it's about our elections.

Senator KLOBUCHAR. Very good. Last, you stressed the importance of privacy legislation and, of course, it's something we're working on here. Senator Kennedy and I have a bill.

Could you talk about how security and economic threats Americans face could get worse if we do nothing when it comes to privacy?

Mr. ROSENBACH. Yes, ma'am. Just real quickly, when information is the most precious commodity in the Information Age, it seems crazy that the U.S. would not have a national bill to regulate this.

Now if we don't do it, California will be the standard or GDPR from Europe will be the standard. So it seems almost——

Senator KLOBUCHAR. That was meant to scare you, Senator Sullivan.

Ms. SACKS. Or China. China actually is further ahead in their legislative process in having a national privacy law. So that may be a bit under the radar.

Senator KLOBUCHAR. OK. That's good to know.

Senator MARKEY. We don't want China to get ahead of us.

Senator KLOBUCHAR. That was a bit of a sarcastic joke by the Ranking Member.

Anyone else want to comment on this?

[No response.]

Senator KLOBUCHAR. All right. Thank you very much.

Senator SULLIVAN. Senator Blunt.

STATEMENT OF HON. ROY BLUNT, U.S. SENATOR FROM MISSOURI

Senator BLUNT. I thought you were getting to me. I was just guessing it was going to my turn.

But I want to join my colleagues who got here earlier, asked questions earlier, with their praise of both of you and the Chairman in creating this committee. I think it's a really important issue that we've been trying to deal with in a number of diverse ways but never quite this focused before.

So I chair the appropriating committee on NIH, Labor, and Health and Human Services, Education, but particularly at NIH, in the last year, and I know you've been paying attention to this, the idea of researchers that are either being wooed by the Thousand Talents Program or are students who are here, particularly from China, and, you know, we've had a problem for a long time of feeling like that the things that we had developed were almost being forced to be given away but now we see maybe dual research,

maybe there's enough information going back and forth to another country that they've set up their own research lab based on our money and our efforts to move research in that direction.

So I guess for whoever wants to take it and maybe more than one of you, what do you think the impact of programs like this are going to be on U.S. research, things like the Thousand Talents Program, and also how do we address that without unduly damaging scientists who are actually there to do scientific research and to do it under all the guidelines that we would hope they would have?

Ms. Sacks, your hand is up, so we'll let you start.

Ms. SACKS. Thank you, Senator. This is the right question to ask because universities are in many ways the bedrock of U.S. power in the world, attracting the best and the brightest. So we have to get this right.

I think there are three distinct issues that often get blurred and I'd like to untangle them. The first one is the Chinese Community Party has a concerted effort to control and monitor its students here. There's a great example from a case of the University of Maryland from a few years ago.

This is distinct from the issue of access to U.S. technology and research and here I think the tools of the national security community and law enforcement are designed to handle that. They are designed to handle when there are real threats and they should continue to be used in that way.

I am deeply concerned that Chinese researchers, scientists, and students are being discriminated against on U.S. campuses. This is highly problematic not just from a moral perspective. It gets at the heart of the openness and the values that define our country.

We need to compete for the best talent in the world and if those students don't feel welcome on our campuses, they will go elsewhere. So we have to get this balance right.

Mr. ROSEN. Senator, we were just part of a production of a study on the relationship between Chinese and American biotechnology industries over the past 20 years that we did for the China Security Commission here on the Hill which you'll be familiar with.

That study does, I think, an excellent job of bringing all available evidence to bear on what the interaction between our two economies has been in that industry. Bottom line is that China's biotech industry today wouldn't exist if it weren't for China's ability to participate in, benefit from the open dynamic of American biotech industry, nor today is our sustainable without the inclusion of tens and tens of thousands of Chinese graduate level researchers which are a big part of the human resources that make us dynamic in that industry, as well.

So this is a tricky one because if we really try to sort of disentangle from things that are benefiting China's capability in this space, we're going to pull a lot of the timber out holding up the roof of our sector here, as well, and so this one really needs care.

There's some good research available in that space to try to make sense of it. I will say that transparency and understanding who are the investors looking to make acquisitions in the United States is an absolute key to getting this right.

Senator BLUNT. Mr. Kallmer, did you have something on this?

Mr. KALLMER. Yes, Senator Blunt, I think I would say at a high level that I associate myself with Ms. Sacks and Mr. Rosen.

Senator BLUNT. Let's go to Mr. Rosenbach then.

Mr. ROSENBACH. So I have to say this doesn't represent Harvard University, just Eric Rosenbach.

I think one thing that's counterintuitive and you hear a lot in Silicon Valley and in Cambridge, which are tech hubs, is that if you could, quote, staple a green card to the diploma of every computer science graduate who's a Chinese or not, they would stay here and they wouldn't go back to China and they would fuel the American economy and that will seem counterintuitive but a strong openness that immigration from the smartest people in the world will be good for the U.S.

Senator BLUNT. OK.

Senator SULLIVAN. Thank you, Senator Blunt.

We're going to go a second round of questions here and we've had a good attendance, so I'm sure there will likely be some other Senators returning.

I want to go back to this idea of reciprocity and a couple issues. You know, one challenge that I see with the idea that we've been discussing, this kind of pure reciprocity, is you could potentially hurt kind of the innovators in America.

Let me just give you an example. Let's say there's somebody in Silicon Valley. He or she, she, I have three daughters, so I always like to say she, she builds an AI company, builds it over 20 years. It's really good, going to sell it, puts it on the market, and the biggest bidder by far is a Chinese-backed/government-backed investment fund. OK. So there you have this issue. We could never buy an AI company from China, but at the same time, you don't want this young American woman who is an entrepreneur, who's going to get a big payday, to be told by the government, well, you can't take the highest bid, even though the highest bid is from a Chinese Communist-backed investment fund. So it creates a dilemma.

But let me also mention, and, Mr. Rosen, you touched on it, I've been looking into this reciprocity issue for a long time, but there's kind of what I call negative reciprocity, so the idea of a bill that we're talking about here.

If we can't do it there, you can't do it here, negative, but there's also what I would consider positive reciprocity, and one of the things the U.S. has done over the decades is we've gone over and done green field investments, right, you know, Google, Microsoft, GM, Ford. We build factories from the ground up. Green field, and by the way, when there was tensions between the United States and Japan in the 1970s and 1980s, one of the things the Japanese did, which was to help reduce those tensions, they came over here and built green field investments. I mean auto factories in the South and Ohio. I mean, Japanese auto manufacturers employ as many or more Americans in that sector than a lot of the Big 3 does.

The Chinese always seem very reluctant to do that. I've spent a lot of time in China in my career and I've always gone to them and said why don't you come to—don't come and buy our companies, right, don't come and try and buy the AI company, but come over and build something from the ground with your capital and your expertise and employ Americans. They're very reluctant to do that.

You talked about this, Mr. Rosen. Are you seeing a change in that? I think it would help reduce tensions. It would be similar to what happened in the 1970s and 1980s with Japan. Are you seeing that? Again, just give me a little bit more of your sense quickly on reciprocity, just pure reciprocity on investment.

Mr. ROSEN. Thank you very much, Senator. Indeed, beyond the numbers I referenced before, just the absolute volumes of direct investment, traditionally defined, the breakdown between M&A versus green field is radically different.

Senator SULLIVAN. So they don't do a lot of green field in America?

Mr. ROSEN. Well, they don't, but——

Senator SULLIVAN. Why don't they?

Mr. ROSEN.—it's partly because, you know,——

Senator SULLIVAN. Why don't they?

Mr. ROSEN.—companies from less-developed markets and economies, their first turn around the block in a highly regulated advanced economy like the U.S., not so easy to build it from scratch, much easier to buy it, especially if you have pretty attractive capital terms available to you. So we can kind of understand that.

Senator SULLIVAN. Do you think they're changing, though, because it would be in their strategic interests and I think ours and could help lower tensions?

Mr. ROSEN. It is changing, not just in the United States, but we're looking at this for comparison very closely in the European Union. There's a tendency for China to start trying to move to green field investments, but I would suggest we need to be a little bit careful here.

Indeed, there are 800,000 Americans working for Japanese-invested firms here, most of them green field, pretty big deal for employment.

Senator SULLIVAN. And working out well for both countries.

Mr. ROSEN. Yes, has been.

Senator SULLIVAN. Pretty much.

Mr. ROSEN. Has been a stabilizing and sort of moderating factor in our relationship over many decades.

However, there are also green field R&D investments taking place. For example, up around Route 128 in Silicon Valley, which overnight are putting out the word anybody who wants to double their salary who's an engineer doing autonomous driving come talk to us and they're absorbing a huge amount of the available best talent in some ecosystem catchment areas for talent and those are green fields, green field R&D operations. So those can be concerning, as well.

So just the green field kind of stream doesn't fully solve the problem but it's something that we need to think about.

Senator SULLIVAN. Let me ask one other quick question before I turn it over to some of my colleagues again.

You know, on the other hand, investments sometimes gives countries leverage and we're starting to hear about—you know, we talk about universities where these Confucius institutions, Senator Portman and his Investigation Subcommittee did some good work on this recently, put out a report, and I don't know. These are just anecdotal, but you're also starting to hear anecdotes about even the

Hollywood movie studios where there's significant Chinese investment, which there is, and when's the last time we saw a movie from a United States movie studio with Chinese investment that was anything remotely critical about China?

Are we starting to see investment in U.S. firms leading to censorship on China-related issues, and, if so, shame on the Hollywood movie studio execs if that's the case, but isn't that something else we should be concerned about? Any comments on that or am I just reading an article that might not be factual?

Mr. ROSEN. If I may, Senator, I've been teaching a class at Columbia for 18 years and in my classroom, my Chinese students, graduate school, are much less willing to engage in an open discussion than they used to be.

Senator SULLIVAN. Why?

Mr. ROSEN. They're concerned about who else is in the room, who their fellow students are, and whether there might be some, you know, consequence to them from speaking frankly.

So this is a very broad concern. It shows up in cultural areas, such as movies, although I have to say that is being sold back off by the Chinese side. They ran into financing troubles. So we'll probably get it back, like we did from the Japanese with Rockefeller Center.

But in any case, it is a broad concern not just to the United States but to virtually everyone in the advanced democratic world.

Senator SULLIVAN. Ms. Simms.

Ms. SACKS. Chairman, you asked about——

Senator SULLIVAN. Sacks, I'm sorry.

Ms. SACKS. Chairman, you asked about how this impacts firms and there's an example from the past year involving U.S. airlines and their not being able to refer to Taiwan as Taiwan but as associated with China. So censorship about the way that Taiwan is talked about and the political system there expanding to airlines and the terminology they use. So I think there's something to be looked into in that.

Senator SULLIVAN. Yes, Mr. Kallmer.

Mr. KALLMER. And I would just add, this is, you know, why it's important to have the tools. I don't know a lot personally about the movie example, but as Ms. Sacks pointed out earlier, under the revised CFIUS framework, use of data could be a relevant national security criterion and so it seems important to be able to say we've got a new thing that doesn't feel right and it almost kind of rings, if it is true, in national security terms, important to look at what the risk is, whether it can be mitigated, which is a critical question, and to be able to address it.

Senator SULLIVAN. Great. Thank you.

Senator Rosen.

STATEMENT OF HON. JACKY ROSEN,
U.S. SENATOR FROM NEVADA

Senator ROSEN. Thank you so much for holding this hearing and I appreciate that two of the panelists also have Rosen in their names. So it makes me feel very welcome here today. I appreciate that. Just had to mention that. Thank you so much.

[Laughter.]

Senator ROSEN. But, you know, this is a really important topic as we talk about China's threats today, and I want to talk really about some of the cyber military threats that we have.

You know, I'm really concerned about the emerging cybersecurity threats from China, including our intellectual property, technology transfer specifically, and cybersecurity. I just came from another hearing. This is what is on everybody's mind, privacy and security. It's what we all worry about as individuals, regardless of what our businesses are, and, of course, in Nevada, we have a lot of defense in Nevada.

Nellis Air Force Base, Fallon Naval Air Station, Nevada National Test and Training Range, Creech Air Force Base, lots of things going on there, and military's very important.

So what I want to ask a little bit and maybe, Mr. Rosenbach or anyone can take this question, what's your assessment of China's use of hybrid warfare methods, mixing conventional attacks with cyber attacks, and how does China use this strategy to influence our other Asian partners and even our allies? Anyone who would like to.

Mr. ROSENBACH. Thank you, Senator, very much, and, you know, you might want to check out some time the Cyber Flag Exercise at Nellis Air Force Base. You can go watch them fight cyber wars.

Senator ROSEN. Yes.

Mr. ROSENBACH. It's very interesting. On your question, which is really smart, the Chinese, just like the Russians, have started to use cyber as part of hybrid warfare, primarily in Southeast Asia and there near abroad.

So when they're trying to advance their interests in the South China Sea, they'll use cyber information ops, diplomacy, and other means of coercion to have the Vietnamese back down, the Philippines, even trying on the Australians.

I have a colleague who wrote a great report on this. If you want, I'd be happy to——

Senator ROSEN. I'd love to have that. Thank you.

Mr. ROSENBACH. Yes, ma'am.

Senator ROSEN. Yes, and anyone else want to respond to this?

[No response.]

Senator ROSEN. And so what do you think in your estimation, knowing that they're doing this, how can we, I guess, give the counterpunch or maybe not the counter—not be reactive. How are we being—how do you think we can best be proactive in this cyber warfare?

Mr. ROSENBACH. Yes, ma'am. In my experience, which is based primarily on all of the interactions I had with the Chinese and the PLA when we were negotiating these things, the Department of State and Defense, it was very clear that unless you give forceful action to the Chinese and you demonstrate that, that they'll continue to take as much space as they can to advance their interests.

That means you need to attribute things publicly when they do nefarious activities. You need to push back. In the Obama Administration, quite frankly, we were very often too passive up until the end and that sent the message to the Chinese that they could do aggressive things, both in cyber——

Senator ROSEN. So we need to take more aggressive approach?

Mr. ROSENBACH. Yes, ma'am, we do.

Senator ROSEN. I want to keep on this a little bit and move it out to commercial investments. Of course, they have ports across South Asia, Africa, the Middle East. What do you think the advantage that these ports provide China in a conflict with us and to what extent do you think the projects that China provides they have leverage over these countries?

Mr. ROSENBACH. I guess that's for me again. In a time of conflict and the Chinese buying key ports in Africa, even in the case of Australia, that's very significant for the U.S. military because the logistics chain is so important to the way in which you would fight a war and, you know, we hope that would never ever happen with China, but if it did, that would be a very logistics transportation heavy-type conflict and if the Chinese controlled ports where we need to have access and move things, that would be a big problem for the Department of Defense.

Senator ROSEN. They can control them not physically but cyber, cyberly, if cyberly is a word.

Mr. ROSENBACH. Cyber or could be through investment. They're doing both, I think.

Senator ROSEN. As well. Thank you. I yield back.

Senator SULLIVAN. Senator Markey.

Senator MARKEY. Thank you. This committee is going to be the Committee in drafting a new privacy policy for the country and there are intensive bipartisan discussions that are taking place right now amongst the members.

My question to you is, should we do cybersecurity simultaneously with privacy? Are they inextricably linked? If we're going to have a comprehensive policy, should we do both at the same time so that there is a new predictable environment not just here but internationally as people are looking at our country? Ms. Sacks.

Ms. SACKS. I mentioned earlier that China is further ahead than we are on this effort and we laughed about it, but the reality is they actually have a personal information protection law in advance stages in the legislative process and under their framework, under the cybersecurity law, cybersecurity and privacy are actually in the same bill and in many ways that's contradictory.

On the one hand, there are actually provisions for consent in the cybersecurity law, but they also have provisions that would allow the state security services to go in and collect more personal information and it creates a contradiction.

But I do urge this committee to think about, to understand that if that is not accelerated here in the U.S., China is moving forward in advancing their own model of what data protection means. So at the moment, we have the European model and we have the China model, and the U.S. is in a reactive position. So I commend you on this work.

Senator MARKEY. Thank you. Mr. Rosenbach.

Mr. ROSENBACH. Yes, sir. Senator Markey, I know the Committee has had several hearings on this and I think it's outstanding because it's probably the most important piece of legislation you could pass when it comes to cybersecurity and, dare I say, competitiveness in the Information Age.

If it's about information and right now the U.S. has a patchwork of laws, mostly driven by the states for this, that introduces a lot of litigation risk to firms trying to figure out what they should do, and it inhibits innovation.

So both from a national security perspective and, my opinion, an economic perspective, having a national law that's both about data protection and privacy and cybersecurity would be good for both of those areas.

Senator MARKEY. Yes, and I agree with you. I mean, I just think that they go hand in glove and ultimately it's the discussion that we put off. We should have had it in the 1990s as we were unleashing the revolution. We did not, but now we can see what the consequences are in terms of the vulnerability of the system and the vulnerability of private citizens' data, corporate data in our country.

Any others who wish to comment on that? Yes, Mr. Kallmer.

Mr. KALLMER. Thank you, Senator Markey. I would just add that this is an issue that's critically important to our members, as well, and we've been putting together actually a framework for how we would suggest the Congress think about consumer privacy legislation for the last several months with the objectives of not only having higher substantive standards for personal data protection, but also making sure that we have something that is globally interoperable and again, as with all these issues, contributes to American leadership.

On the question of how and whether to marry it up with cybersecurity topics, I think that's an intriguing idea and one we'd be interested to talk more about. There is a lot—recognizing Senator Klobuchar's good question about cybersecurity leadership, there is a lot of activity that the U.S. Government and industry work in partnership on when it comes to cybersecurity.

So I think mechanically we just want to make sure we're doing the right things in the right way, but no doubt the concepts are linked and we need to think about them together.

Senator MARKEY. Yes, and, you know, up in Greater Boston, we are now the cybersecurity capital. We're like a mini-Israel in terms of cybersecurity companies that are being developed, but it's all in reaction to the vulnerability of the system and I think it's critical for us and a lot of members are talking about that, as well, on this committee, that we develop those cybersecurity standards.

What are the expectations that we have, you know, for our corporate side but also from our governmental side in terms of the safeguards that they are going to build in because this is a daily attempt to break through the more limited safeguards which were put on the books thus far and it's only going to intensify as the years go by.

Mr. Rosenbach.

Mr. ROSENBACH. Yes, sir. I was just going to say you brought up the example of Israel and the model there is you use cybersecurity encryption, data protection as a center of gravity to build new areas of the economy that could drive the U.S. forward. So both would be great for the country from a national security perspective but great from an economic perspective in the Information Age.

Senator MARKEY. Thank you. Any others?

[No response.]

Senator MARKEY. Thank you, Mr. Chairman.

Senator SULLIVAN. A couple other follow-up questions. I want to change the subject slightly.

Mr. Rosenbach, you had mentioned this issue, which I think is a really important one, where the Chinese Government, kind of coordinated with companies, is engaging in activities that not only our government doesn't do, that people do it in government or in the private sector, they would violate laws.

So the biggest one there is the Foreign Corrupt Practices Act, right. We don't go and bribe foreign government officials to get deals and if American companies go bribe foreign officials to get deals, they can go to jail. That's just the way Congress thought that should be addressed.

I'm going to submit for the record here a *Wall Street Journal* investigation. It's called "Wall Street Journal Investigation: China Offered to Bail Out Troubled Malaysian Fund in Return for Deals." Without objection for the record.

[The *Wall Street Journal investigation follows:]*

WSJ Investigation: China Offered to Bail Out Troubled Malaysian Fund in Return for Deals - *The Secret discussions show how China uses its political and financial clout to bolster its position overseas.*

By: Tom Wright and Bradley Hope
January 7, 2019

Senior Chinese leaders offered in 2016 to help bail out a Malaysian government fund at the center of a swelling, multibillion-dollar graft scandal, according to minutes from a series of previously undisclosed meetings reviewed by The Wall Street Journal.

Chinese officials told visiting Malaysians that China would use its influence to try to get the U.S. and other countries to drop their probes of allegations that allies of then-Prime Minister Najib Razak and others plundered the fund known as 1MDB, the minutes show.
The Chinese also offered to bug the homes and offices of Journal reporters in Hong Kong who were investigating the fund, to learn who was leaking information to them, according to the minutes.

In return, Malaysia offered lucrative stakes in railway and pipeline projects for China's One Belt, One Road program of building infrastructure abroad. Within months, Mr. Najib—who has denied any wrongdoing in the 1MDB matter—signed $34 billion of rail, pipeline and other deals with Chinese state companies, to be funded by Chinese banks and built by Chinese workers.
Mr. Najib also embarked on secret talks with China's leadership to let Chinese navy ships dock at two Malaysian ports, say two people familiar with the discussions. Such permission would have been a significant concession to Beijing, which seeks greater influence across contested waters of the South China Sea, but it didn't come to pass.

Tightening LinksMalaysia has grown more dependent on China in recent years with more imports and awidening trade deficit with China.Sources: World Integrated Trade Solution; Malaysia External Trade Development CorporationNote: 2018 figures are through October
.billionExports to ChinaImports from
China2008'09'10'11'12'13'14'15'16'17'18152025303540$45

A Journal examination of the China-Malaysia projects, based on documents and interviews with current and former Malaysian officials, offers one of the most detailed accounts to date of the political forces at work behind China's Belt and Road program, a signature initiative of building ports, railways, roads and pipelines in some 70 countries to generate trade and business for Chinese companies.

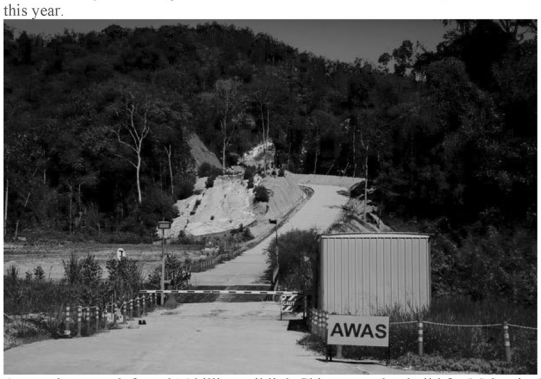
U.S. officials say China is using the program to increase its sway over developing nations and trap them in debt while advancing its military aims. Several countries, including Pakistan and the Maldives, have been reviewing One Belt, One Road projects amid allegations some deals unfairly advanced Beijing's interests.

American national-security officials regard the Chinese efforts in Malaysia as Beijing's most ambitious attempt to leverage the program for geostrategic gain, said a person familiar with U.S.

discussions. Minutes of the Chinese-Malaysian meetings say that although the projects' purposes were "political in nature"—to shore up Mr. Najib's government, settle the 1MDB debts and deepen Chinese influence in Malaysia—it was imperative the public see them as market-driven. The Chinese government information office didn't respond to requests for comment.
China has said its Belt and Road projects promote development that benefits all sides. Nations wouldn't welcome the program as they have if it carried the financial and geopolitical risks asserted by critics, China's Foreign Ministry has said. It has denied that money in the program was used to help bail out the troubled Malaysian fund.

Documents reviewed by the Journal show Malaysian officials suggested that some of the infrastructure projects be financed at above-market values, generating excess cash for other needs. Investigators from the current Malaysian government, which replaced Mr. Najib's last year, believe some of the money helped Mr. Najib finance his political activities and cover maturing debts of 1MDB, a fund he set up in 2009 to finance local development.
Mr. Najib was aware of the 2016 Malaysian-Chinese meetings, according to people familiar with them. Asked about them, the former prime minister issued a statement saying the rail project would have brought tens of thousands of jobs to Malaysia and stating that under his leadership, the country experienced nine years of continuous economic growth.

Current Malaysian Prime Minister Mahathir Mohamad, who ousted Mr. Najib in an election last May, put the Chinese projects on hold. Malaysia has since charged Mr. Najib with crimes that include money laundering and breach of trust. He has denied them, is free on bail and faces trial this year.



A tunnel approach for a $16 billion rail link China agreed to build for Malaysia. The government that took over in Malaysia last year has suspended the project.
PHOTO: JOSHUA PAUL FOR THE WALL STREET JOURNAL

Malaysia, rich in natural resources and on a sea lane, is a prized ally in the U.S.-China contest for influence in Asia. The U.S. once courted Mr. Najib as it sought alliances in the region. In July

2015, the Journal reported that $681 million of funds originating with 1MDB, known formally as 1Malaysia Development Bhd., had flowed into Mr. Najib's personal bank accounts. Mr. Najib's office said the money was a gift from a Saudi Arabian it didn't identify and said most of it was eventually returned.

The U.S. Justice Department began investigating. Its probe damaged Washington's relationship with Mr. Najib, according to officials in both countries, helping drive Malaysia into Beijing's arms.

By 2016, Mr. Najib was in a bind because the fund had borrowed $13 billion it couldn't repay. He turned to Jho Low—a Malaysian financier the U.S. Justice Department has alleged was the mastermind of a multibillion-dollar theft of 1MDB funds—to negotiate with China to resolve the crisis, according to current and former Malaysian officials.

Jho Low, a central figure in a multibillion-dollar scandal at a Malaysian development fund. A now-suspended Chinese 'Belt and Road' project in Malaysia might have partially bailed out the fund's debts.
PHOTO: KRISTIN CALLAHAN/ZUMA PRESS

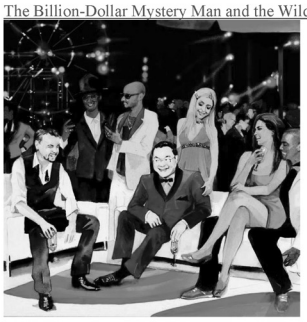
Mr. Low faces criminal charges in both Malaysia and the U.S. related to the Malaysian fund. The U.S. has sought to seize hundreds of millions of dollars of his luxury assets it alleges were acquired with the fund's money. Mr. Low has denied wrongdoing. He is a fugitive, living in

China under Beijing's protection, according to Malaysian officials. Chinese officials have declined to comment on that.

Mr. Low drew up plans for Malaysian meetings with Chinese officials and attended some of them, according to current and former Malaysian officials.
A spokesman for Mr. Low said he denies the allegations, calling them "baseless political accusations" and "a selection of half-truths, mixed in with fiction, to create a misleading and oversimplified narrative."

Malaysia's new government discovered the documents, including minutes from Chinese-Malaysian meetings over several months, after a sweep of Mr. Najib's offices, according to members of the government. The Journal, besides reviewing the documents, interviewed people in position to know the events, among them a former official of Mr. Najib's government.
The documents describe a plan proposed by Malaysian officials for Chinese state companies to build two large projects with funding from Chinese banks. One, the $16 billion East Coast Rail Link, would be a railway across Malaysia connecting two ports. The other, the $2.5 billion Trans Sabah Gas Pipeline, would be built partly on Malaysia's portion of the island of Borneo.

The Billion-Dollar Mystery Man and the Wildest Party Vegas Ever Saw



The projects would provide "above market profitability" to the Chinese state companies, the documents say. The rail link should have cost only $7.25 billion to build, according to an earlier estimate by a Malaysian consultancy, said a Malaysian government official.
The public must believe "all initiatives are market driven for the mutual benefit of both countries," Chinese official Xiao Yaqing said at a meeting on June 28, 2016, according to minutes of the meeting.
Mr. Xiao, chairman of China's State-owned Assets Supervision and Administration Commission, said he had "cancelled all his key engagements in Beijing to attend" because the matter "has been approved by President Xi Jinping, Premier Li Keqiang " and another senior

Chinese official, according to the minutes. Mr. Xiao's agency didn't respond to requests for comment.

At a meeting the next day, Sun Lijun, then head of China's domestic-security force, confirmed that China's government was surveilling the Journal in Hong Kong at Malaysia's request, including "full scale residence/office/device tapping, computer/phone/web data retrieval, and full operational surveillance," according to a Malaysian summary of that meeting.

Chinese official Xiao Yaqing, seen at a June summit of China's 'Belt and Road' program of building infrastructure in dozens of other countries.
PHOTO: ANTHONY KWAN/BLOOMBERG NEWS

"Mr. Sun says that they will establish all links that WSJ HK has with Malaysia-related individuals and will hand over the wealth of data to Malaysia through 'back-channels' once everything is ready," the summary reads. "It is then up to Malaysia to do the necessary."
It couldn't be determined whether China provided any information. Mr. Sun didn't respond to requests for comment.

A Journal spokesman said, "We employ experts on security and cybersecurity to work with our journalists on safety and secure communications with sources of information."
Mr. Sun also promised to use China's "leverage on other nations" to get the U.S. and others to drop their 1MDB investigations, according to the meeting summary. The Justice Department investigation continued, as did probes in Singapore, Switzerland and elsewhere.
At one meeting, the Malaysians asked that the Chinese state company that would build the rail link assume $4.78 billion of 1MDB debt, a plan they hoped China would agree to quickly "due to the time sensitive nature" of the fund's debts, according to the documents.
A Chinese negotiator worried this would be "very noticeable" in financial statements of the builder, China Communications Construction Co. , meeting minutes show.

A month later, the Malaysians proposed that Chinese state companies instead make payments that would "indirectly be used to repay 1MDB debt," according to meeting minutes.

Five years into China's massive Belt and Road Initiative, the U.S. is trying to respond to Xi Jinping's infrastructure-building spree. Illustration: Crystal Tai
Notes of a discussion on Sept. 22, 2016, say the sides agreed to move ahead with the infrastructure deals even though "they may not have strong project financials." Participants needn't "waste time studying the actual project financials to see if they can sustain the debt etc.," because Malaysia's government backed the deals for strategic reasons, the documents say.

Notes from that meeting said Malaysia was working to enhance bilateral ties, citing support Mr. Najib voiced for China's position in the South China Sea during a regional summit in Laos. Two months later, Mr. Najib went to Beijing and signed the deals. Together with other projects, they made Malaysia the second-biggest recipient of One Belt, One Road funding after Pakistan. Money was flowing by the middle of 2017 as the Export-Import Bank of China issued the first loans. By fall the bank had paid out 80% of the $2.5 billion pledged to state-owned China Petroleum Pipeline Bureau to build the pipeline, although little work had been done, according to Malaysian officials.

Malaysian Prime Minister Mahathir Mohamad, center, suspended plans for Chinese companies to build costly rail and pipeline projects in Malaysia.
PHOTO: RAHMAN ROSLAN/BLOOMBERG NEWS

When campaigning for Malaysian parliamentary elections began early in 2018, China openly sided with Mr. Najib, its ambassador at one point campaigning with members of his coalition. Against the odds, Mr. Mahathir, a prominent former prime minister then 92 years old, led his coalition to victory.

Now, Mr. Mahathir is negotiating with Beijing over potential new terms for the railroad project and seeking the return of Mr. Low. Excavators for the rail projects are idle, and workers' quarters are vacant. Mr. Mahathir is expected to cancel the pipeline deal.
—Lekai Liu contributed to this article.

Write to Tom Wright at tom.wright@wsj.com and Bradley Hope at bradley.hope@wsj.com

87990cbe856818d5eddac44c7b1cdeb8
Appeared in the January 8, 2019, print edition as '.'

Senator SULLIVAN. This is a really extensive *Wall Street Journal* report that shows the extent to which at the most senior levels in the Chinese Government official corruption was pushed as part of the policy to get Chinese predatory infrastructure financing through the bribery of foreign officials around the world.

Now, of course, this puts American companies at a comparative disadvantage if they're trying to do infrastructure developments in other parts of the world and Chinese senior government officials are bribing officials in those countries.

Can any of you speak to this issue of corruption, official Chinese corruption with regard to global deals and how you think we should be trying to address that, as well? You want to start, Mr. Rosenbach?

Mr. ROSENBACH. Honestly, Senator, I don't have any factual data on that. I only know what we would hear often or see in intelligence about Chinese officials offering things on the side for deals, in particular connected to telecom deals in Africa.

Senator SULLIVAN. But do you think that that's something again us as a country and our allies should be working on together so we essentially say to the Chinese this is unacceptable,——

Mr. ROSENBACH. Yes, of course.

Senator SULLIVAN.—not acceptable?

Mr. ROSENBACH. Right. It's unfair for an American firm to have to do all the due diligence that goes into upholding the Foreign Corrupt Practices Act, which is expensive just from a legal perspective, and to know that people aren't playing by those same rules and could be sliding money across the table to win a deal when they don't even have the best technology or the best services.

Senator SULLIVAN. Mr. Rosen, you had a comment?

Mr. ROSEN. Senator, if I can broaden the concern you're expressing a little bit to not just to corrupt factor in the equation, if you will, but all sorts of politicization of the investment process, right. That ultimately creates a risk of financial instability which is a concern, a national security concern to us and our allies, as well.

We've worked, you know, post World War II, kind of half that period. We, unfortunately, were part of building up debt loads in a lot of developing countries and then the second half of that period, we've tried to remedy that and improve the development outlook for, you know, the same 75 or hundred countries that China is now trying to design the belt and road program for.

I just have a tremendous concern that China's attempt to cut corners on diligent investment at home has created the biggest trap of all for China itself, right. We talk about the risk to China's growth outlook now because it's been so over-reliant at home on debt. Well, as it now goes abroad with the development program, it's essentially exporting the same risks that are woven into its economic structure and model into a lot of other very fragile nations around the world.

We know, unfortunately, from experience that when fragile, politically fragile places, like Venezuela, avail themselves of easy credit card options, just like college students, they tend to wind up in trouble and we're seeing that in too many places today. So that's not corruption alone, but it is something which I think deserves our

attention. The spillovers of China's model, how that can be deleterious to our national security interests.

Senator SULLIVAN. Let me ask a final question of all of you from my perspective and again I appreciate it. This has been a really good discussion and unless there's additional followup, OK, and, well, maybe I'll have Senator Rosen ask her question and then I'll end with mine.

Senator Rosen.

Senator ROSEN. Thank you. I appreciate it. You know, in order to respond to security threats and, of course, prepare for new challenges across the spectrum frankly, we have to ensure that we have enough trained cybersecurity and just IT professionals in general. So here in Congress, we set great legislation, apprenticeships, opportunity grants, tax credits, whatever tools we have available to us.

So what Federal investments do you think we can best make right now so we can be proactive against these threats? Anyone? No? No one has an idea of investments that we can make into our——

Mr. ROSEN. I love the expanded——

Senator ROSEN.—economy, into our work force?

Mr. ROSEN.—provisioning for human resources around the CFIUS process and now the FIRRMA expanded CFIUS process to make sure there's an adequate team of people who can quickly go over many more transactions, not tying up American commerce with long lengthy review time tables, but instead turn back clarity, as all the panelists have said.

Most important is that we can quickly narrow down to the transactions that are concerning to us and let the ones that are not concerning go through quick so people can create jobs.

Senator ROSEN. So maybe I'm not exactly clear. I'm talking about what investments can we make in human capital or even hardware capital, computing capital, if you will, quantum computing, artificial intelligence that's going to help with this, so we need both? Please.

Mr. KALLMER. So a lot of things that we can do and we have worked with the Congress and the Administration and are eager to continue doing it.

Some of it has to do with developing capacity on emerging technologies, AI, 5G, quantum computing. We recently made a recommendation to the Administration to work with the Congress to promote that because the growth and leadership potential is significant. STEM education so that we can continue to build a U.S. workforce of people that are prepared for these jobs, continued partnerships with universities, continued R&D investment in precompetitive basic research, the kind of things that we've had legendary cooperation on.

Senator ROSEN. Right. Not just first stage research but research going all the way through.

Mr. KALLMER. So it's a great question and something we think about a lot.

Senator ROSEN. Thank you.

Ms. SACKS. I have two recommendations. In my previous life, I worked with Siemens in their Industrial Cybersecurity Business

and I think that the next frontier and risk is what we call operating technology or where the IT meets the physical infrastructure and this is an idea where I think we absolutely should focus more resources in training expertise.

The second is on diversity and inclusion issues, focusing more on how can we get sort of multiple voices. Gender is a particular one in the cybersecurity space. When we think about issues like algorithmic bias, that's going to be very important.

Senator ROSEN. I had a Code like a Girl Bill. I'm a former computer programmer. That was the first bill I put when I was in Congress. I'm going to be reintroducing that again. So we'll be addressing that one.

Thank you.

Mr. ROSENBACH. I was just going to say one thing real quick. You know, I teach and students are always looking for a way to get into government and serve and so something that would be like an ROTC program for undergrads or maybe grads where they then go into government, serve in cyber-security.

Senator ROSEN. Like a reserve program.

Mr. ROSENBACH. They could go into the private sector.

Senator ROSEN. Like a cyber reserve, like the Army.

Mr. ROSENBACH. We have a long tradition in the military doing that in the U.S. and Israel. Something like that I think could be effective.

Senator ROSEN. I think that's a great idea. Thank you so much.

Senator SULLIVAN. Senator Blumenthal.

STATEMENT OF HON. RICHARD BLUMENTHAL, U.S. SENATOR FROM CONNECTICUT

Senator BLUMENTHAL. Thank you, Mr. Chairman. I understand and I apologize that I've been at various other hearings, as all of us have been, that Mr. Rosenbach notes that authoritarian regimes have stolen large amounts of sensitive personal data from consumers.

There are a list of them, a litany. This information directly provides China with strategic intelligence and economic advantage but it also feeds into a surplus of raw material that can be developed, used to develop new technologies.

Do members of the panel agree that privacy rights with respect to China or any other of these countries are also a matter of national security and that in pursuing privacy, as we are doing in this committee, for consumers in general, we are helping to protect national security? Mr. Rosen.

Mr. ROSEN. I think my colleagues have offered more considered perspectives on the integration of the privacy agenda with cyber and security agendas. So I would defer to them to elaborate.

Mr. KALLMER. Happy to do so, Senator Blumenthal. It's a great point, and I think what we've observed is that there absolutely can be alignment. In fact, one of the topics we've discussed a little bit today is the revised CFIUS bill, which, of course, is a process designed round national security and inward investments and other economic activity.

The fact that it is now expanded to include a reference to the use of data, the use of personal data as a potential national security

criterion is positive. The U.S. Government has to be flexible to address new kinds of threats that come around and also explore whether those threats can be mitigated so as not to interfere with business and innovation, but it's a good question.

Senator BLUMENTHAL. Do you agree?

Ms. SACKS. (Nods.)

Senator BLUMENTHAL. Let me shift to Huawei. Should the U.S. Government and our allies be satisfied by the show and tell that this company has offered us? What are the tactics that Huawei could use in terms of back door use of its equipment and is it preventable?

Mr. ROSEN. I will offer that that's principally a technical question and so again I would defer to my colleagues that are from the technology backgrounds.

However, I will say that from a sort of high-level perspective, the basic problem of China in our time is that in previous years, China explicitly identified its own need to separate commercial and government intentions and combination in the marketplace.

In just the past few years, that objective on China's part and the need for it has become very murky and that is prima facie concerning to any other market economy concerned that if you don't have a nice crisp boundary around what's official and what's commercial, it's very hard for other nations to embrace especially critical infrastructure-related offerings from those vendors.

Senator BLUMENTHAL. Let me explain the reason for my question and maybe I asked it in too shorthand a way.

This company, as you know, has continued to court our allies in Europe principally. One of its tactics there has been to allow governments to inspect the source code of their devices. In other words, to kind of peek under the hood and assume that everything else is fine, everything else is safe, but experts warn that the result is a false sense of security.

Huawei doesn't simply hand over the equipment. It provides software updates and often directly manages the network. All of these services create ongoing potential vulnerabilities and they're not just vulnerabilities that serve the company but they serve a potential adversary in terms of national security, as you have correctly characterized them.

So I welcome any other views on this topic.

Ms. SACKS. When we talk about the risk of Huawei, I think it's important first to identify three distinct risks so we can mitigate around that. These often get blurred. So one is does Huawei have a back door that would allow access? The other is shoddy engineering and, quite frankly, that's what our partners in the U.K. have found, which is different, and the third is what would a company like Huawei be prevailed upon to do in a warlike situation?

So what cybersecurity practitioners will say is an outright blanket ban is not the most effective way to deal with that risk. Instead, you identify specific quantifiable risks associated with certain technologies and you design a management system around that.

Mr. ROSENBACH. I know we're overtime, so you all tell me if I need to be quiet, but I would say, Senator, this is really important to look at.

The example you had of looking at the source code is an example in which just that day you would be able to say this looks clean because they'll do a software upgrade. They will have remote access. The gear with Huawei core routers is configured so that you can have remote access.

In the case of the U.K., this is about 5 years ago, they set up a center that reviewed all the gear, looked at it, put it into their network. Today, because of both shoddy engineering and concerns about security, they're ripping it all out of their network.

So you just need to keep in mind a glimpse and a snapshot on 1 day does not mean that there's not special sauce baked in there and down the road.

Senator BLUMENTHAL. Well, I think that point is extremely important and you put it better than I did, but let me just say in conclusion because I'm out of time, we are in a warlike setting.

Ms. SACKS. Are we?

Senator BLUMENTHAL. I don't think too many people would doubt having read, heard, seen the conflicts that are ongoing in the cyber domain that we are in a warlike setting and I think that's the reason that justifiably I and many of my colleagues have called for much greater advocacy to protect our national security.

Senator SULLIVAN. Senator Markey.

Senator MARKEY. Thank you so much. According to reports, China and the United States have agreed on a pact that would require Beijing to purchase American agriculture and energy goods while also lowering some trade barriers inhibiting U.S. companies from accessing Chinese markets.

But those reports suggest that the deal would not ensure that China curtails intellectual property theft, cyber attacks or subsidies that create uneven playing fields for American companies.

Should those concessions also be a part of any deal given that we know these have long-term implications for our country if we don't deal with them right now and China does want to deal? Yes, Mr. Kallmer.

Mr. KALLMER. I don't know the state of the pact right now, but if it were an agreement that only dealt with purchases and didn't make serious inroads on the structural systemic issues, it would be a colossal missed opportunity. The Administration has done great work in getting to this point with the Chinese taking it seriously, but it needs to address those issues. It needs to have meaningful enforcement and verification mechanisms and ultimately it needs to be a multinational effort to make sure China abides by it.

Senator MARKEY. OK. Great. And I'm concerned about Beijing's efforts to hack U.S. defense contractors and research institutions to steal sensitive military information.

Earlier this week, the *Wall Street Journal* reported that a known Chinese hacking group is behind a series of cyber attacks on universities in the United States in an elaborate scheme to steal research about maritime technology.

Ms. Sacks, what should we be doing at the Federal level in order to protect our military secrets from Chinese hackers?

Ms. SACKS. The Chinese Government under Xi Jinping has invested tremendously in elevating cyber policy. They created a very

powerful entity within the Chinese bureaucracy to funnel much more resources and focus to this issue.

So I think it's imperative that on our side we also invest in making sure that cyber is a high-priority element within the U.S. Government bureaucracy because they certainly are doing so.

Senator MARKEY. Yes. And any other comments on that?

Mr. ROSENBACH. Sir, I would just say we have worked on this problem for almost a decade. The Chinese continue to take aggressive action like this, very strategically targeting an area in which they need to leap ahead the United States Navy in submersible technology autonomous underwater vehicles and so they do it very consciously.

It's just not fair to expect a university doing research on this to be protecting itself and spending money at the level that you're trying to thwart the PLA and so you need to think about ways that maybe even the government or another defense contractor is bringing cybersecurity solutions because otherwise that investment is flowing out the door. The Chinese and the PLA are reaping the benefits of that.

Senator MARKEY. Yes, so I thank you. So, you know, from my perspective, Mr. Chairman, just an incredibly successful first hearing——

Senator SULLIVAN. Yes.

Senator MARKEY.—on this subject, and we're just scratching the surface of all of the issues that we're going to have to deal with.

When I think of the Chinese and I think of their Belt and Road Initiative and trying to move into countries very friendly, like want to help you there in Sri Lanka, want to help you there in Malaysia, we'll give you all this discount access to what it is that you might need for your infrastructure and then buyer's remorse on the part of these countries. What have we done in allowing them in without asking the questions upfront in terms of what the strings are that are attached, this Trojan horse strategy which they have in technology after technology in country after country.

So when we talk about Huawei, we talk about any of the rest of these issues that are in this whole complex, that it's critical for us to start asking questions and then proposing answers because we're already deep in and it's pretty obvious that we haven't had the national conversation that will create the policies that can give us a strategy that matches the magnitude of the strategy which the Chinese already have in effect.

So I thank you, Mr. Chairman, and I thank the witnesses for this very good hearing.

Senator SULLIVAN. Thank you. I'll just wrap it with a comment and then a final opportunity for comments from our witnesses, but thank you. You guys have done a great job for our first hearing.

You know, I think what we're seeing here is a strong bipartisan sense of a challenge that we need to address and in some ways that's good that we're working together on this, and I also do want to compliment the President and his Administration.

If you've looked at, for example, the National Security Strategy of the Trump Administration, the National Defense Strategy, these are very serious documents. I think they have a lot of bipartisan support.

Our friends in the media don't write about that a lot, but they've also recognized the challenge, right. The big National Security Strategy's a shift from, you know, rightfully we've been looking at the challenge of violent extremist organizations since 9/11 as the primary challenge to our Nation's security. That's still, of course, an ongoing challenge, will be for a long time.

But the Trump Administration's National Security Strategy and National Defense Strategy recognizes that the return of great power rivalry with China as the pacing threat is the biggest geostrategic challenge for the next 50 to a hundred years. I happen to believe that. That's why we had this hearing as our first hearing.

I also think they're doing a good job on these trade issues. The tariffs are controversial to some, but I think the President and his team have put this front and center. So they're in these negotiations now. A number of us have been working with the Administration on things like structural reforms, enforcement mechanisms, starting to address this corruption issue.

There are some, you know, in the United States who are saying cut this deal now, get it done. The stock market will probably go up if you do it.

Any final thoughts for the Administration as they are engaged in a tough negotiation and again to their credit, they've put this front and center in ways that I think previous Administrations, Democrats and Republicans, for a number of reasons have kind of swept it under the rug. So kudos to them.

But any final thoughts to the Administration on this near-term challenge of what they should be trying to achieve? Mr. Kallmer, you already mentioned it. Anyone else, just thoughts for Ambassador Lighthizer and Secretary Mnuchin and others? Yes, Ms. Sacks.

Ms. SACKS. Last week, Ambassador Lighthizer testified before the House Ways and Means Committee and he said the negotiations ongoing are really dealing with the structural issues, IP, tech transfer, cyber espionage, and so I would really encourage this Administration to use this moment of potential leverage to really tackle these issues and to not settle for a cosmetic deal.

We heard that China has announced they're going to make technology transfer illegal, but let's get——

Senator SULLIVAN. Haven't they been saying that for 30 years?

Ms. SACKS. Right. And so that's why I bring up the issue of standards. Look at where are these vulnerabilities actually occurring and come up with a targeted way to get at them, right. Don't just look at this Made in China 2025 being as being a rollback.

Senator SULLIVAN. Great. Anyone else for final—Mr. Rosen.

Mr. ROSEN. Any deal that does not include an extraordinary amount of structural work that China commits to doing, an extraordinary amount of acknowledgement by China that its freedom to swing its fist stops where other people's noses begin, and that its non-market choices right now are having deleterious consequences for others, any deal that doesn't have those elements and others is not going to be a deal that lasts more than about 45 minutes.

So there's really two deals we need to prepare for. One in which China gets back to believing that marketization is in its own interests and is the only path forward, which Deng Xiaoping, Zhu Rongji and many of the other leaders we've seen in the past 40 years believed, and another deal that we have to be prepared for in which China continues to think that there's an alternative model that it can pursue.

In the latter case, there's only so much engagement that's going to be possible between us and it's going to be very painful to us to have to live with that.

Senator SULLIVAN. But we need to work with our allies on this, too. Does everybody agree with that?

Mr. ROSEN. Right. There's no way we can absorb the cost of that if it's 20 different advanced economies all trying to cut their own deals.

Senator SULLIVAN. Well, listen, thanks again. I think this has been a great hearing.

The hearing record will remain open for two weeks. During this time, Senators may submit additional questions for the record. Upon receipt, the witnesses are respectfully requested to submit their written answers to the Committee as soon as they can.

I thank again the witnesses for appearing here today.

This hearing is now adjourned.

[Whereupon, at 11:59 a.m., the hearing was adjourned.]

A P P E N D I X

RAIL SECURITY ALLIANCE
March 6, 2019

Hon. DAN SULLIVAN,
Chairman,
Subcommittee on Security,
U.S. Senate Committee on Commerce, Science, and Transportation,
Washington, DC.

Dear Chairman Sullivan:

The Rail Security Alliance congratulates you in convening the inaugural hearing of the Senate Committee on Commerce, Science, and Transportation's Subcommittee on Security. The topic of the hearing "China Challenges for U.S. Commerce" is a timely topic that is vital to both the economic and national security interests of the United States. We appreciate the opportunity to communicate to you the work of the Rail Security Alliance and the importance of protecting U.S. commerce from the unfair practices from the People's Republic of China.

The Rail Security Alliance is a coalition of North American freight rail manufacturers, suppliers, unions, and steel interests that is committed to ensuring the economic and national security of passenger and freight rail systems. This alliance was formed in response to the merging of China's two rail manufacturers into one massive state-owned enterprise, the China Railroad Rolling Stock Corporation (CRRC). CRRC, by their own calculation, controls roughly 83 percent of the global rail market. As a state-owned enterprise, CRRC has access to unlimited state funding that allows them to win contracts around the world by underbidding every other competitor, jeopardizing the future of this industry.

Over the past three years, the Chinese state-owned enterprise China Railway Rolling Stock Corporation (CRRC) has aggressively targeted the U.S. market as a means of advancing China's "Made in China 2025" initiative, which aims to overtake the United States and other nations in critical industries like passenger and freight railcar manufacturing. Using state-backed financing and other anti-competitive tactics, CRRC has now secured $2.6 billion in contracts to build metro transit cars for Boston, Chicago, Philadelphia, and Los Angeles, sometimes underbidding its competitors by as much as several hundred million dollars.

This threat is now knocking on the doors of Washington. WMATA, Washington's metro system, is seeking to procure new metro cars this year and it is becoming increasingly clear that CRRC could win this contract. With no Buy America or Disadvantaged Business Enterprise (DBE) requirements for this contract, CRRC is well positioned to make a compelling bid. Needless to say, the prospect of metro cars manufactured by the Government of China running under or near the Pentagon, the Capitol, the White House, and other sensitive installations should raise every alarm across this city.

The freight system is not immune to CRRC either. CRRC has also attempted to enter the North American freight rail manufacturing sector—first with a joint venture in North Carolina that fortunately did not come to full-fruition, and now with a separate facility in Moncton, New Brunswick. We have seen this pattern before. CRRC entered the Australian market in 2008 and decimated its domestic manufacturers in just nine years. We would be naïve to think that cannot and will not happen here.

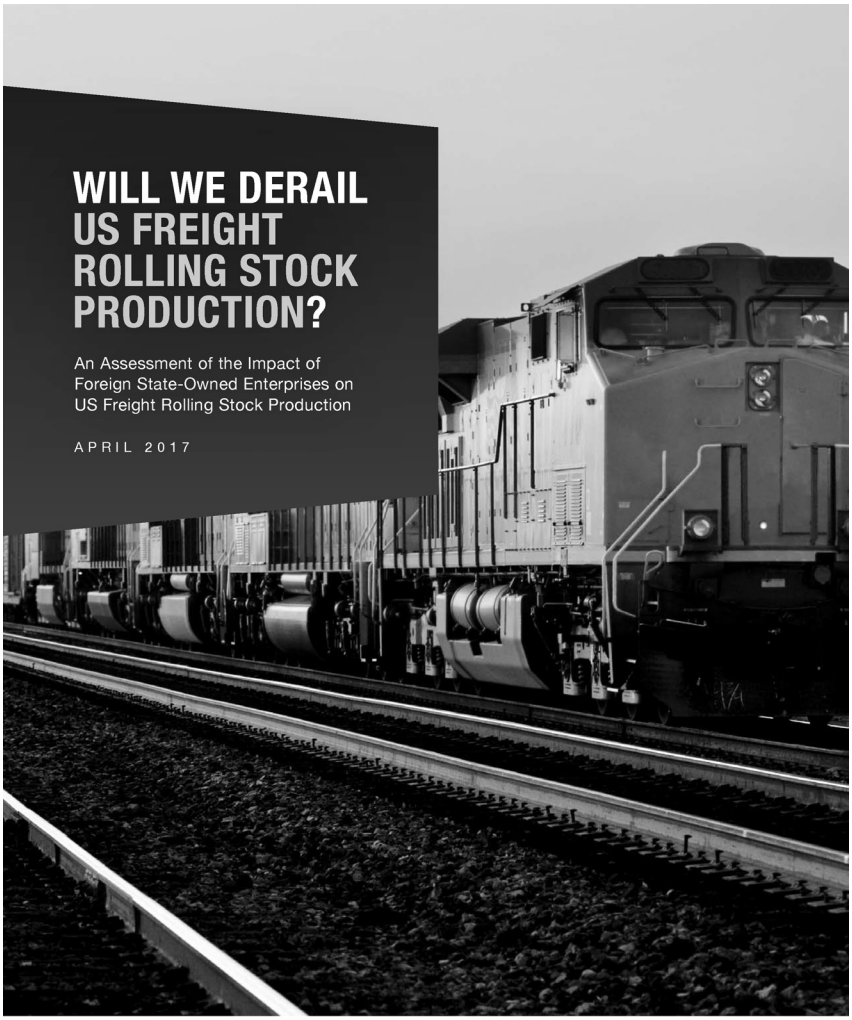
We have attached for the Committee record a report from Oxford Economics illustrating how a similar pattern in the United States could result in the loss of roughly 65,000 American jobs in the freight sector alone, along with a $6.5 billion reduction in U.S. GDP. Furthermore, we have also included a report from Brig. Gen. John Adams (USA, Ret.) on the national security risks inherent in allowing a Chinese state-owned enterprise access to our freight and transit rail systems.

Allowing Chinese state-owned enterprises to continue expanding and operating in the United States without appropriate oversight presents major risks to the economic and national security of our country. The United States can no longer risk an unchecked China doing business on our shores.

Again, congratulations on chairing the inaugural hearing for the Subcommittee on Security. We appreciate that you chose to highlight the threat of China to American commerce and we look forward to our continued work together.

Respectfully submitted,

ERIK ROBERT OLSON,
Vice President,
Rail Security Alliance.



CONTENTS

OXFORD ECONOMICS

ABOUT OXFORD ECONOMICS

Oxford Economics was founded in 1981 as a commercial venture with Oxford University's business college to provide economic forecasting and modeling to UK companies and financial institutions expanding abroad. Since then, we have become one of the world's foremost independent global advisory firms, providing reports, forecasts, and analytical tools on 200 countries, 100 industrial sectors and over 3,000 cities. Our best-of-class global economic and industry models and analytical tools give us an unparalleled ability to forecast external market trends and assess their economic, social and business impact.

Headquartered in Oxford, England, with regional centers in London, New York, and Singapore, Oxford Economics has offices across the globe in Belfast, Chicago, Dubai, Miami, Milan, Paris, Philadelphia, San Francisco, and Washington DC. We employ over 300 full-time people, including more than 200 professional economists, industry experts, and business editors—one of the largest teams of macroeconomists and thought leadership specialists. Our global team is highly skilled in a full range of research techniques and thought leadership capabilities, from econometric modeling, scenario framing, and economic impact analysis to market surveys, case studies, expert panels, and web analytics. Underpinning our in-house expertise is a contributor network of over 500 economists, analysts, and journalists around the world.

Oxford Economics is a key adviser to corporate, financial and government decision-makers and thought leaders. Our worldwide client base now comprises over 1000 international organizations, including leading multinational companies and financial institutions; key government bodies and trade associations; and top universities, consultancies, and think tanks.

April 28, 2017

The modeling and results presented here are based on information provided by third parties, upon which Oxford Economics has relied in producing its report and forecasts in good faith. Any subsequent revision or update of those data will affect the assessments and projections shown.

EXECUTIVE SUMMARY

Up to 65,000 jobs at risk

In the US if foreign state-owned enterprises collapse domestic freight rolling stock manufacturing

Estimate based on foreign SOEs capturing the $5 Billion freight rail manufacturing market

Up to $6.5 billion lost in US GDP

Includes $5 Billion lost in freight rail market, plus loss productivity in domestic supply chains and lost domestic wages and spending

Estimate based on foreign SOEs capturing the entirety of the freight rail manufacturing market

The North American Freight Rail system is one of the most dynamic in the world and has been a key driver of US prosperity. To support the development, growth, and operations of the US rail system, a vast network of suppliers and producers has been established. The future of these long-established producers and suppliers is now potentially at risk because of alleged anti-competitive practices—such as state-supported financing–carried out by foreign state-owned enterprises, predominately from China. Findings from original research and modeling describe the potential losses to the US economy should foreign SOEs achieve dominance over the US freight rail market.

Manufacturers in the US have been producing railcars and rolling stock for more than 170 years. Over time this has had a transformative impact on parts of the US economy, and to this day, American companies still produce the majority of freight railcars seen on tracks across the country. However, the pace of globalization and the arrival of entrants from countries such as China into the US market, are threatening domestic competitiveness. In passenger rail manufacturing, the fallout is already being felt nationwide, from Boston to Chicago and Los Angeles.

Serious concerns are being raised about the aims and impact of state-owned enterprises, especially from China, on domestic producers—ranging from steel products to washing machines. Well-functioning capitalist markets, of course, thrive on fair and open competition to promote efficiency, reduce costs and improve innovation. However, this can be undermined by the activities of state-owned enterprises (SOEs), which are advantaged by the subsidies and support they receive from their home country at the expense of other companies that do not receive such benefits.

In the passenger rail market, the arrival of foreign SOEs is already threatening the ability of domestic US manufacturers to compete.

Concerns have been raised regarding unfair practices—such as subsidized financing from the Chinese government—which may have played a key part in the ability of one SOE to underbid the next lowest competitor by more than $150 million for a recent project with Boston's MBTA as well as winning other projects in Chicago, L.A. and Philadelphia. In 2015, a Chinese SOE publicly stated its goal of doubling its export sales, particularly targeting the North American passenger and transit car market.[1]

The experience of Australia suggests that the end result could be the collapse and/or offshoring of railcar manufacturing in the US. Over the past roughly 15 years, Australia experienced a rapid decline of domestic railcar production and increased reliance on foreign-produced railcars from Chinese SOEs and other SE Asian countries. This experience is discussed in detail in Section 3 of the report.

In the US freight railcar market, the potential for disruption and loss to the US economy may be even more acute than in Australia, especially given the larger size of US freight railcar demand. The recent expansion of Chinese SOE passenger and transit railcar production in the US, therefore, justifies an examination of the possible implications for US jobs and output as Chinese SOEs seek to expand their presence in the North American freight car market. Through a joint venture, one SOE has already established a beachhead for Chinese railcar manufacturing in the North America freight market. Importantly, the analysis in this paper quantifies how the economic implications of such a shift would extend beyond railcar producers themselves, with wider, knock-on ramifications for US-based supply chain manufacturers as well.

The analysis in this report captures multiple scenarios of potential SOE disruption. The outcome of each scenario results in a loss of jobs and productivity to the US economy through the allocation of some or all of the supply-chain to the SOE's home country. However, the degree of loss varies depending on the course of action and US expansion taken by an SOE.

As many as 12,860 U.S. jobs are at risk for every $1 billion in market output that China's SOE takes from U.S. manufacturers. **Since freight railcar production in the US constitutes roughly a $5 billion market, the implication of a full loss of domestic freight car production would represent a loss of almost 65,000 jobs in the US.**

---

1 Cao, Bonnie. China Trainmaker CRRC Plans to Double its Overseas Sales. Bloomberg. September 11, 2015. Retrieved at https://www.bloomberg.com/news/articles/2015-09-10/china-trainmaker-crrc-plans-to-double-overseas-sales-in-5-years

The magnitude of impact will depend on the production and export approaches of any SOE entrants. If US freight railcar production collapsed and is completely off-shored, then the job loss effects would be most heavily felt in the following sectors:

- Manufacturing: up to 22,050 jobs
- Business Services: up to 10,020 jobs
- Trade, Transportation, and Utilities: up to 9,980 jobs
- Leisure and Hospitality: up to 5,420 jobs
- Financial Activities: up to 5,220 jobs

In terms of GDP, the impact could be as high as a $6.5 billion loss, which reflects the direct, indirect (supply chain), and induced (from spending out of employee wages) impacts of the $5 billion freight manufacturing industry. The industry sectors that can be expected to feel these effects most keenly include rail: car manufacturers, rail parts manufacturers, a range of iron & steel product manufacturers and companies involved in business services and financial activities, such as financing and leasing.

1. INTRODUCTION

THE IMPACT OF SOEs ON GLOBAL COMPETITION

Well-functioning capitalist markets thrive on fair and open competition to promote efficiency, reduce costs and improve innovation. In this context, traditional state-owned enterprises (SOEs) are regarded by many as anti-capitalist in Western countries because of their government-controlled operations, the benefits they may receive from state subsidies and the preferential treatment they are afforded.[2] State-owned enterprises are seen to stifle efficiencies and innovation in the market, suppress competition and incur losses for the public.[3] When governments play the triple role of regulator, regulation enforcer, and owner of business assets, the potential for favorable treatment of SOEs arises—whether through direct subsidies, concessionary financing, state-backed guarantees, and/or exemptions from antitrust enforcement or bankruptcy rules. These all affect fair and open competition.[4]

Nevertheless, SOEs, which are diverse in their corporate structures, comprise a large share of global production and economic activity. Moreover, in the domestic context, such organizations can create vital public value. For example, where markets fail to provide goods and services to the public, or where governments wish to allocate national resources and capital to promote economic development or improve the livelihoods of their citizens, SOEs can play a pivotal role. National governments may subsidize production locally to help ensure that domestic social goals and outcomes are achieved. In the US, public utility companies such as Tennessee Valley Authority, as well as rail operators such as Amtrak are examples of SOEs.

Even in a wholly domestic context, having a large part of output being either

2 Blanding, Michael. Not Your Father's State-Run Capitalism. Harvard Business School, Working Knowledge. 22 October, 2012.
3 Geddes, Richard R et. al. Competing with the Government: Anticompetitive Behavior and Public Enterprises. Hoover Institution Press Publication No. 523. Stanford University. 1994.
4 Buge, Max, et. al. State-owned enterprises in the global economy: Reason for concern? Center for Economic Policy Research. 02 May 2013. Accessed: 04/10/2017. http://voxeu.org/article/state-owned-enterprises-global-economy-reason-concern

wholly or partially state-owned can lead to inefficiencies.[5] From international perspective, however, the more pressing issue arises when SOEs seek to expand their activities outside of their home countries and seek to compete in the global marketplace. In an international trading landscape, unbalanced or unfair business practices from companies based abroad can undermine the performance of competitive, private-sector businesses at home. Domestic subsidies that are turned outward into the global market disrupt fair competition in target countries since SOEs may seek to undercut competitive prices by completing the bulk of production in the SOEs' home country. They may thereby take advantage of explicit and implicit government subsidies, and then export finished or near finished products to the target market. Such concerns are increasingly being raised in regards to the arrival of Chinese SOEs in US and other international markets.

THE ECONOMIC IMPACT FOR DOMESTIC MANUFACTURERS

The impact of SOEs on target market manufacturers is felt in terms of jobs and (taxable) economic activity throughout the manufacturers' supply chain. The channels of impact vary by industry sector; however, in general, domestic supply chains, which support the manufacture of final products, are particularly at risk of such moves. In addition to parts manufacturers, this includes domestic transportation and logistics services, as well as financial services. Rather than support the established supply chain in a new market, Chinese SOEs have been observed to rely on their pre-existing supply chain, joint venture or sub-contractor relationships—often located in China. A specific example of this is increasing vertical integration of the entire railcar, including cast bogie, forged wheel, and forged axle production. Therefore, several tiers of value-added production are controlled by very few SOEs.[6]

In some cases, measures have already been put in place to protect US domestic production. For example, under the Buy America Act (BAA) and other programs, certain government-funded investments or purchases must comply with specific minimum requirements for locally-produced inputs (e.g. concrete, steel/iron, labor, etc.). Understanding the potential impact on domestic markets as Chinese SOEs seek to widen their market share in the US and elsewhere will, however, require further investigation.

---

5 Yu, Fan. Chinese Bond Defaults Could Accelerate in 2017. Epoch Times. January 1, 2017. Accessed March 17, 2017. Source: http://www.theepochtimes.com/n3/2205130-chinese-bond-defaults-could-accelerate-in-2017/

6 China Railroad Rolling Stock Corp (CRRC). 24 April 2017. Products & Services – Castings & Forging. Retrieved: http://www.crrcgc.cc/g6653.aspx

PURPOSE AND STRUCTURE OF THE REPORT

In the context set out above, this paper conducts original research into the rail and rolling stock sector within the US and the changing landscape of domestic production—specifically, within freight rolling stock and with an emphasis on Chinese SOEs. The recent emergence and growth of SOEs in passenger rolling stock, as well as the establishment of a joint venture partnership in the US to produce freight rolling stock, provides a good foundation for analysis of potential disruption in the US freight railcar sector.[7,8]

The fundamental components of this analysis include:

- formulating reasonable assumptions regarding potential adjustments to domestic supply chains emanating from domestic freight railcar displacement by foreign SOEs;
- detailing the adjustments' effects on productivity within domestic supply chains;
- quantifying the effects on domestic jobs, output, and taxes; and
- contextualizing the disruptions across affected industry sectors.

The report contains five sections detailing assumptions, rationales, and modeling outcomes. Section 2 explores the evolution of SOEs in China, followed by an examination of the Australian experience of Chinese SOEs in the country's domestic freight rolling stock industry—found in Section 3. This section documents shifts in the Australian rail rolling stock supply chain and its increased reliance on imported components. This provided motivation for assumptions relating to potential impacts of similar shifts in the United States. Section 4 presents original modeling results of potential impacts on US jobs, GDP, labor income, and taxes associated with Chinese SOE entry into the freight railcar manufacturing sector as well as its ripple effects within the US economy through the use of an input-output model. Lastly, Section 5 summarizes the findings and provides concluding remarks.

---

7 We assume there is compatibility in the production between freight and passenger rolling stock, which could enable ease of entrance into the freight rolling stock sector with marginal capital investment.

8 Metzger, Andy. US urged to probe Chinese company building MBTA subway cars. Boston Globe. July 19, 2016 accessed at https://www.bostonglobe.com/metro/2016/07/19/urged-probe-chinese-company-building-mbta-subway-cars/wRTd80HIyx3oDxT1o2KheK/story.html

2. THE INTERNATIONAL EXPANSION OF CHINESE SOEs

Spurred by an overcapacity in the production of commodities and goods such as steel, the last several years have witnessed a push toward the increased globalization of Chinese SOEs. This has resulted in prices being driven down, and in increased disruption of certain goods-producing sectors elsewhere in the world. This in turn has raised concerns from businesses regarding their ability to effectively and fairly compete over the long-term.[9] These practices have drawn criticism from foreign manufacturers and policymakers as being anti-competitive and an example of dumping tactics, which are in violation of anti-dumping agreements such as the General Agreement on Tariffs and Trade (GATT).[10] A specific example is allegations of steel dumping into the North American market by Chinese producers. The US International Trade Commission specifically cites cold rolled steel flat products from China and Japan as injurious to U.S. industry, amongst dumping of other steel-related products.[11] Tariffs were enacted to discourage such behavior. However, the effects of the tariffs may not curb this behavior, as foreign SOEs will likely seek to circumvent the tariffs by: a) re-routing products illicitly through other countries (referred to as "country hopping");[12] b) moving up the value chain of produced products from inputs such as steel to products such as steel wheels;[13] and/or c) establishing

9 Kowalski, Przemyslaw, et. al. "State-owned enterprises: Trade effects and policy implications." OECD Trade Policy Papers No. 147. OECD. 2013.

10 Dumping is the act of charging a price for comparable goods in a foreign market that is less than the price for the same good in a domestic market—or selling a good at less than "normal value" on the same level of trade that would occur during the ordinary course of trade. Source: Van den Bossche, Peter (2005). "The Law and Policy of the World Trade Organization." Cambridge, UK: Cambridge University Press. p. 42. ISBN 978-0-511-12392-4

11 Williamson, Irving A (Chairman). Cold-Rolled Steel Flat Products from China and Japan. US ITC Investigation Nos. 701-TA-541 and 731-TA-1284. Publication 4619. July 2016.

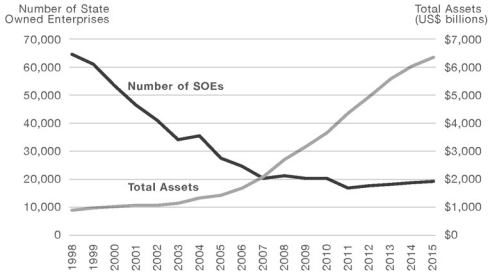
12 Liu, Xuepeng, et. al. "Anti-dumping Duty Circumvention through Trade Re-routing: Evidence from Chinese Exporters." Remin University of China. August 2016.

13 Anti-dumping tariffs generally apply to a specific country and product—though sometimes they may pertain to a specific company. By changing the product through value-added production, countries can circumvent the tariff.

final assembly facilities in the target market to mitigate fair trade protectionist measures.[14]

The number of SOEs in China has been declining since the late 1990s, through closure, privatization, and more recently, consolidation or reform toward less state ownership. This reduction in the number of SOEs has broadly not diminished the capacity for production. Instead, the reduction of SOEs combined with the expansion of total SOE assets has concentrated production activity into the hands of fewer SOEs. Fig. 1 displays the decreasing number of SOEs in China, relative to the increasing value of total assets of SOEs.

Fig. 1: Number of SOEs in China, 1998 to 2015



Source: National Bureau of Statistics, CEIC

An example specific to rolling stock manufacturing is the merger of two Chinese SOEs, CSR (China Southern Rwy Co) and CNR (China Northern Rwy Co), in 2015 to become CRRC. CRRC is now the largest rolling stock producer in the world and employs over 183,000.[15] Ironically, the two firms were initially one firm but were spun off in 2000 and 2002 by China's State-Owned Assets Supervision and Administrations Commissions (SASAC) with the goal of introducing competition into the market.[16]

---

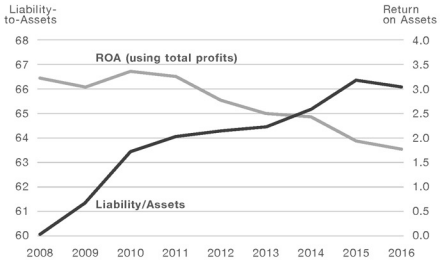
14 This method is evident in the rail rolling stock sector wherein SOEs have established final assembly plants for transit railcar production to meet local content requirements.

15 CRRC Corporation Limited. 2016 Annual Results Announcement. 29 March 2017. P. 48

16 Hong'e, Mo. "Regulator approves CNR, CSR merger deal." ECNS Wire. 29 April 2015. Accessed 04/20/2017: http://www.ecns.cn/cns-wire/2015/04-29/163624.shtml

Moreover, Chinese SOEs still ultimately comprise a significant share of the output and assets in the Chinese economy and more importantly, are increasing their international influence.[17] This is particularly significant in the context of their heightened financial riskiness. Fig. 2 shows that the liability to asset ratio for these SOEs crept up from 60 percent in 2008 to 66 percent in 2016. By comparison, the liability to asset ratio for private-owned enterprises has dropped to about 53 percent in 2016 from about 58 percent in 2007. This indicates that the majority of SOEs' assets are financed through implicitly government-supported debt (not equity), which increases the risk of default in the long-term. Simultaneously, the return on assets (a measure of profitability) has been decreasing, again leading to a higher risk of default. However, in the short-run, this structure enables SOEs to price their products at lower-than-competitive-market costs, absorb any losses and drive out competition—both domestically and abroad.

Fig. 2: Chinese SOE liability/assets and ROA, 2008 to 2016



Source: National Bureau of Statistics, CEIC

Additionally, the low profitability of Chinese SOEs places a further economic burden on the owning government. Compared to the average Chinese private industrial enterprise, whose profitability is around 10 percent return on assets, the low return on SOE assets—at about 1.8 percent—places implicit pressure

17 Xu, Gao. State-owned enterprises in China. How big are they? The World Bank. January 19, 2010. Accessed 4-7-2017. http://blogs.worldbank.org/eastasiapacific/state-owned-enterprises-in-china-how-big-are-they

on the government—as the owner of the state-owned enterprise as well as the agent of monetary policy—to lower interest rates in order to allow their SOEs to maintain their low-return investments.[18] A 2013 study by the Center for Strategic and International Studies found that Chinese SOEs obtained loans at rates as low as 1.6 percent from state banks, while private banks typically offered loans at 4.7 percent.[19] As Chinese SOEs turn outward into the international marketplace, their high levels of debt financing and low rates of returns add further credibility to claims of anti-competitive pricing behavior. This consequently adds further risk to competing privately owned enterprises in target countries—including the US.

Unfair competition from SOEs runs the risk that SOEs end up creating monopolies or near monopolies in foreign markets once they've squeezed out domestic competition. This squeezing out of competition ultimately results in one of two outcomes (or potentially both, in sequence). The first is that consumers are subjected to prices that are higher than competitive prices in the long run. The second is that a target country's displaced sectors face large capital start-up costs to revive the displaced sectors if the SOE folds.

The rail rolling stock sector has experienced the impact of Chinese SOEs first hand, both recently in the US, as well as over a longer period in other countries. The experience in Australia serves as a good case study of how domestic industries risks displacement due to SOE business practices and is explored in more detail in the following section.

18 Wildau, Gabriel. China deploys state enterprises to economic stimulus effort. Financial Times. June 21, 2016. Accessed 3-31-2017. https://www.ft.com/content/3d10e5cc-3754-11e6-a780-b48ed7b6126f

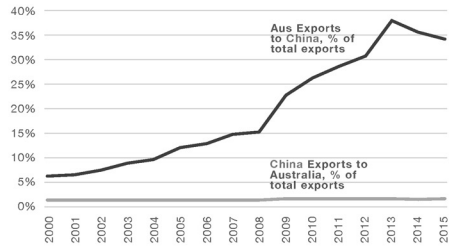
19 Aburaki, Kiyoaki. China's Competitiveness: Myth, Reality, and Lessons for the United States and Japan. Center for Strategic and International Studies. January 2013.

3. AUSTRALIA'S RAIL ROLLING STOCK EXPERIENCE

THE TRADING RELATIONSHIP BETWEEN CHINA AND AUSTRALIA

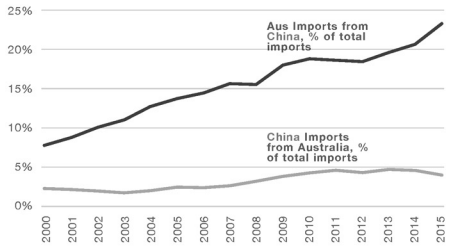
Australia's economy has long been dependent on its relationship with China. Over the past 15 years, however, this dependency has significantly deepened. Since 2000, Australia has increasingly relied on China to buy its goods. In 2000, just six percent of Australian exports went to China; by 2015 this increased to 34 percent (see Fig. 3). China's economic dependence on Australia is comparatively smaller. While China relies heavily on raw minerals, materials, and agriculture products from Australia, over the past 15 years, Chinese imports of Australian goods have grown only modestly, from 2 percent in 2000 to 4 percent in 2015 (see Fig. 4).

Fig. 3: Australia and China exports to each other, 2000 to 2015



Source: Oxford Economics

Fig. 4: Australia and China imports from each other, 2000 to 2015



Source: Oxford Economics

In terms of overall outcomes, both countries have benefitted from increased trade.[20] However, specific sectors in Australia appear to have suffered significantly in the wake of trade with China. This is explored further in the next section.

THE IMPACT OF CHINESE SOES ON THE AUSTRALIAN RAIL ROLLING STOCK SECTOR

In response to pressures from low-cost foreign competition, many domestic Australian manufacturers responded by offshoring key aspects of their production, consolidating businesses through mergers and acquisitions (M&A), or closing down altogether. The rail rolling stock sector is a prime example of this pattern.

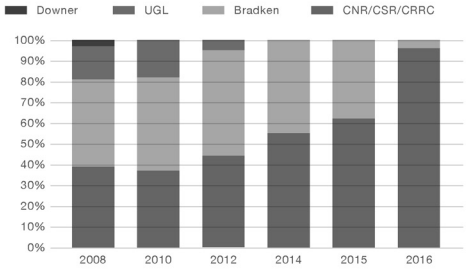
In 2010, Bradken, one of the largest domestic Australian producers of freight railcars, moved some of its manufacturing operations to China. The company cited its inability to compete with Chinese manufacturers as the reason for the move, ultimately opting to produce in China to more effectively compete.[21] By 2014 Bradken moved all of its freight railcar production to China.[22] A recent Australian press article reflects on the decline and demise of the Australian manufacturing sector, commenting that in "the rail industry, the crunch was

20 See, e.g., Myers, Joe. 5 Things to know about China and Australia's economic ties. World Economic Forum. April 11, 2016. Accessed: April 3, 2017 https://www.weforum.org/agenda/2016/04/5-things-to-know-about-china-and-australia-s-economic-ties/
21 Smail, Stephanie. "More Rail Manufacturing Could move to China." ABC Radio National. 9 August 2010.
22 Bradken Limited. Annual Report. 2014

even more sudden [than in the rest of the manufacturing sector]. As recently as 10 years ago [c. 2004], most rail vehicles were designed and made by Australian-owned companies. The rail operators began buying more wagons from China, and most of the hopper wagons used in the recent expansion of coal and iron ore mining were imported. Local production ceased."[23]

Fig. 5 illustrates the rapid decrease in Australia's freight railcar manufacturing, in the wake of Chinese SOE growth. In under 10 years, all Australian manufacturers have largely ceased production or have gone out of business. The remaining producer, Bradken, has largely exited the Australian market.

Fig. 5. Australia/Pacific's freight railcar delivery by manufacturer (units)



Source: SCI Verkehr[24]

Further explanation was given by two bodies—German Industry and Commerce (GIC) and German Chamber of Commerce, Hong Kong (GCC):[25]

> *China's SOEs are known for a state-supported market access strategy in the course of huge package deals that involves multiple industry sectors. In the case that a Chinese SOE like Sinopec is interested in the raw material deposits of say an African country, they would offer in exchange*

23 Szanto, Frank. "The End of Australian Manufacturing." ABC Radio National. 26 May 2014. Accessed 4/1/2017: http://www.abc.net.au/radionational/programs/ockhamsrazor/the-end-of-australian-manufacturing/5478190

24 Special data compilation by SCI Verkehr on behalf of Amsted Rail

25 German Industry and Commerce Ltd./GCC. China's Locomotive and Rolling Stock Industry. Issue III. 2014. Accessed 3/12/2017: http://china.ahk.de/fileadmin/ahk_china/pub_bilder/hk_GCcomm201406_full_web.pdf

> *for access to the resource a comprehensive package of favorable credit terms by a Chinese state-owned bank and infrastructure development carried out by Chinese construction SOEs (the so-called 'Angola mode').[26] Those construction enterprises usually buy their equipment from fellow Chinese companies, for example in March, CNR exported three locomotives to Ethiopia, which will be used in railway construction by a Chinese SOE. Furthermore, once such new rails are finished a demand for trains to operate on the rails will be created - with Chinese train makers having a competitive edge, due to their lower cost products and their existing local contacts…*
>
> *Nevertheless, Chinese train manufacturers do not solely deliver their trains to the usual suspect markets in developing countries. For instance CNR claims to have sold more than 12,000 freight wagons to Australia since 2000.*

The message of these comments is that the structuring of international trade and business development largely served to undermine fair competition for Australian domestic producers. The undermining of fair competition stems in part from subsidized financing from state-owned banks, as discussed in Section 2 above, wherein SOEs received loan rates as low as 1.6 percent, compared to privately owned enterprises receiving loans that averaged closer to 5 percent. This finding serves as a key assumption in the impact analysis in Section 4.

EXPLANATIONS FOR RAPID DECLINE OF AUSTRALIAN INDUSTRIAL MANUFACTURING

As Fig. 4 and Fig. 3 show in Section 3.1, trade between Australia and China increased during the global financial crisis, as Australia exported resources such as energy and mining products, while trade with other countries stagnated. This helped Australia to weather the global financial crisis.

After 2007, as the global economic downturn was starting to percolate through foreign economies, Chinese SOEs began to invest more extensively in many of Australia's industrial sectors—including the rail rolling stock sector. It has been estimated that Chinese SOEs accounted for approximately 80 percent by volume and 94 percent by transaction value of all Chinese investment into Australia between September 2006 and December 2012.[27]

---

26 Angola-mode: The Chinese strategy of swapping infrastructure projects for mineral resources. Predominantly in resource rich African countries.

27 KPMG and University of Sydney 2013, 'Demystifying Chinese Investment in Australia: Update March 2013', Report, University of Sydney China Studies Centre and KPMG, March 2014, pp 1, 15

Three specific factors at play in Australia have led to a reduction in domestic manufacturing and an increased reliance on manufactured imports from other countries such as China. First, as noted by the Parliament of Australia, the high value of the Australian dollar since 2002 reduced the country's long-term competitiveness in manufacturing.[28] Second, the China-Australia free trade agreement (ChAFTA) changed the market landscape for the manufacturing sector. As Australia sought to purchase cheaper imports, China, in turn, gained greater access to Australia's minerals, such as iron ore, and energy.[29] Third, along with the impact of the ChAFTA agreement, in 2006 Australia recognized China as a full market economy.[30] This designation effectively changed the trade relationship between the two countries (before the finalization of ChAFTA), through legal acknowledgment of fair business and trade practices within China—including state-owned enterprises. However, Australia still imposed import duties on certain types of Chinese steel to protect domestic steelmakers from surplus steel being exported from China—as evidenced from The Anti-Dumping Commission in 2016.[31] In other words, the Australian government found that China's trading behavior in Australia unfairly threatened Australia's manufacturing sector to such an extent that it was forced to step in on behalf of its domestic steel producers. This is counter to the market economy status Australia recognized in 2006.

With respect to the US market, the economic context is partially similar to the Australian experience, specifically with a high relative value of the US domestic currency to China's yuan and an expanding trade relationship with China. This situation has helped provide the framework for the baseline assumptions of Chinese SOE activities in the US described in Section 4.

For foreign enterprises from a number of countries (including state-owned ones), free trade agreements[32] have resulted in increased market access to Australian consumers. These foreign enterprises have benefitted from lower barriers to entry (e.g. lower tariffs and higher thresholds to trigger government oversight review of FDI), as well as increased capital investment in and ownership of Australian operations—most prominently in energy, mining and basic manufacturing. In the Chinese case, there have been a number of major

28 Priestley, Michael. Australia, China and the Global Financial Crisis. Parliament of Australia. Research Publications. 12 October, 2010

29 Ibid

30 Full market economy is a designated status that a country operates on market principles and does not compete unfairly in a global marketplace, such as receiving government subsidies to undercut competitor prices.

31 Westbrook, Tom and Hogue, Tom. Australia imposes dumping duties on Chinese steel. Reuters. April 23, 2016.

32 E.g., AANZFTA (ASEAN-Australia-New Zealand), ChAFTA (China-Australia).

new investment projects by Chinese enterprises, such as the Citic Pacific's Sino Iron mining operation.[33]

While the overall macroeconomic effects appear to have benefitted all trading partners involved, notable negative repercussions have emerged in specific sectors—especially in manufacturing.[34] Australian manufacturers have argued that, within ChAFTA, they were not afforded a level playing field and the same tariff reductions afforded to Chinese manufacturers.[35] Other Australian manufacturing-related industry groups expressed similar concerns at the onset of the free trade negotiations with China going as far back as 2005. For example, the Australian Manufacturing Workers' Union (AMWU) heavily questioned the fairness of the proposed trade deal, outlining risks including China's dumping of goods, lax labor standards, a growing deficit with China and the risk of offshoring of domestic Australian production to China, among many other concerns.[36]

A retrospective analysis of manufacturing output in Australia supports some of the concern articulated by the AMWU and other industry groups—especially as it pertains to iron and steel, a key input for rail rolling stock manufacturing and other significant industrial and consumer goods manufacturing. Fig. 6 shows the import and export share of iron and steel in Australia. Around approximately 2004, Australia moved from being a net exporter of iron and steel to China to a net importer of iron and steel from China. During this period, the value-added production of iron and steel in Australia dropped significantly—see Fig. 7. Consequently, Australia's output of crude steel dropped from about 7.1 million tons in 2000 to approximately 4.9 million tons in 2015—a 28 percent decline in output. Value-added production of iron and steel also experienced a near 94 percent decline between 2000 and 2016, dropping from $6.2 billion in 2000 to $400 million in 2016. This largely reflects increasing costs of inputs as well as decreasing prices in the high-surplus world steel market.

---

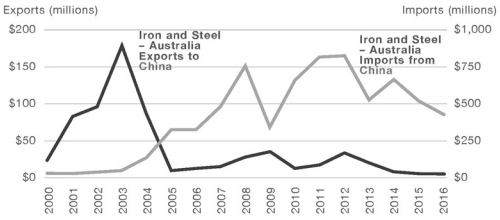
33 Sackur, Stephen. Australia leases out mineral-rich land as China's hunger for resources grows. The Guardian. 12 April 2011. Accessed 4/7/2017. https://www.theguardian.com/world/2011/apr/12/china-australia-mining-iron-coal (Note that since this investment, the iron ore project has amassed significant losses, leading to a multi-billion write down of Citic's asset, which is as risk of closure.)

34 Manufacturing experienced declines before the ChAFTA. However, value-added manufacturing production began declining significantly in 2007—during the global financial crisis, as well as just after Australia's recognition of China as a market economy.

35 See, e.g., Willox, Innes. "The Australian Industry Group letter to the Joint Standing Committee on Treaties." Submission 86. 17 June 2015. Accessed 4/7/2017. https://www.cfmeu.org.au/sites/cfmeuvic-7-x.com.au/files/uploads/Sub%2080%20-%20REVISED%20-%20CFMEU%20JSCOT%20ChAFTA%20-%2017%20August%202015%20(1).pdf

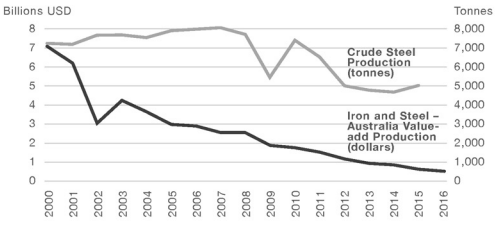
36 Australian Manufacturing Workers' Union. Submission to the Department of Foreign Affairs and Trade Concerning a Possible China-Australia Free Trade Agreement. June 2005

Fig. 6: Australia's iron and steel trade with China, 2000 to 2016



Source: Oxford Economics

Fig. 7: Australia's iron and steel production, 2000 to 2016



Source: Oxford Economics and World Steel Association

THE IMPACT ON THE RAILROAD ROLLING STOCK SUPPLY CHAIN

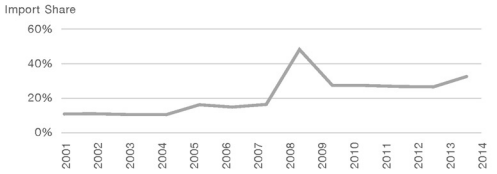
To help to explain the economic effect of the trade agreements on the manufacturing sector in Australia, Oxford Economics has undertaken an independent analysis of the flows of goods and services between Australia and the rest of the world. Specifically, we have evaluated inter-industry purchases within the rail rolling stock manufacturing sector, to better understand fundamental shifts in international supply chains.[37] The goal of this analysis is twofold:

37 In addition to freight car manufacturing, the railroad rolling stock industry includes engine manufacturing, passenger car manufacturing, certain industry-specific parts manufacturing, and repair and rebuilding services for existing rolling stock

- to describe the transition from domestic-produced supply chains and final goods to foreign produced supply-chains and final goods, and
- to use this analysis as a starting point to characterize how the US rail rolling stock sector might be affected by the entrance of foreign SOE competitors into the US market.

Australia has always historically imported some elements of rail rolling stock production from overseas. However, between 2007 and 2014, a noticeable shift in the type of imports occurred. Specifically, the use of foreign steel, and components made from iron and steel increased. This was coupled with an increase in the number of imported railcars. Between 2004-05 and 2013-14, the most recent year for which Australian macroeconomic (input-output) data are available, the imports of finished rolling stock jumped from 10 percent of Australia's rolling stock purchases to 33 percent.[38]

Fig. 8: Share of railroad rolling stock that is imported to Australia, 2001-2014



Source: Australian Bureau of Statsitics / Oxford Economics analysis

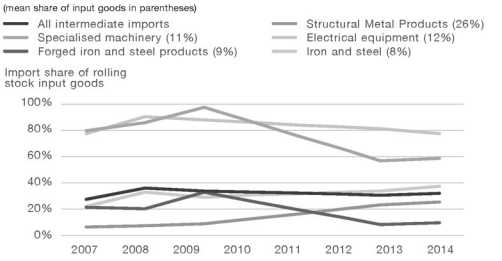
Explanations for this aggregate trend differ depending on whether the purchaser of particular final products is a private company or government agency. In the case of private companies, an increase in purchases of Chinese rolling stock presumably reflects its lower cost compared to domestically produced rolling stock. For government agencies, by contrast, there will often be some regard taken of domestic production.[39] Provisions might, for example, dictate the percentage of local content required in any final rolling stock product purchased by a public organization. In order to comply with these types of provisions, however, foreign producers use mechanisms such as working with different partners, suppliers and conglomerate partnerships to enable them to achieve local content goals.

38 See http://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/5209.0.55.001Main+Features12013-14.
39 Note: This is not always the case. Queensland does not generally have this provision for rail rolling stock, whereas New South Wales has a local content provision when public funds are used to purchase goods.

In the case of Australia, freight railcars (purchased by the private sector) were increasingly produced in China and other low-cost countries and shipped to Australia, resulting in the closure, or exit of local producers.[40] In the passenger rail market—where local content provisions were enacted (note: the purchasers were generally state/local government bodies), many of the components and overall structure for railcars are still produced in the SOE home country (usually China), but final assembly and maintenance/support are completed in Australia.

In addition to an increase in imports of final railroad rolling stock, there was also a shift in the use of imported intermediate inputs into domestic rolling stock production over this period. A look at Australian economic data reveals that although the overall import share of all intermediate inputs used in rolling stock production only increased from 24 percent in 2007-08 to 28 percent in 2013-14, this obscures increases in the imports of some goods, decreases in others, and changes in production patterns. For example, imports of structural metal product manufactured goods increased from 5 percent in 2007-08 to 23 percent by 2013-14. Similarly, imports of iron and steel manufacturing increased from 19 percent to 33 percent in the same time period (see Fig. 8).[41] Overall, this supply chain adjustment resulted in reduced demand for Australian-produced iron and steel inputs—especially in iron, steel, and other metal manufacturing, which tend to have higher job multipliers associated with production. Instead, production of iron and steel has increasingly shifted to China, resulting in lost jobs and GVA in the Australian economy.

Fig. 9: Import shares of top railroad rolling stock input goods, 2007-2014



Source: Oxford Economics

40 Szanto, Frank. The End of Australian Manufacturing. ABC Radio National. 26 May 2014. Accessed 4/1/2017: http://www.abc.net.au/radionational/programs/ockhamsrazor/the-end-of-australian-manufacturing/5478190

41 Oxford Economics data

4. THE IMPACT OF SOEs IN THE US FREIGHT ROLLING STOCK SECTOR

The Australian experience provides a platform from which to better understand the potential consequences of increased competition from foreign SOEs in the US economy. Similar adjustments in the supply chain structure could be expected, for example, in situations with comparable local content provision requirements—e.g. where government agencies are the purchasers and owners of rolling stock. However, notable differences between the Australian experience and the US experience merit discussion.

The case of Australia is not completely comparable to the US due to the unique nature of the economic relationship between Australia and China, e.g. the importance of natural resources trade. However, the strategy undertaken by SOEs in their interaction with the Australian market may help to predict how SOEs might seek to operate within the US. Especially comparable to the Australian experience and relevant to the context of this research is the high relative price of production in the US compared to China—caused in part by SOEs' access to low-cost financing and state subsidies—and the increasing trade relationship that the US has with China.

In the absence of key provisions regarding trade and production such as local content provisions (which are typically not applicable to freight railcar purchases), the Australian experience suggests SOEs will seek to minimize costs by leveraging low-cost production in their home country. The impact of these shifts can be modeled in the US economy. In order to quantify the supply-chain effects associated with these changes, we used an input-output model, specifically an impact modeling software produced by IMPLAN.[42] Using

42 IMPLAN is an economic impact software that uses Input-Output tables showing the relationships between industries to evaluate the full economic contribution of one industry throughout the economy. IMPLAN is an industry standard for assessing economic impacts.

this, we were able to calculate the economic impact of the freight rolling stock sector currently, and model the impact of changing trade structures—in GDP, jobs, labor income, and taxes (see box below for a discussion of economic impact analysis).

KEY ASSUMPTIONS AND LIMITATIONS OF THE IMPACT MODEL

Since this report focuses on freight railcars, we assume the following:

- purchasers of freight railcars are private companies or rail operators;
- absent local content provisions, SOEs will ship completed freight railcars for minimal assembly to private companies in the US;
- in the presence of local content provisions, SOEs will produce and ship the large majority of iron and steel inputs and complete final assembly in the US; and
- through state-supported subsidies, SOEs will consistently undercut US producers of freight rolling stock.

With these key assumptions in place, we evaluate two scenarios of potential disruptive effects to the US freight rail rolling stock sector. In one, fully finished, or nearly finished, railcars are shipped to the US by a foreign SOE. Thus in this scenario, we calculate the economic loss of $1 billion in US freight railcar output to a foreign SOE. This can be easily scaled to evaluate the collapse of the entire (roughly $5 billion) US freight railcar production sector. In the second scenario, we evaluate a situation in which final production is completed in the US, though an increased share of key iron and steel parts (as well as certain business services) are sourced from the SOE's home country.

MODELING INPUT ASSUMPTIONS

The railroad rolling stock industry in the United States, which includes freight, passenger, and locomotive manufacturing, as well as certain rail-specific parts manufacturing and repair activities, produced about $22 billion of output in 2015.[43] According to the Railway Supply Institute, the North American output specifically of railroad freight was about $9 billion in 2015, up from $7 billion in

43 Annual Survey of Manufactures.

AN INTRODUCTION TO ECONOMIC IMPACT ANALYSIS

A standard economic impact assessment identifies three channels of impact that stem from an activity:

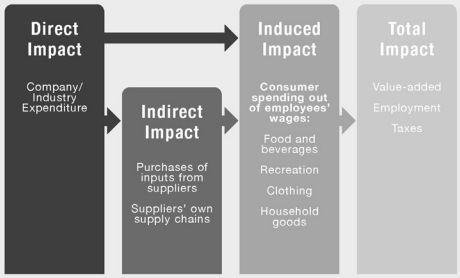
- **Direct effect**, which measures the economic benefit of industrial manufacturing operations and activities in the US.
- **Indirect effect**, which encapsulates the activity driven by the supply chain as a result of the procurement of goods and services from other businesses.
- **Induced effect**, which captures the impact of workers spending their wages on locally produced goods and services. This supports activity across the spectrum of consumer goods and services and their supply chains. An example of this is the purchases a worker makes using his wages, including groceries, clothing, transportation, and utilities.

In accordance with standard economic impact assessments, the scale of the impact of freight railcar manufacturers is measured using four key metrics:

- **GVA**—the gross value added (GVA) contribution to GDP.
- **Employment**—employment is measured in terms of headcount of workers.
- **Wages**—the compensation paid to workers within the industry, the industry's supply chain and induced wages paid to workers in consumer industries.
- **Taxes**—gross tax receipts paid at federal, state and local levels.

All monetary impacts in this report are presented in current 2015 (i.e. non-inflation adjusted) US$.

Fig. 9: The channels of economic impact



2014 and $6 billion in 2013 and 2012. Oxford Economics estimates US freight railcar output at roughly $5 billion per year on average.[44]

In order to produce this output, the freight rolling stock manufacturing industry incurs four broad categories of costs: compensation paid to labor, profits and other payments (e.g. interest) paid to capital, direct taxes paid to government (this does not include indirect taxes on wages, profits, or inputs), and intermediate inputs into the production of rolling stock. Fig. 11 presents three production patterns, which breaks out the cost of production among these four groups:

- real data on the railroad rolling stock industry as a whole;[45]
- assumptions for current US production of freight based on the railroad rolling stock industry as well as interviews with and surveys of freight manufacturers; and
- assumptions about hypothetical future Chinese production in the US.

The assumptions on current US production are based primarily on a survey of five major US freight railcar manufacturers. The Chinese assumptions are based on expert opinion and analysis of Australian rolling stock production.[46]

Fig. 11. Spending patterns for the railroad rolling stock industry, and assumptions for US freight rolling stock production and hypothetical Chinese production

	Rail Rolling stock industry	Current US freight production	Hypothetical future Chinese freight production in US
US capital income	3.3%	5.0%	0.0%
Labor income	10.8%	20.0%	10.0%
Direct taxes	0.6%	0.5%	0.5%
Intermediate inputs	85.3%	74.5%	84.5%

Source: IMPLAN, Oxford Economics based on industry survey

44 Based on the above statistics, expert opinion, survey responses, and published financial data from major producers. As demonstrated by the RSI figures, annual freight output is volatile, and orders frequently extend over multiple years of production.

45 These data are taken from IMPLAN economic impact software and are based on Bureau of Economic Analysis data.

46 US freight producers consistently reported spending more on labor than the rolling stock industry as a whole. Chinese production is expected to use less US-based labor, and instead to import more fully assembled inputs.

The intermediate inputs into production (i.e., the last row of Fig. 11) can be further divided into major categories of inputs as shown in Fig. 12. As before, assumptions are made about current US freight railcar production and hypothetical future Chinese production based on data on the broader industry, industry surveys, expert opinion, and the Australian experience.[47]

Fig. 12. Intermediate inputs for the railroad rolling stock industry and assumptions for US freight rolling stock production and hypothetical Chinese production

	Rail Rolling stock industry		Current US freight production		Hypothetical future Chinese freight production in US	
Inputs	Input share	% US	Input share	% US	Input share	% US
Metallic parts	34.5%	78%	40.0%	90%	35.0%	45%
Electrical parts	7.4%	55%	3.0%	80%	3.0%	40%
Other parts	5.4%	69%	3.0%	80%	3.0%	40%
Rolling stock	19.0%	94%	15.0%	100%	30.0%	30%
Business services	17.4%	97%	12.0%	100%	12.0%	75%
Utilities	1.6%	99%	1.5%	100%	1.5%	100%
Total	85.3%	83%	74.5%	93%	84.5%	45%

Source: IMPLAN, Oxford Economics based on industry survey

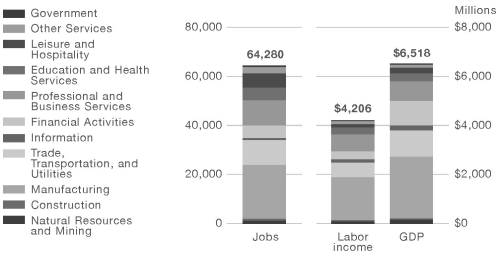
THE IMPORTANCE OF FREIGHT ROLLING STOCK PRODUCTION TO THE US ECONOMY

As shown in Fig. 13, we estimate the total economic impact of the current $5 billion freight railcar manufacturing industry in the US at approximately $6.5 billion and 64,280 jobs, with a total labor income of $4.2 billion. This impact generates $813 million in federal and $446 million in state and local taxes. If US

47 Surveys of major freight manufacturers generally showed a greater use of metallic versus other parts, lower use of business services, and a higher share of US-made products relative to the railroad rolling stock industry as a whole. Chinese production is assumed to use more imports, and to rely more heavily on railroad rolling stock as an input, i.e. on inputs that have already been processed to the point of being distinctly rail products rather than more general metallic and non-metallic intermediate goods. Note that the import share is only applicable to the goods themselves; US-based trade and transport margins are still included on imported goods.

freight railcar production were to cease, then we would expect the economic loss to the US to reflect these results.

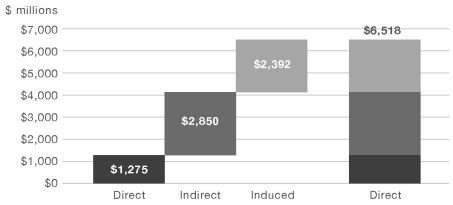
Fig. 13. Economic impact of US freight rolling stock manufacturing industry in 2016



Source: Oxford Economics, IMPLAN

This impact includes the direct impact of freight industry itself, the indirect impact of the industry's supply chain, and an induced impact that occurs as those employed in the industry and its supply chain spend their wages in the wider consumer economy. This breakout is shown in Fig. 14. Detailed results are presented in Appendix A.

Fig. 14. Direct, indirect, and induced GDP impact of US freight rolling stock manufacturing



Source: Oxford Economics, IMPLAN

THE IMPACT ON THE US ECONOMY FROM INCREASED CHINESE SOE FREIGHT RAILCAR PRODUCTION

This section considers the impact of China absorbing $1 billion of the US freight railcar produciton market, roughly one-fifth of current production. Because the model is linear, the effect of shifting all $5 billion of production overseas would increase the impacts by five times. The time frame of the scenario is unspecified, but all results are presented in 2015$.

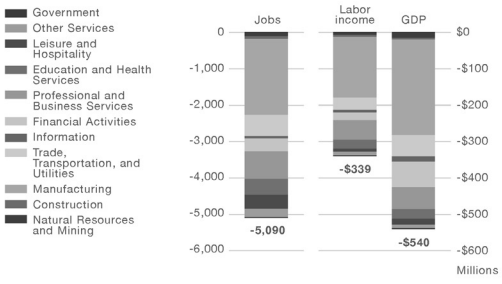
Two scenarios are considered below:

- In scenario 1, Chinese-owned SOEs assemble freight rolling stock in the United States, but with more of the value-add being done in China than is currently the case. Specifically, the production pattern is as described in Fig. 10 and Fig. 12 above.
- In scenario 2, fully Chinese-made freight rolling stock is imported into the US, displacing $1 billion worth of the existing freight railcar industry.

SCENARIO 1: Increased freight railcar imports from China but final assembly in the US

The modeling shows that a $1 billion shift from current US production to increased percentage of key supply-chain inputs that are imported from China (or elsewhere) would be associated with a reduction of 5,090 US jobs and $540

Fig. 15. Impacts of a $1 billion shift to Chinese SOE freight railcar final assembly in the US



Source: Oxford Economics, IMPLAN

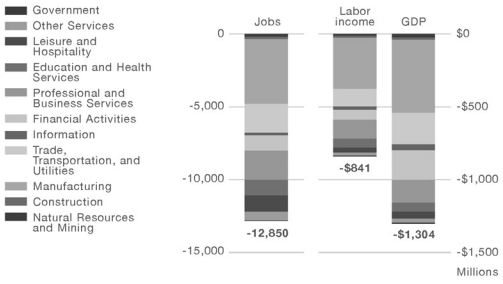
million of US GDP.[48] Some of the production and final assembly of the rolling stock would still be maintained in the US, while other portions of the supply-chain would be offshored.

SCENARIO 2: Imported Chinese-made freight railcars

In the event that US production is replaced by imports of finished, or nearly finished Chinese freight car products, rather than retaining the final assembly stage in the US, the economic impact of these Chinese imports on the US economy would be effectively nil. Therefore, the freight railcar economic impact presented in Fig. 13 above would be reduced proportionally. That is, the results presented here for the loss to the US economy are exactly one-fifth the results shown in Section 4.3 above, and reflect the full loss of $1 billion of freight railcar production.[49]

These values are shown in Fig. 16 below. This includes a loss of 12,850 jobs and $1.3 billion in US GDP.

Fig. 16. Impacts of $1 billion shift to Chinese imported freight railcars



Source: Oxford Economics, IMPLAN

48 Note: given the right macroeconomic conditions, these workers could be absorbed into other areas of the labor market, though skills training may be required.

49 Production in China may rely on a small amount of US exports to China; those impacts are believed to be small and are not modeled.

IMPACT TO THE US SUPPLY CHAIN

The loss of freight manufacturing may impact key supply chain industries by reducing scale economies in those industries and therefore hurt other downstream users of these same products. Understanding the key inter-industry relationships between industry sectors is, ultimately, critical in understanding the potential ramifications of significant disruption and loss in key purchasers of manufactured inputs—even those who do not produce freight railcars yet require some of the same inputs as freight railcar producers.

Fig. 17 presents the top five supply chain goods used in the production of railroad rolling stock, along with the top other industries using these products. Freight's share of the output of these goods serves as a measure of the extent to which the loss of the freight market might hurt that industry. For example, at 3.8 percent, freight railcar producers consume a significant share of the US plate manufacturing production, and the loss of this market has the potential to significantly harm the domestic US plate manufacturing industry. This could raise the price of domestic plates, which would hurt industries that rely heavily on this industry, such as the printing machinery and equipment manufacturing industry, whose use of plates is equal to 11.1 percent of industry output.

Fig. 17. Top intermediate input goods and other industries relying on same

Top freight intermediate input goods	Freight purchases ($ millions)	Input's share of freight output	Freight's share of domestic production	Top using industries	Input's share of industry output
Plates	$375	7.5%	3.8%	Printing machinery and equipment manufacturing	11.1%
				Machine shops	4.6%
				Motor vehicle gasoline engine manufacturing	4.2%
Spring and wire products	$97	1.9%	1.1%	Mattress manufacturing	9.6%
				Rolled steel shape manufacturing	4.5%
				Beef cattle ranching and farming	2.1%
Ferrous metals	$228	4.6%	1.0%	Motor vehicle steering, suspension, and brake mfg.	6.2%
				Motor vehicle transmission and power train parts mfg.	5.9%
				Turbine and turbine generator set units manufacturing	5.4%
Iron and steel forgings	$49	1.0%	0.5%	Speed changer, industrial high-speed drive, and gear mfg.	4.1%
				Mechanical power transmission equipment mfg.	2.4%
				Motor and generator manufacturing	2.4%
Balls and roller bearings	$62	1.2%	0.6%	Tire manufacturing	7.6%
				Cut and sew apparel contractors	2.6%
				Apparel accessories and other apparel manufacturing	1.9%

Source: IMPLAN and Oxford Economics

5. CONCLUSION

State-owned enterprises clearly have an important role to play in a country's national economy. However, as SOEs reach outwards in search of growth opportunities in foreign markets, domestic producers in those markets face significant risks. The findings of this study suggest that much of the impact to the US freight rolling stock production sector will depend on how an SOE conducts business. If an SOE opts to build manufacturing facilities in the US and source the majority of input materials through US supply chains, then the overall downside economic effects on the US will be moderate.[50] If, however, an SOE opts to produce freight railcars in their home country—through state-owned supply chains—and then ship whole or nearly completed railcars to the US, then the impact to the US economy will be more significant across manufacturing and service sectors.

The Australian experience with China's rail rolling stock manufacturing SOEs suggests that the second of these is the more likely outcome, and serves as a cautionary tale for US manufacturing as a whole, as well as freight railcar production in particular. However, even a more "middle ground" approach by foreign SOEs (i.e., the first outcome above) would still threaten US jobs and productivity. For example, an SOE's construction of final assembly facilities in the US, while providing US-based jobs in assembly, would still risk US jobs elsewhere in the existing US railroad rolling stock supply chain. This would occur because key elements of product design, development and parts assembly would likely take place in China, before the resulting parts were shipped to the US for final assembly. Local content provisions in contracts with mass transit/commuter rail authorities are in the realm of 60 percent, meaning 40 percent of the value of the railcar can be satisfied through non-US production. In the case of freight rail production, such provisions are generally non-pertinent as most purchasers are private companies not relying on government funding.

50 Note: the SOE may nevertheless receive preferential finance options from state-owned banks, which may still enable them to undercut competition. This could force a consolidation within the freight car manufacturing market, which may result in increased prices as competition is diminished. Therefore, careful monitoring of fair competitive business practices would still be warranted.

96

The results and descriptions provided in this analysis are designed to offer key perspectives on potential outcomes and risks to freight railcar manufacturers and other domestic industries resulting from unfair trade practices by SOEs. This analysis is intended to provide contextual understanding of the broader issues and challenges associated with SOEs, international trade, and potential effects on the US economy. Different assumptions regarding SOE behavior, or the sources of key supply chain inputs would lead to different results.

APPENDIX A: DETAILED TABLES

IMPACT OF US FREIGHT MANUFACTURING

Fig. 18. GDP impact ($ million) of US freight manufacturing industry

Sector	Direct	Indirect	Induced	Total
Natural Resources and Mining	$0	$94	$53	$148
Construction	$0	$31	$24	$55
Manufacturing	$1,275	$1,020	$205	$2,501
Trade, Transportation, and Utilities	$0	$631	$447	$1,077
Information	$0	$94	$118	$212
Financial Activities	$0	$322	$679	$1,001
Professional and Business Services	$0	$542	$250	$792
Education and Health Services	$0	$0	$333	$333
Leisure and Hospitality	$0	$61	$156	$217
Other Services	$0	$38	$103	$141
Government	$0	$19	$23	$42
Total	$1,275	$2,850	$2,392	$6,518

Source: Oxford Economics, IMPLAN

Fig. 19. Jobs impact of US freight manufacturing industry

Sector	Direct	Indirect	Induced	Total
Natural Resources and Mining	0	460	630	1,090
Construction	0	420	330	740
Manufacturing	11,700	9,060	1,290	22,050
Trade, Transportation, and Utilities	0	4,530	5,450	9,980
Information	0	440	460	890
Financial Activities	0	2,020	3,200	5,220
Professional and Business Services	0	6,660	3,360	10,020
Education and Health Services	0	10	5,460	5,470
Leisure and Hospitality	0	1,520	3,900	5,420
Other Services	0	490	2,510	2,990
Government	0	170	220	390
Total	11,700	25,760	26,810	64,280

Source: Oxford Economics, IMPLAN

Fig. 20. Labor income ($ million) impact of US freight manufacturing industry

Sector	Direct	Indirect	Induced	Total
Natural Resources and Mining	$0	$43	$36	$79
Construction	$0	$24	$19	$42
Manufacturing	$1,000	$661	$94	$1,755
Trade, Transportation, and Utilities	$0	$354	$261	$615
Information	$0	$52	$52	$104
Financial Activities	$0	$153	$184	$337
Professional and Business Services	$0	$467	$205	$673
Education and Health Services	$0	$0	$306	$306
Leisure and Hospitality	$0	$38	$100	$139
Other Services	$0	$28	$94	$122
Government	$0	$15	$19	$34
Total	$1,000	$1,837	$1,369	$4,206

Source: Oxford Economics, IMPLAN

IMPACT OF SCENARIO 1—US FINAL ASSEMBLY

Fig. 21. GDP ($ million) impact of $ 1 billion shift to Chinese production in the US

Sector	Direct	Indirect	Induced	Total
Natural Resources and Mining	$0	-$10	-$4	-$14
Construction	$0	-$2	-$2	-$3
Manufacturing	-$150	-$97	-$17	-$263
Trade, Transportation, and Utilities	$0	-$23	-$36	-$59
Information	$0	-$5	-$10	-$14
Financial Activities	$0	-$15	-$55	-$70
Professional and Business Services	$0	-$41	-$20	-$61
Education and Health Services	$0	$0	-$27	-$27
Leisure and Hospitality	$0	-$3	-$13	-$15
Other Services	$0	-$2	-$8	-$10
Government	$0	-$1	-$2	-$3
Total	-$150	-$197	-$193	-$540

Source: Oxford Economics, IMPLAN

Fig. 22. Jobs impact of $ 1 billion shift to Chinese production in the US

Sector	Direct	Indirect	Induced	Total
Natural Resources and Mining	0	-40	-50	-90
Construction	0	-20	-30	-50
Manufacturing	-1,170	-830	-100	-2,100
Trade, Transportation, and Utilities	0	-160	-440	-600
Information	0	-20	-40	-60
Financial Activities	0	-90	-260	-350
Professional and Business Services	0	-500	-270	-770
Education and Health Services	0	0	-440	-440
Leisure and Hospitality	0	-70	-310	-380
Other Services	0	-30	-200	-230
Government	0	-10	-20	-20
Total	-1,170	-1,770	-2,160	-5,100

Source: Oxford Economics, IMPLAN

Fig. 23. Labor income ($ million) impact of $1 billion shift to Chinese production in the US

Sector	Direct	Indirect	Induced	Total
Natural Resources and Mining	$0	-$4	-$3	-$7
Construction	$0	-$1	-$2	-$3
Manufacturing	-$100	-$61	-$8	-$168
Trade, Transportation, and Utilities	$0	-$12	-$21	-$34
Information	$0	-$3	-$4	-$7
Financial Activities	$0	-$7	-$15	-$22
Professional and Business Services	$0	-$37	-$17	-$53
Education and Health Services	$0	$0	-$25	-$25
Leisure and Hospitality	$0	-$2	-$8	-$10
Other Services	$0	-$2	-$8	-$9
Government	$0	-$1	-$2	-$2
Total	-$100	-$129	-$111	-$339

Source: Oxford Economics, IMPLAN

IMPACT OF SCENARIO 2—FULL IMPORT

Fig. 24. GDP ($ million) impact of $ 1 billion shift to Chinese imports

Sector	Direct	Indirect	Induced	Total
Natural Resources and Mining	$0	-$19	-$11	-$30
Construction	$0	-$6	-$5	-$11
Manufacturing	-$255	-$204	-$41	-$500
Trade, Transportation, and Utilities	$0	-$126	-$89	-$215
Information	$0	-$19	-$24	-$42
Financial Activities	$0	-$64	-$136	-$200
Professional and Business Services	$0	-$108	-$50	-$158
Education and Health Services	$0	$0	-$67	-$67
Leisure and Hospitality	$0	-$12	-$31	-$43
Other Services	$0	-$8	-$21	-$28
Government	$0	-$4	-$5	-$8
Total	-$255	-$570	-$478	-$1,304

Source: Oxford Economics, IMPLAN

Fig. 25. Jobs impact of $ 1 billion shift to Chinese imports

Sector	Direct	Indirect	Induced	Total
Natural Resources and Mining	0	-90	-130	-220
Construction	0	-80	-70	-150
Manufacturing	-2,340	-1,810	-260	-4,410
Trade, Transportation, and Utilities	0	-910	-1,090	-2,000
Information	0	-90	-90	-180
Financial Activities	0	-400	-640	-1,040
Professional and Business Services	0	-1,330	-670	-2,000
Education and Health Services	0	0	-1,090	-1,090
Leisure and Hospitality	0	-300	-780	-1,080
Other Services	0	-100	-500	-600
Government	0	-30	-40	-80
Total	-2,340	-5,150	-5,360	-12,860

Source: Oxford Economics, IMPLAN

Fig. 26. Labor income ($ million) impact of $1 billion shift to imports

Sector	Direct	Indirect	Induced	Total
Natural Resources and Mining	$0	-$9	-$7	-$16
Construction	$0	-$5	-$4	-$8
Manufacturing	-$200	-$132	-$19	-$351
Trade, Transportation, and Utilities	$0	-$71	-$52	-$123
Information	$0	-$10	-$10	-$21
Financial Activities	$0	-$31	-$37	-$67
Professional and Business Services	$0	-$93	-$41	-$135
Education and Health Services	$0	$0	-$61	-$61
Leisure and Hospitality	$0	-$8	-$20	-$28
Other Services	$0	-$6	-$19	-$24
Government	$0	-$3	-$4	-$7
Total	-$200	-$367	-$274	-$841

Source: Oxford Economics, IMPLAN

NATIONAL SECURITY VULNERABILITIES OF THE U.S. FREIGHT RAIL INFRASTRUCTURE AND MANUFACTURING SECTOR—THREATS AND MITIGATION

Brigadier General John Adams, U.S. Army (Retired)—October 22, 2018

Our country depends upon the privately owned and operated North American freight railroad system to provide safe, reliable, and effective transportation for our Nation's industries, our defense industrial base and to ensure the security of our homeland. Our nation's future depends upon the reliability and security of freight rail as the primary mode of transportation not only for every imaginable type of industrial cargo, but also for military equipment, fuels, chemicals, and hazardous waste. 140,000 miles of main-line U.S. freight rail infrastructure connect ports to rural and urban inland hubs, tie military bases to key logistical nodes throughout the nation, and link the U.S. to key allies and trading partners.

In short, U.S. freight rail is crucial to our Nation's global economic competitiveness and a strategic asset that our armed forces depend upon to maintain readiness and preserve our defense capacity.

Yet, while we have recognized certain threats to the security of our freight rail system, we have begun to allow foreign interests to make incursions into the rail industry in ways that could threaten our national interests for decades to come. The Government of China has made it a priority to target the U.S. freight rail system, building inroads into freight rail supply chains and taking aim at rolling stock asset ownership. Beijing's "Made in China 2025" plan aims for comparative advantage in the global advanced rail sector, along with nine other industrial sectors. Now is the time for our Nation to push back on China's strategy to overtake U.S. freight rail, because a failure to do so means tremendous security risk at home. As a retired Brigadier General and 30-year veteran of the U.S. Army, I know that Chinese dominance of U.S. rail would turn the system from a bedrock industrial and strategic asset into a potentially crippling vulnerability.

In the pages that follow, I review the many reasons that we should be concerned about the advancing efforts by the Government of China to take control of U.S. freight rail; reflect on the state of those efforts thus far; and make specific recommendations for policy action that should be taken to keep our rail, and our nation, safe.

OHN ADAMS,
Brigadier General,
U.S. Army (Retired),
President,
Guardian Six Consulting LLC.

Executive Summary

The privately owned and operated U.S. freight rail system is the most sophisticated, productive, and capital-intensive in the world. Freight rail is vital to our economy, our commercial transportation system, and our homeland security infrastructure. Today, on more than 140,000 miles of track, freight rail carries 40 percent of all American intercity freight and 13 percent of the Nation's goods.

The sustainability of this extensive and sophisticated network is now under threat as the Government of China seeks to make inroads into increasingly large and vital portions of the freight rail manufacturing sector and its supply chain. Unlike other transportation sectors, freight rail products do not have Buy America protections. Therefore, Chinese state-owned enterprises (SOEs) could undercut U.S. suppliers. If we allow Chinese SOEs to continue their efforts to target and undermine U.S. freight rail interests, we risk not only tens of thousands of U.S. jobs, but also larger potential damage to the industrial base, our critical infrastructure, and the security of this Nation.

The threat of Chinese dominance of our freight rail sector is more than just a market concern. The national security implications of U.S. industry and military interests being forced to rely on Chinese government-manufactured railcars are jarringly self-evident: Chinese penetration of the rail system's cyber-structure would provide early and reliable warning of U.S. military mobilization and logistical preparations for conflict. Were the Chinese to gain access to advanced U.S. freight car technology (notably specific rolling stock asset health, waybill commodity information on loaded freight cars, or precise GPS train location) the potential exists for the generation of a false negative (or positive) sensor activation—something particularly worrisome given that freight rail carries most nuclear waste and hazardous material that we transport in this Nation. A false sensor reading (*e.g.,* tank car outlet dome cover is secure) could lead to a false level of confidence that tank car serv-

ice valves are secure. If service valves are disturbed and undetected a release of toxic chemicals could result in catastrophic consequences to life and the environment. Moreover, Chinese intelligence about U.S. rail freight logistical movements could provide China with a destabilizing economic competitive edge. Chinese access to or control of U.S. freight rail would also mean that risk of other actors'—including terrorists'—malicious intrusion would become more difficult for U.S operators to detect or counter.

We depend on technology, machinery, and a robust system of intellectual property protections to support our national security; when we allow foreign states to interfere—especially our strategic competitors—we risk that security. While Congress has recognized and taken steps to address similar threats to products such as computer chips and cellular technology, policymakers may not fully understand China's ongoing incursion into an increasingly digitized rail network. Indeed, there are few places where this risk is more acute than with the U.S. freight rail system, and few actors who threaten the security of the freight rail system more than the Chinese government.

Yet in recent years, we have witnessed an unabated and aggressive entry into the U.S. rail market by China's national rail company, China Railway Rolling Stock Corporation (CRRC). This show of force, intended to serve the long-term strategic and technological aims of the Chinese government, as well as that nation's desire to ensure a massive external market for the oversupply of its railcars, components, and raw materials, threatens the survival of U.S. freight rail manufacturing. This, in turn, raises one of the most serious security risks we have faced in the postwar era.

CRRC's history of using underhanded tactics to overtake rail manufacturing in other countries is well known. Over a span of just nine years, CRRC decimated the Australian freight manufacturing marketplace. Now, without immediate action, the U.S. freight rail manufacturing risks a similar fate. If this pattern continues in the U.S., Chinese state-directed efforts will eventually force U.S. companies out of business, endangering as many as 65,000 U.S. manufacturing jobs [1] and putting our national security at risk.

Chinese intrusion into the U.S. rail system's supply chain threatens the health and sustainability of this vital economic pillar, especially in a national emergency. Were China to gain inroads into those operations, management, and supply chains, the ability of U.S. to effectively utilize and leverage the freight rail network in a crisis could be crippled. Moreover, the extensive telematics and digitization of the American rail network, while integrating the most modern technology, also exposes the system and those who use it to a wide array of cyber risks. While there is no single solution that will mitigate these concerns, we must modernize our national policies to reflect these security risks. Three key reforms are needed from Congress and the administration:

1) Develop comprehensive restrictions and additional reviews on investments from foreign state-backed entities in critical infrastructure integral to our national defense.

2) Ensure that appropriate federal agencies, in coordination with states and localities, develop robust standards for cyber and data integrity applicable to any rail or transit sector contracts involving foreign state-backed entities.

3) Strengthen oversight of Buy America laws to ensure that existing laws and regulations are adhered to in federally-funded transit and rail procurements including railcar manufacturing and explore new avenues to further protect the manufacturing capabilities of freight rail and other core domestic industries that are integral to support and maintain our defense industrial base.

I. The Impact and Importance of Rail in America

The U.S. freight rail network, in comparison with freight moved by water, pipeline, truck, and air, accounts for approximately 40 percent of U.S. freight moved by ton-miles and 16 percent of freight moved as measured by tons.[2] In 2014, the operations and capital expense of the major U.S. freight railroads supported approximately 1.5 million jobs (1.1 percent of all U.S. workers), nearly $274 billion in U.S. economic output (1.6 percent of the total), and $88 billion in wages (1.3 percent of the total).[3] The thoroughly integrated rail systems of the United States, Canada and Mexico are a cornerstone of the North American market as well as the foundation

for the safe, reliable, and efficient transportation of goods from rural communities to urban areas to seaports and government and military installations.

Railroads not only serve as the primary mode of transport for an array of key products and commodities, but they also regularly transport U.S. military equipment, hazardous waste, potentially toxic and hazard commodities (*i.e.,* chlorine, anhydrous ammonia, ethylene oxide) and flammable liquids (*i.e.,* petroleum products, ethanol). The North American railcar fleet includes more than 1.6 million cars. With seven Class I railroads,[4] 21 regional railroads, and 525 local railroads,[5] more than 140,000 miles of active railroad, more than 1.65 million freight cars in North America, and 39,521 locomotives, an estimated 12,000 trains operate daily.[6]

The U.S freight rail industry moves more freight than any other rail system worldwide. These figures include the $6.5 billion U.S. freight rail manufacturing sector which directly supports 65,000 jobs.[7] The rail industry provides numerous public benefits including reductions in road congestion, highway fatalities, fuel consumption, logistics costs, and public infrastructure maintenance costs. As private organizations responsible to their shareholders, U.S. freight railroads depend upon profits for reinvestment and capital improvement. The average U.S. manufacturer spends about 3 percent of revenue on capital expense. The comparable figure for freight railroads is nearly 19 percent, more than 6 times higher than other industries.[8] The majority of this goes to maintenance and repair, and up to 20 percent gets reinvested to enhance capacity.[9]

Most commercial freight (*i.e.,* container freight) ships intermodally. Rail's ability to transfer cargo intermodally—train transport of goods before or after transfers from other modes of traffic (aircraft, vessels, or trucks)—is vital to the economic viability of U.S. ports and urban hubs, and for the past four decades, constitutes the fastest growing segment of the freight rail industry.[10] Though the viability of American ports also depends upon the ability to deliver to and receive inland cargo by all transportation modes, freight rail connectivity at ports is increasingly and uniquely important to attract containerized cargo when the origin-destination pairs are more than 500 miles apart.[11] Indeed, U.S. railroads moved over 1 million intermodal loads in July 2018, a 5.5 percent increase over July 2017.

U.S. military vehicles are transported by freight rail near Greenville, SC in July 2018.

Half of all freight traffic is interchanged. This means that, except for captive unit train movements on a single railroad from origin to destination, using only that railroad's own cars (*i.e.,* coal or grain hoppers), most of the cars in any given freight train will be owned by someone other than the handling carrier. Approximately 70 percent of all freight cars in North America are owned by non-railroad entities (*e.g.,* private car owners, leasing companies, banks, shippers, and utilities). Interchanged traffic is vital to smooth international commerce for Canada, Mexico, and the United States.

The U.S. freight rail system is also one of the most technologically advanced in the world, with a rapidly expanding scope of digitization, thoroughly incorporating the network into the Internet of Things (IoT). Onboard freight telematics incorporate a vast network of wireless sensors that monitor asset health and location, sending the information to communication management units as well as to displays in locomotive cabs. U.S. railroads depend upon the continual upgrade and development of advanced technology to reduce risks, improve safety, and improve the network's efficiency. As Federal Railroad Administration (FRA) Administrator Ronald Batory stated at his swearing in on February 28, 2018: "We must aggressively embrace the Internet of Things and artificial intelligence, along with seeking autonomous functions that can foster an environment towards minimal to non-existent risk." [12]

II. China's Government Aims to Dominate U.S. Rail

Rail manufacturing is one of the 10 industries included in the Chinese government's "Made in China 2025" initiative,[13] a plan targeting global dominance in sectors that the Government of China considers most strategic to its global aims. As the White House Office of Trade and Manufacturing Policy noted in a recent report, "[T]he Chinese government has institutionalized the industrial policy of inducing investment in 'encouraged' high technology sectors using the financial resources and regulatory instruments of the State." [14] Toward these ends, China's government has brought to bear a range of state subsidies, state financing, and other resources to support the market entry and market ascension objectives of its wholly government-owned, $33 billion conglomerate, China Railway and Rolling Stock Corporation (CRRC), an enterprise that—with more than 183,000 workers—is now the largest rolling stock producer in the world.[15] While it is owned by the Chinese government, CRRC is *controlled* by the Communist Party of China, and it has set about to build a foothold in the U.S. market, with a near-term goal of overtaking our rail sector.

Indeed, CRRC's own bylaws state that the company will seek guidance from the Communist Party of China on significant matters affecting the company's operations.[16] Three of CRRC's current board members previously held high-level positions at state-owned defense companies, Aviation Industry Corporation of China (AVIC), which produces fighter and bomber aircraft, helicopters, and unmanned aerial vehicles for the Chinese Army, and China Shipbuilding Industry Corporation (CSIC), which produces submarines, warships, and other naval equipment for the Chinese Navy. Furthermore, two former CRRC board members held positions at AVIC and China North Industries Group Corporation Limited (NORINCO), a state-owned defense company that supplies tanks, aircraft, missiles, firearms, and related products for the Chinese military.

The latter two of these entities, CSIC and NORINCO, have been subject to allegations of espionage and sanctions evasion by the U.S. government, raising serious questions about the connections of CRRC board members to these activities. In 2007, AVIC was reputed to have stolen data on the F–35 fighter jet from Lockheed Martin and used it to build the Chinese J–31 fighter.[17] Similarly, CSIC was indicted in 2016 by the U.S. Department of Justice for entering into contracts with another Chinese company for the purchase of industrial materials that were created using stolen trade secrets from an American firm.[18] NORINCO has also been sanctioned by the U.S. State Department on six occasions for contributing to Iranian nuclear weapons development.[19] Two of CRRC's board members were respectively employed in high-level positions at CSIC and NORINCO at the time these offenses occurred, suggesting that they were likely aware of, if not complicit in, this illicit activity.

These actions are a compelling example of how the Communist Party places pressure on SOEs to fulfill directives such as Made in China 2025. To advance these plans, CRRC has first set its sights on the U.S. municipal transit sector, seeking to get major new contracts to sell transit cars to transit agencies in Boston, Chicago, New York, Los Angeles and Philadelphia, among others. The Chinese government is banking on the fact that once CRRC secures sufficient U.S. municipal transit contracts, it can pivot quickly and inexpensively toward the more strategically important freight rail sector. There, China can unload much of its current freight car manufacturing capacity oversupply—offsetting its own, slowing domestic market while continuing its strategy of using exports to sustain the Nation's employment base.

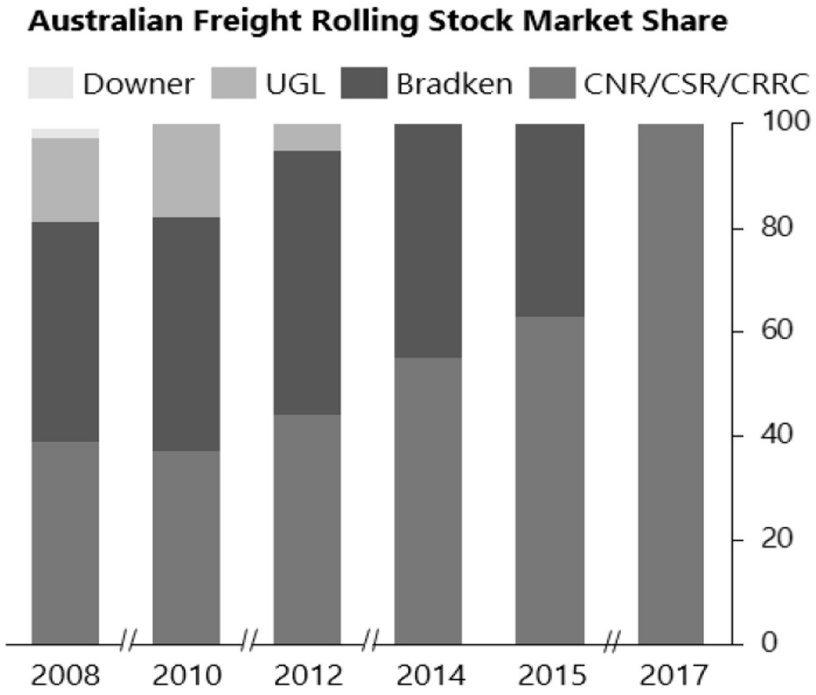
Given China's manufacturing capacity oversupply and long-term goals for global dominance, CRRC hardly needs to profit on short-term sales. As such, the Government of China is able to sweeten CRRC's bids for new U.S. transit car contracts; not only by subsidizing CRRC's operating costs but also, in many instances, providing below-market financing terms to municipal buyers, making CRRC's prices enticingly low compared to other bids. In fact, CRRC's own 2016 annual report shows

that it has leveraged China's state-owned banks to the tune of almost $27 billion to finance its expansion plans.[20] CRRC has used those resources to make its bids for major U.S. project opportunities more attractive, underbidding other competitors by as much as 50 percent, and—since 2015—winning $2.6 billion in transit rail contracts to supply "Made in China" railcars for the Boston, Los Angeles, Philadelphia, and Chicago metro systems, among others.[21] Soon, CRRC will have the chance to apply the same tactics to metro transit rail contracts in Atlanta, Washington, D.C., New Jersey and New York City.

With these massive successes under its belt, CRRC has built two U.S. transit assembly plants in Springfield, Massachusetts and Chicago. These are not where railcar manufacturing occurs, since China has little interest in shifting its manufacturing to the United States. Instead, these facilities are where Chinese components and subcomponents are shipped and assembled into cars that are then sold to U.S. buyers. Most of the transit cars must have more than 65 percent of their content sourced from American components if transit authorities want to qualify for Federal funding. In the case of the Boston transit contract, however, CRRC met the desire of Massachusetts for an in-state assembly facility and bid the lowest price by more than $150 million under the next competitor.[22] With no Federal funding supporting this procurement by the state transit authority MBTA, CRRC avoided all otherwise applicable Federal Transit Administration "Buy America" requirements. In November of last year, CRRC shipped the first fully-built, shrink-wrapped transit rail cars that had been made completely in China into the Port of Boston.

And while U.S. transit rail is typically subject to such domestic content requirements, no similar requirements apply to freight railcar manufacturing. This means that CRRC can effectively import complete or nearly complete freight rail cars to the United States or complete minor assembly at CRRC U.S. facilities at an even lower discount than transit cars have received. Having already established major operations in the U.S., CRRC's current assembly facilities in the United States can easily be modified to accommodate freight assembly as well, which are in fact a downgrade for facilities to produce compared to transit.

CRRC's entry into the freight rail manufacturing poses a direct threat to a major strategic and economic asset of the United States. Indeed, a 2017 Oxford Economics study found Chinese competition in freight rail threatens U.S. economic competitiveness.[23] That same study projected that up to 65,000 U.S. jobs could be eliminated if we allow China to displace U.S. freight rail manufacturing, a sector that has many U.S.-headquartered players today, as well as a long U.S. supply chain since the industry is a major consumer of U.S.-made steel. Even so, signs of Chinese targeting of North American freight rail are already evident, with CRRC having recently opened freight car assembly facilities in Wilmington, North Carolina and Moncton, New Brunswick.[24,25]



Source: Oxford Economics

If the prospect of losing domestic freight rail capabilities seems far-fetched, we need only remind ourselves of recent CRRC activities in Australia to understand how far China is willing to go to dominate in rail. Within a decade after entering Australia's once-thriving domestic rail manufacturing industry, CRRC used underpricing and other anti-competitive tactics as described above to wipe out Australia's domestic rail manufacturing base entirely.[26] Today, Australia's railcar manufacturing is wholly controlled by CRRC. As a clear reminder of China's intentions of continuing—this trend, CRRC itself Tweeted recently about its plans for market dominance, announcing, "So far, 83 percent of all rail products in the world are operated by #CRRC or are CRRC ones. How long will it take for us conquering the remaining 17 percent?"[27]

The European Union and Israel recognize this threat and are exploring and enacting policies to better protect their domestic rail manufacturing and production sectors.[28] [29] As of this writing, even though freight rail is considered by the Department of Homeland Security to be a key element of our Nation's critical infrastructure, similar U.S. measures have not been enacted at the Federal level to directly protect American freight rail manufacturing from the Government of China and its designs for global dominance.

III. China's Rail Agenda Threatens U.S. Cybersecurity

"The possibility of causing mayhem remotely could make train hacking an attractive priority for terrorists."[30]

In 2010, the world witnessed the first case of weaponized malware when the nuclear industry fell prey to Stuxnet, prompting the possibility of attacks on industrial controls in cyber-systems. The possibility has since become far more real as we have witnessed growing numbers of cyberattacks that threaten and at times undermine key segments of the world's economies, power, financial systems, and other assets.

Predatory Chinese efforts to penetrate our freight rail market create the potential for disruption to the most advanced technologies upon which our rail system depends for safety and efficiency. Commercial railroads are, of course, aware of the risks they face from potential cyber-security incursions and are investing in cybersecurity capabilities. Even so, we significantly increase the risk of Chinese

cyber-espionage or even cyber-terrorism by allowing CRRC to displace U.S. rail interests and shift our freight rail supply reliance to the Government of China. If allowed to penetrate the U.S. freight rail system, Chinese government-backed entities could simply vacuum data from individuals and firms connected to the rail network. China's history of cyberattacks on U.S. interests, combined with the Chinese Government's known efforts to use facial recognition and artificial intelligence for tracking its own citizens through "a vast and unprecedented national surveillance system" make this security risk all the more acute.[31]

In other U.S. economic sectors where Chinese SOEs have engaged aggressively, the U.S. Government has responded with targeted restrictions to mitigate clear security risks. Such measures have included a reported U.S. government ban on contracting with the Chinese computer firm Lenovo,[32] a ban on the purchase of Chinese drones,[33] and the removal of Chinese-made security cameras from U.S. military bases.[34] In April 2018, DoD banned Huawei and ZTE cell phones from sale in U.S. military exchanges world-wide.[35] We have yet to do the same to protect Chinese incursions into the U.S. freight rail manufacturing base.

According to the National Institute of Standards and Technology, the following are cyber-threats to industrial control systems, all of which must be taken into account when we consider control of U.S. freight rail assets:

- *Blocked or delayed flow of information through ICS networks, which could disrupt ICS operation.*
- *Unauthorized changes to instructions, commands, or alarm thresholds, which could damage, disable, or shut down equipment, create environmental impacts, and/or endanger human life.*
- *Inaccurate information sent to system operators, either to disguise unauthorized changes, or to cause the operators to initiate inappropriate actions, which could have various negative effects.*
- *ICS software or configuration settings modified, or ICS software infected with malware, which could have various negative effects.*
- *Interference with the operation of equipment protection systems, which could endanger costly and difficult-to-replace equipment.*
- *Interference with the operation of safety systems, which could endanger human life.*[36]

Furthermore, as freight trains become increasingly sophisticated, incorporating more technology and systems integration, these types of cyber-security concerns become more palpable. In U.S. freight rail, industrial controls have replaced the mainframes and protocols that have historically undergirded the industry, and these controls present vulnerabilities not only relative to the freight rail systems themselves, but also through outside data connections that could threaten both public safety and operating continuity.[37] Significant technology and rapidly expanding IoT capabilities in the U.S. freight rail network create potential security challenges that include:

- *A digitized railroad network/the Internet of Things:* Like other high-tech industries, the freight railroad industry has embraced digitization and the IoT. Integrated teams of data scientists, software developers, and engineers develop and apply technology across every aspect of the nationwide freight rail network. Indeed, such technology has generated significant improvements in operational safety and network efficiency. These benefits also have increased the vulnerability of onboard systems, individual train operations, and perhaps even the industry's metadata warehousing centers to cyber threats.
- *Rail Signaling:* In California in 2008, a Metrolink passenger train collided with a Union Pacific train, causing 25 fatalities and 135 passenger injuries. Congress responded mandating the installation of positive train control (PTC) systems on much of the Nation's rail system including the Class I network by 2015. The statutory deadline was later extended by Congress to December 31, 2018, subject to certain alternative schedule criteria. PTC is designed to prevent four specific accident scenarios: train-to-train collisions, over-speed derailments, unauthorized train incursions into right-of-way work zones, and misaligned track switches. A malicious cyber breach of PTC or underlying existing rail signaling systems could wreak havoc and cause accidents on the highly interdependent freight railway network.
- *Locomotives:* Latest generation diesel locomotives have hundreds of sensors which generate thousands of asset health and performance indicators per minute.

- *Onboard Freight Car Location & Asset Health Monitoring:* There are 25,000 freight cars equipped with telematics or remote monitoring equipment. Over 85 percent of the installations are on tank cars and the vast majority of those are materials: chlorine, anhydrous ammonia, ethylene oxide, and flammable liquids. Thetracking technology includes a wireless communication management unit to track precise near-real time lat-long location via GPS, direction of travel, speed, and dwell time within the 45 Transportation Security Administration (TSA) designated high-threat urban areas (HTUAs)[1] and thousands of chemical shipper/consignee defined geo-fences. Wireless sensor nodes measure and/or alert:
- loaded or empty car condition
- accelerations and peak impacts in yards & on line-of-road roller bearing temperature
- lading temperature in tank cars
- tank car hatch covers open (based upon degree of tilt)
- handbrake on or off (unattended train securement issue)
- *End-of-Train Telemetry (EOT):* The FRA requires all freight trains operating on excess of 30 mph to be equipped with a 2-way EOT device. EOTs include a flashing blue light indicating the last car in a train as well as the rear brake pipe pressure which is transmitted to the lead locomotive in the train. EOTs also include GPS location. The 2-way feature means that the locomotive engineer can initiate an emergency brake application from the rear of the train as well as the front. This is critical safety technology (a pool of 12,000 devices on the Class I railroads) since Class I railroads are stretching some trains from 10,000–12,000 feet long as opposed to a typical 5,000–6,000-foot train.

A. Industrial Cybersecurity Considerations

"Chinese industrial espionage is not new . . . but it is practiced more openly these days," writes former Navy Secretary J. William Middendorf and the State Department's Dan Negrea.[38]"

Every company shipping goods on U.S. freight rail—which transports nearly 13 percent of products across our country, for industries ranging from agriculture to chemicals to mining—should be concerned by the prospect of China controlling key aspects of the U.S. freight rail system. In 2016, U.S. railroads originated over 1.5 trillion tons of freight in 27 million carloads. 40 percent of all intercity freight goes by rail, including 67 percent of the coal used by electric utilities for power generation.[39] Similarly, the chemicals we use to keep our water supply pure and much of the food products we consume are shipped by private freight rail. Therefore, ensuring that these products arrive at their destinations and are free from tampering is of paramount concern.

The Transportation Security Administration, in the Preamble to its November 26, 2008 Rail Transportation Security Final Rule, noted that "Due to the open infrastructure of the rail transportation system, freight trains can be particularly vulnerable to attack" and "[f]reight trains, transporting hazardous materials are of even more concern, because an attack on those trains. . .could result in the release of hazardous materials" and that "the release of PIH materials in a densely populated urban area would have catastrophic consequences." Rail also carries some of the most hazardous materials (HAZMAT) between industries and military installations in America, often through densely populated areas and cities. Typically railroads move 1.7–1.8 million carloads of HAZMAT every year—items that are essential to our economy and our society—and about 105,000 carloads are so-called "poisonous by inhalation hazard" (TIH) materials such as chlorine or anhydrous ammonia. Freight rail is also a principal mode of transport for nuclear waste. Indeed, the majority of TIH materials in this country are transported via rail, which underscores the paramount emphasis on freight rail safety, free from tampering and malicious intrusion. The safety consequences of any HAZMAT incident, especially those involving the most dangerous worst commodities (*e.g.,* poisonous by inhalation hazard) are substantial: In January 2005, for example, a rail tank car ruptured in Graniteville, SC as the result of a derailment, releasing chlorine that forced the evacuation of 5,400 people within a mile radius of the site. Ultimately 9 people died, and 75 others required treatment for chlorine exposure.[40]

---

[1] The Transportation Security Administration defines an HTUA as an area comprising one or more cities and the surrounding areas, including a 10-mile buffer zone.

B. Transportation Operations Cybersecurity Considerations

Given the crucial role of rail in our economy and our defense industrial base, U.S. Presidential Policy Directive 21 classifies freight rail as part of our Nation's critical infrastructure.[41] And yet, no Federal law specifically restricts foreign government ownership of our freight rail supply sector. At the same time, many of the same critical infrastructure features designed to boost the quality of and operation of our freight rail system also raise serious vulnerability concerns in the hands of a foreign government.

Policymakers should recall that the ubiquitous freight rail network traverses nearly every major city in the nation, particularly the 45 TSA designated continental HTUAs. Many rail yards and storage locations are close to densely populated areas, which at any time could contain large numbers of loaded HAZMAT tank cars.[42] Additionally, freight and passenger rail are highly interdependent; they use many of the same bridges, tunnels, control centers, tracks, signals, and switches. Amtrak—the principal U.S. provider of inter-city passenger rail—operates on more than 22,000 miles of track owned by freight railroads, and many commuter and light rail systems also operate on freight rail tracks.[43] A freight rail or railyard incident could be triggered to cause tremendous direct and collateral damage on large population centers as well as vital transportation networks.

Finally, railroads have information-based operating systems that also pose vulnerabilities. The Railway Alert Network (RAN), for instance, distributes intelligence between and among the Federal Rail Administration, commercial railroads and U.S. law enforcement; RAN, which is now operated by the American Association of Railroads (AAR), allows for analysis and dissemination of threat communications from DOT and DHS to AAR's members.[44] Tapping into the RAN system would give an unfriendly outside government access to secure information, including network data analytics and traffic analysis, that should not be shared. The AAR developed its AskRail mobile app in 2014. First responders are able to instantaneously access the specific hazardous materials commodity in a tank car as well as the hazards posed. AskRail employs GIS mapping to identify vulnerable areas like hospitals and schools and rivers. Obviously, unauthorized access to AskRail by those with malicious intent poses a security threat.

C. Military Cybersecurity Considerations

The Department of Defense (DoD) has a longstanding reliance on freight rail in the United States. Most of the military's heavy and tracked vehicles are transported by freight rail meaning that freight rail runs through every military base in the United States.[45] DoD's Military Traffic Management Command (MTMC) has designated nearly 39,000 miles of freight rail track as being uniquely important to our Nation's defense, and thus part of the Strategic Rail Corridor Network, or "STRACNET." STRACNET serves 193 U.S. defense installations, connecting military bases with maritime ports of embarkation and other key points across the country.[46]

Freight rail is also at the heart of the U.S. Transportation Command (TRANSCOM), DoD's global defense transportation system, coordinating people and transportation assets around the world. The Surface Deployment and Distribution Command (SDDC), which is a component of TRANSCOM, operates 10,000 containers and some 1,350 rail cars of its own to deliver equipment and supplies for deployed members of the Army, Navy, Air Force, Marines, and Coast Guard. SDCC also, of course, leverages commercial freight rail to provide important components of DoD's surface transportation requirements.[47] SDCC also utilizes a special heavy-duty flatcar fleet of 1,850 specially designed heavy-duty flatcars managed by a company owned by the major freight railroads.

Because of the deep reliance of our military on U.S. commercial rail, MTMC monitors and evaluates data on railroad industry construction, industry mergers, bankruptcies and other similar events to determine how they may affect DoD's mobility and readiness capabilities. We can assume that MTMC is aware of the ongoing efforts by China's Government to dominate the U.S. rail sector. We must act on this concern to stop CRRC's activities to assert itself in the U.S. marketplace.

IV. Policy Action is Needed

America's domestic freight rail manufacturing base has always played a vital role in the economic and national security of the United States. As this report demonstrates, freight rail is the lifeblood of the American economy—employing tens of thousands of workers, shipping millions of tons of consumer goods and materials through every major artery in the country and adding over $6.5 billion in GDP. Simultaneously, freight rail is an indispensable part of our Nation's defense infrastructure, a vital transportation system that supplies and connects U.S. military in-

stallations across the continent. Despite our longstanding reliance on freight rail, America remains unprepared to protect itself from foreign entities with ambitions directly at odds with our own. Even current cooperative efforts between industry and the Department of Homeland Security—while commendable—remain inadequate. The good news is that there is still time to address this threat. Federal and state policymakers have an opportunity to adopt meaningful laws and regulations that can significantly slow the Chinese government's intrusion into the U.S. freight manufacturing space and, in turn, bolster America's security in the face of ever-changing global threats. The goal of this report is to encourage America's political leaders to strongly consider any and all of the following recommendations.

1) Develop comprehensive restrictions and reviews on investments from foreign state-backed entities in critical infrastructure integral to our national defense.

The recent reforms to the Committee on Foreign Investment in the United States (CFIUS) through the broadly supported Foreign Investment Risk Review Modernization Act (FIRRMA) were a welcomed step forward for U.S. policy and come at a pivotal moment. Nevertheless, CFIUS continues to face shortcomings. Greenfield investments—wherein a foreign entity creates entirely new investments, rather than through an acquisition, merger, or joint venture—are still not explicitly covered under CFIUS's scope of authority. This means that CRRC and other Chinese SOEs can continue to build new facilities in the U.S. without oversight. To date, only five transactions have ever been blocked by CFIUS,[48] suggesting that we should explore alternative tools to ensure the integrity of the rail manufacturing sector and its associated supply base.

One such tool that has been proposed has been to create a parallel committee to CFIUS under the authority of the Department of Commerce to review transactions for the effects they would have on economic security. With a broader mandate that would allow the Committee to take economic considerations into effect, we could address many of the restrictions that have plagued CFIUS. Another more attainable option is for Congress to take steps to ensure that Federal funds are not used to further the aims of SOEs like CRRC. Three of the four manufacturing contracts that CRRC won in the U.S. were awarded using Federal Transit Administration (FTA) dollars, meaning that the U.S. government effectively subsidized a Chinese state-owned enterprise to further the Made in China 2025 initiative at the expense of American workers and security.

2) Ensure that appropriate Federal agencies, in coordination with states and localities, develop robust standards for cyber and data integrity applicable to any rail or transit sector contracts involving foreign state-backed entities.

As technology continues to advance, so must our standards for cybersecurity. If foreign SOEs are permitted to produce any aspect of the thousands of detector and monitoring systems onboard trains around the country, we will face a continued national security threat capable of halting our entire rail network. These technologies present countless opportunities for hacking and surveillance, and with the cybersecurity risks of other Chinese entities having been well-documented in numerous other industries, action is urgently needed. The Department of Homeland Security and the Department of Transportation should coordinate with state and local agencies to develop and implement standards that ensure cyber and data security for our rail system in any interface with a foreign SOE. These agencies should also engage with private industry to determine what other appropriate measures to address the cybersecurity concerns posed by foreign SOEs and, if appropriate, establish a task force of key stakeholders involved in the manufacturing, operations, and oversight of the freight rail sector. Under new and existing authority, officials must take robust steps to ensure the cyber integrity from any SOE threat of all rail network systems and data streams.

3) Strengthen oversight of Buy America laws to ensure that existing laws and regulations are adhered to in federally funded transit and rail procurements including railcar manufacturing and explore new avenues to further ensure the manufacturing capabilities of freight rail and other core domestic industries that are integral to support and maintain our defense industrial base.

CRRC's pattern of investment in other markets like Australia suggest that China will use the transit railcar manufacturing sector as a beachhead to then move into freight railcar manufacturing, implicating even more pressing national security concerns. In the transit railcar manufacturing sector, Buy America laws offer the most comprehensive protections for the industry that, when followed, can help mitigate the financial and strategic advantages that the Government of China offers state-owned companies like CRRC. However, various loopholes and lax enforcement has

limited the effectiveness of these laws, allowing CRRC to advance into the transit railcar manufacturing sector unabated.

In April 2017, President Trump signed an executive order to strengthen Buy America laws, requiring Federal agencies to develop policies to maximize the use of domestic workers and materials in procurements as well as to recommend new policies to strengthen the implementation of Buy American laws.[49] Nevertheless, little has been done since then to strengthen Buy America. Buy America laws have proven to be a vital protection for the U.S. manufacturing and industrial base, ensuring the employment of thousands of American workers while strengthening our ability to respond to foreign threats in the process. These laws, however, can be easily manipulated as Federal agencies often lack the resources to effectively police them, relying all too heavily on the claims of manufacturers and suppliers. When those manufacturers are foreign state-owned enterprises, we have little incentive to take them at their word. Congress and the administration should explore avenues to strengthen domestic content provisions and ensure that existing laws are being followed to protect American workers and security.

V. Conclusion

The Government of China's attack on our rail system is insidious and ingenious. China enters at the local level, subsidizes the assembly of Chinese transit rail cars, and supplies them to cash-strapped transit systems at bargain prices. In the process, Chinese companies bring small numbers of assembly jobs to the U.S. while the manufacturing, technology, and R&D stay in China. Today and for the foreseeable future, no American company makes transit rail cars, but the evidence is compelling that the Chinese government has now directed state-owned entities to target the U.S. freight rail manufacturing sector as well. Our freight railcar industry is now in China's sights.

As our Nation's freight railcar manufacturers continue to incorporate innovative new technologies to enhance the safety and productivity of our rail system, the growing presence of China's CRRC is all the more concerning. From rural communities to major cities to seaports and government installations, freight rail not only serves as the primary mode of transport for an array of key products and commodities, but also for sensitive U.S. military equipment, hazardous nuclear waste, and toxic chemicals. We must take urgent measures to ensure freight rail remains secure and American-run. We must retain the know-how and technology to improve our rail system in the future, and safeguard against disruption of this strategically vital sector of our economy and pillar of our national security.

Endnotes

[1] Oxford Economics, "Will We Derail U.S. Freight Rolling Stock Production," May 2017. *https://www.oxfordeconomics.com/recent-releases/will-we-derail-us-freight-rolling-stock-production*

[2] Federal Railroad Administration, "National Rail Plan Progress Report", September 2010. Cited in *https://www.fra.dot.gov/page/P0362*

[3] Towson University, Regional Economic Studies Institute, June 2016 (quoted in AAR President Ed Hamberger's April 11, 2018 Statement to the House Appropriations Committee THUD Subcommittee hearing on Rail Safety, and Infrastructure).

[4] Federal Register, "Indexing the Annual Operating Revenues of Railroads," Cited in *https://www.fra.dot.gov/page/P0362*

[5] Federal Railroad Administration, 'Freight Rail Background," March 2012. Cited in *https://www.fra.dot.gov/page/P0362*

[6] Department of Homeland Security, "Transportation Systems Sector." *https://www.dhs.gov/transportation-systems-sector*

[7] Oxford Economics, "Will We Derail U.S. Freight Rolling Stock Production," May 2017. *https://www.oxfordeconomics.com/recent-releases/will-we-derail-us-freight-rolling-stock-production*

[8] Towson University, Regional Economic Studies Institute, June 2016 (quoted in AAR President Ed Hamberger's April 11, 2018 Statement to the House Appropriations Committee THUD Subcommittee hearing on Rail Safety, and Infrastructure).

[9] Federal Railroad Administration, "National Rail Plan Progress Report," September 2010. Cited in *https://www.fra.dot.gov/page/P0362*

[10] Federal Railroad Administration, "Freight Rail Overview," *https://www.fra.dot.gov/page/P0362*

[11] Louisiana Department of Transportation & Development, "A Comparative Analysis of Intermodal Ship-to-Rail Connections at Louisiana Deep Water Ports." August 2007. *http://www.sp.dotd.la.gov/Inside_LaDOTD/Divisions/Multimodal/Marine_Rail/Misc%20Documents/A%20Comparative%20Analysis%20of%20Intermodal%20Ship%20to%20Rail%20Connections%20at%20Louisiana%20Deep%20Water%20Ports.pdf*

[12] As Prepared Remarks of Ronald L. Batory Swearing-In Ceremony as the 14th Administrator of the Federal Railroad Administration, U.S. Department of Transportation Headquarters, Washington, DC, February 28, 2018. *https://www.fra.dot.gov/Elib/Document/17848*

[13] The Made in China 2025 plan identifies ten priority sectors: next-generation information technology; high-end numerical control machinery and robotics; aerospace and aviation equip-

ment; maritime engineering equipment and high-tech maritime vessel manufacturing; advanced rail equipment; energy-saving and new energy vehicles; electrical equipment; new materials; biomedicine; and agricultural machinery.

[14] White House Office of Trade and Manufacturing Policy, "How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World," June 2018. *https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf*

[15] CRRC 2016 Annual Report, April 2017. *http://www.hkexnews.hk/listedco/listconews/SEHK/2017/0427/LTN201704272466.pdf*

[16] "CRRC Corporation Limited Articles of Association," CRRC Corporation Limited, at 70. *http://www.crrcgc.cc/Portals/73/Uploads/Files/2018/6-4/636637164457871915.pdf*

[17] "America's most expensive weapons system, the F–35, is a key symbol of Trump's trade gripe with China," CNBC, March 22, 2018 *https://www.cnbc. com/2018/03/22/americas-most-expensive-weapons-system-the-f-35-is-a-key-symbol-of-trumps-trade-gripe-with-china.html*

[18] "Chinese Nationals Stole Marine Technology to Benefit Chinese Regime, According to U.S. Justice Department," Epoch Times, April 30, 2018. *https://www. theepochtimes.com/chinese-nationals-stole-marine-technology-to-benefit-chinese-regime-according-to-u-s-justice-department_2509135.html*

[19] "United States Imposes Sanctions Against Chinese Firm," Nuclear Threat Initiative, September 22, 2004. *https://www.nti.org/gsn/article/united-states-imposes-sanctions-against-chinese-firm/*

[20] "CRRC 2016 Annual Report," CRRC Corporation Limited, April 28, 2017 *http://www.crrcgc.cc/Portals/73/Uploads/Files/2017/4–28/636289739063167304.pdf*

[21] Focusing initially with transit freight contracts allowed CRRC the opportunity to work with local governments and small businesses, leveraging CRRC's economies of scale at a much lower level than were CRRC to initially tackle the larger-scale, higher visibility, more stringent review process associated with freight rail contracts.

[22] "China-based T supplier keeps rolling," CommonWealth, March 24, 2017. *https://commonwealthmagazine.org/politics/china-based-t-supplier-keeps-rolling/*

[23] Oxford Economics, "Will We Derail U.S. Freight Rolling Stock Production," May 2017. *https://www.oxfordeconomics.com/recent-releases/will-we-derail-us-freight-rolling-stock-production*

[24] William Vantuono, "New tank car builder coming on line," Railway Age, February 13, 2014. *https://www.railwayage.com/financeleasing/new-tank-car-builder-coming-on-line/*

[25] "CRRC to build North American wagon plant in Canada," Railway Gazette, May 5, 2017. *http://www.railwaygazette.com/news/news/n-america/single-view/view/crrc-to-build-north-american-wagon-plant-in-canada.html*

[26] Letter from Rail Security Alliance to U.S. Trade Representative, December 14, 2017.

[27] @CRRC_global, "Following CRRC's entry to Jamaica, our products are now offered to 104 countries and regions. So far, 83 percent of all rail products in the world are operated by #CRRC or are CRRC ones. How long will it take for us conquering the remaining 17 percent?" Twitter, January 11, 2018. *https://twitter.com/CRRC_global/status/951476296860819456*

[28] Yosi Melman, "Cause for Concern? Chinese Investment and Israel's National Security," The Jerusalem Post, April 7, 2018. *https://www.jpost.com/Jerusalem-Report/Chinese-TAKEAWAY-546692*

[29] Hermine Donceel and Eric Maurice, "EU Parliament approves new anti-dumping methodology," EU Observer, November 15, 2017. *https://euobserver.com/economic/139866*

[30] David Morris, "Railroad Association Denies Smart Train Cyber Vulnerabilities," Fortune, January 22, 2016. *http://fortune.com/2016/01/22/railroad-association-denies-smart-train-cyber-vulnerabilities/*

[31] Paul Mozur, "Inside China's Dystopian Dreams: A.I., Shame and Lots of Cameras," The New York Times, July 8, 2018. *https://www.nytimes.com/2018/07/08/business/china-surveillance-technology.html*

[32] Sophie Curtis, "Spy agencies 'ban Lenovo from secret networks," The Telegraph, July 29, 2013. *https://www.telegraph.co.uk/technology/news/10208578/Spy-agencies-ban-Lenovo-from-secret-networks.html*

[33] Alwyn Scott, "China drone maker steps up security after U.S. Army ban," Reuters, August 14, 2017. *https://www.reuters.com/article/us-usa-drones-dji/china-drone-maker-steps-up-security-after-u-s-army-ban-idUSKCN1AU294*

[34] Max Greenwood, "US Army base removes Chinese-made surveillance cameras," The Hill, January 12, 2018. *http://thehill.com/policy/defense/368710-us-army-base-removes-chinese-made-surveillance-cameras*

[35] Hamza Shaban, "Pentagon tells U.S. military bases to stop selling ZTE, Huawei phones," The Washington Post, May 2, 2018. *https://www.washingtonpost.com/news/the-switch/wp/2018/05/02/pentagon-tells-u-s-military-bases-to-stop-selling-zte-huawei-phones/?utm_term=.bf1e99041b11*

[36] Keith Stouffer *et al.,* "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication 800–2, Revision 2, May 2015. *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf*

[37] "The state of cybersecurity in the rail industry," Rockwell Collins, August 2017. *https://www.rockwellcollins.com/-/media/Files/rc2016/marketing/C/Cybersecurity-solutions/The-state-of-cybersecurity-in-the-rail-industry-white-paper.pdf?lastupdate=20171215210046*

[38] J. William Middendorf II and Dan Negrea, "China takes a wrong turn," The Washington Times, March 11, 2018. *https://www.washingtontimes.com/news/2018/mar/11/china-takes-a-wrong-turn/*

[39] Testimony of Michael T. Haley, "Update on Federal Rail and Public Transportation Security Efforts," Hearing before the Subcommittee on Transportation Security and Infrastructure Pro-

tection, of the Committee on Homeland Security, U.S. House of Representatives, February 6, 2007.

[40] "Transportation Sector-Specific Plan: Freight Modal Annex," U.S. Department of Homeland Security, 2007, Pg. 2. *https://www.hsdl.org/?view&did=474331*

[41] "Presidential Policy Directive 21—Critical Infrastructure Security and Resilience," The White House, February 12, 2013. *https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil*

[42] Government Accountability Office, "Freight Rail Security: Actions Have Been Taken to Enhance Security, but the Federal Strategy Can Be Strengthened and Security Efforts Better Monitored," Report No. 09–243, April, 2009, Pg. 7. *https://www.gao.gov/products/GAO-09-243*

[43] Id at 7. 44 Testimony of Michael T. Haley, "Update on Federal Rail and Public Transportation Security Efforts," Hearing before the Subcommittee on Transportation Security and Infrastructure Protection, of the Committee on Homeland Security, U.S. House of Representatives, February 6, 2007.

[45] "Strategic Rail Corridor Network (STRACNET)," Global Security, 2012. *https://www.globalsecurity.org/military/facility/stracnet.htm*

[46] Id.

[47] "About SDDC," U.S. Army Military Surface Deployment and Distribution Command, 2016. *https://web.archive.org/web/20110818114337/http://www.sddc.army.mil/What/default.aspx*

[48] James Jackson, "The Committee on Foreign Investment in the United States (CFIUS)," Congressional Research Service, July 3, 2018. *https://fas.org/sgp/crs/natsec/RL33388.pdf*

[49] Executive Order No. 13788, "Buy American and Hire American," April 18, 2017. *https://www.whitehouse.gov/presidential-actions/presidential-executive-order-buy-american-hire-american/*

Response to Written Question Submitted by Hon. Marsha Blackburn to Daniel H. Rosen

Question. Question: In your testimony, you state that China is mixing political guidance with corporate governance, which distorts market outcomes and generally serves the interests of firms in China. Moreover, you note that given China's scale and weight, these distortions can quickly put firms in other nations out of business. In the context of communications and information technology equipment, to what extent can Chinese firms put serious downward pressure on Western technology companies?

Answer. In the context of information and communications technology (ICT) equipment, the benefits of Chinese industrial policies for native firms, including a mixture of political and economic incentives, can impair the commercial viability of Western technology companies. Chinese Communist Party committees present in all state and many private firms have a heavy, if not controlling, influence over leadership assignments and compensation, including at the major banking institutions. Those financial institutions are mandated to promote stability and other political goals, in addition to commercial efficiency. This can translate into permissive financing terms for domestic ICT firms, to support the government's goals in areas like job creation and innovation. Since political stability is not a mandate for creditors to western firms, those firms do not enjoy the financial flexibility that their Chinese competitors do.

Chinese industrial policy can also affects the Nation's outbound direct investment flows in a manner that creates an unlevel playing field for foreign firms. Following decades of unsuccessful attempts to develop a domestic semiconductor industry, for example, in 2014 China enacted a national policy to accelerate the development of its semiconductor industry which included overseas investment as one key element. After the announcement of that initiative, private investors and government funds embarked on an unprecedented buying spree of assets along semiconductor production chains in Asia, Europe and North America.

Before the strategy was announced, outbound investment from China into the global semiconductor industry was low, never exceeding $1 billion in a single year. In 2014, the combined value of Chinese takeovers announced globally increased to $3 billion. In 2015, that figure rose to $35 billion. The total value of transactions actually completed since 2000 adds up to $8.1 billion, a smaller figure as many deals either fell through or were rejected for national security purposes. But nearly all of that $8.1 billion occurred in the 3 years since the Chinese government announced its 2014 strategic plan. Most of these transactions were supported by funding offered on favorable terms from strategic finance vehicles set up by China's central government with an industrial policy mandate.

Western firms that make imprudent bets on acquisitions don't survive. If their Chinese competitors can do so without bearing the same consequences, they will disrupt the competitive ecosystem on which American competitiveness depends.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TODD YOUNG TO JOSH KALLMER

Question 1. Mr. Kallmer—in your testimony you raise a key point—that China may propose many more standards in international standards organizations, but that there is no "first mover advantage" that would give them an advantage in the development of 5G. Could you please expand on this topic?

Answer. As I noted in my testimony, China is rapidly developing a large quantity of domestic standards on various technologies, but quantity does not denote quality. Chinese national standards can often be inadequate for international adoption for a number of reasons, including a lack of technical sophistication, insufficiently addressing interoperability, or because they overtly favor a single vendor's technology, which is unacceptable in an international forum. While Chinese standards are often developed on short timelines with a great deal of downward administrative pressure to generate tangible "deliverables," international standards setting bodies go through a far more rigorous process of review with a wide range of members from the international community. International standards setting bodies have governance processes in place that enable participants to hold any contribution accountable for technical viability and equality for all implementers. The rules have been created so that all contributors are on a level playing field and thus the notion of a "first mover advantage" is a mischaracterization. If their industry produces meaningful technical submissions and submits them to the international process, they will have the same opportunity as the submission from any other participants. There is no doubt that being a contributor is a stronger position than being an observer and that is why ITI has long been a proponent of policies and practices that encourage tech sector R&D investment. The strongest counter to any contribution, from any country, is highly credible technical content of our own. For the U.S. to be most successful 5G standards development, we recommend that the U.S. Government:

- Support U.S. industry R&D investment in 5G space with encouragement and support for international standards participation by the private sector;
- Ensure robust competition in U.S. wireless markets, which results in stronger U.S. companies that are able to innovate and successfully contribute to 5G standards; and
- Maintain a strong USG presence in the international standards arena in order to maintain a healthy standardization system.

Question 2. Shouldn't we encourage U.S. industry to develop wireless technology that will inform international standards in the future? How can we best do that?

Answer. Yes. The U.S. should continue to incentivize R&D in the private sector through programs like the Small Business Innovation Research (SBIR) program, increase public-private partnerships along with strengthening Federal R&D in this area, and ensure robust U.S. competition in wireless, which allows American companies to gain the experience and revenue to make investments in 5G and beyond. With regard to developing standards, the U.S. model for consensus-based, voluntary, industry-led standards is the very approach that has allowed its industry to thrive in the technology space. This approach enables the formulation of standards through qualitative and comprehensive participation from industry technical experts. Because the private sector is at the cutting edge of developments, the long-held U.S. standards development approach has great flexibility and is responsive to often rapid changes in technology. We encourage the U.S. government to continue supporting that approach—helping to facilitate and convene important conversations on pressing standardization issues—while also investing in R&D and innovation as mentioned above.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARSHA BLACKBURN TO SAMM SACKS

Question. Question: Through the Made in China 2025 plan, the Chinese have been exerting influence on critical technology markets, including polysilicon, which is the critical input for semiconductors. What else can the U.S. be doing to help fight back on this front?

Answer. The Chinese government aspires to control the entire 5G supply chain from applications that run on top down to servers and chips. This kind of vertical integration would give Chinese companies greater influence in global technology markets in ways that are harmful from a national security and competitiveness standpoint to U.S. interests.

The U.S. government should create more incentives for U.S. companies to invest in bolstering U.S. capabilities in polysilicon as a critical input for semiconductors. Seeding investment in research and development (R&D) and other forms of public-private partnership that can help reduce the reliance of U.S. industry on China will be key.

U.S. government efforts related to Diminishing manufacturing sources and material shortages (DMSMS) can serve as important resource on the challenge. The Defense Advanced Research Project Agency (DARPA) also has a key role to play.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. TODD YOUNG TO SAMM SACKS

Question 1. Ms. Sacks—you touched on U.S. policymakers adopting a "small yard, high fence" approach in addressing the challenges posed by China. In short, we must be selective in choosing our battles and the technologies that we are willing to go to the mat over.

Today, what are the top three technologies you believe ought to be a part of such an approach and how would you start to address the challenges China poses?

Answer. Updating the export control regime is a long overdue step and necessary considering China's efforts to catch up and surpass the U.S. in technology. The Department of Commerce has issued a list of technologies that may be subject to new export controls due to their importance for national security and has solicited feedback from industry.

The challenge of identifying specific technologies in need of stronger barriers is a very complex one that must be done in close coordination among technical experts across the U.S. government, the private sector, and the academic and research communities. Now is an important window to have these discussions as the export control regime is the process of undergoing major changes.

I have several recommendations:

Under the current export control framework, the term "essential" should not be interpreted to encompass technology that is simply used or is usable by the military, especially since the defense industry is increasingly reliant on commercial off-the-shelf technology.

Related, some experts like MIT's R. David Edelman have commented that distinguishing between civilian and military uses of AI may be impossible, and Jack Clark at OpenAI has said the risk of making an error with AI export controls is therefore quite large.

It is very difficult to prevent code from crossing borders. Many state-of-the-art AI systems like facial recognition are produced by industry and are then (in part or fully) published openly online. It wouldn't be too difficult for a foreign military to pick up the technology and leverage it in a military application. In addition, research is often done collaboratively through networks of engineers around the world that do not confirm neatly to national borders. This further complicates the ability of export controls to prevent potentially harmful uses of American AI tech by foreign governments.

As discussion of new export controls moves forward, processes should be put in place to assess the practical effects given the global nature of R&D and understanding the American competitiveness and innovation underpins security.

In terms of technologies that should be subject to stronger restriction, I believe that greater access to some kinds of semiconductor manufacturing equipment (such as photolithography machines) could enable China to eventually replace foreign suppliers. This is critical to American technological competitiveness since semiconductors underpin much of the advanced computing hardware used to train AI systems. While the Chinese government has spent over $2 billion on a national investment fund and devoted major policy resources to support indigenous industry, local Chinese fabs in China still lack high-end equipment to attain the kind of self-sufficiency to which China's leaders aspire. This is one technology that should perhaps be subject to stronger restriction.

Quantum computing is another area of technology in which to consider stronger export restrictions. While speculation on the construction of a powerful quantum computer varies in the range of a few decades, its development is currently competitive across governments, firms, and academic and other research institutions. Quantum computers essentially would have far greater computing complexity than standard computers in use today. If a powerful quantum computer were developed, the entity in control would likely be able to leverage its capabilities in applications ranging from advanced chemical modeling to new, more sophisticated ways of training AI systems. Powerful quantum computing capabilities may also enable new ap-

proaches to cryptography. Related, there is a substantial risk that a powerful quantum computer would allow the holder to break existing public key encryption algorithms that currently protect information "in transit" across the Internet and other networks.

RESPONSE TO WRITTEN QUESTION SUBMITTED BY HON. MARSHA BLACKBURN TO HON. ERIC ROSENBACH

Question. In regards to information security, there's so much emphasis on the real-time sharing of cyber threats. While this is clearly important, isn't is just as important to have a long term outlook to analyze trends in the marketplace, potential choke points in the supply chain, hi-jacking of standards setting bodies, and things of that nature?

Answer. Yes, while real-time information sharing is a critical element of our defensive strategy, there are at least three longer-term tactics the U.S. can adopt immediately to protect the country from foreign attacks and takeovers.

First, the U.S. must incentivize the use of strong encryption. Making America the world leader in encryption technology could advance both economic and national security interests. Protecting the Nation's most important resource will require a significant expansion in the use of encryption. The nation's defense and security agencies have relied on encryption to protect its most precious secrets for many decades—DoD, in fact, is the largest user of encryption in the world. The U.S. must both clarify the legal questions around encryption and develop real incentives to promote the use and growth of encryption products and platforms that allow individuals and organizations to protect their data.

Second, the U.S. should limit foreign ownership and provide resources to support firms in key information sectors. Over the past decade China has systematically targeted investment in and ownership of firms developing technology, such as AI, that will drive strategic advantage in the Information Age. Congress took encouraging action by reforming and passing legislation that increased limitations and oversight of foreign ownership and involvement in data-rich sectors. This was important, but should be supplemented with new sources of incentives to sustain American tech firms whose technology does not have an immediate commercial application.

Third, good defenses are important, but defense alone will not mitigate the threat of foreign attacks. The U.S. needs to quickly develop precise and legal offensive cyber operations that change the current dynamic of simply sitting back and absorbing the blows of adversarial actions. The private sector cannot meet this challenge: the U.S. Government, led by the Department of Defense, needs to bolster its capabilities to disrupt and degrade Chinese cyber operations before they succeed.

At the same time, the U.S. still has room to improve information sharing efforts. The increased willingness of the Intelligence Community, DHS, and FBI publicly to attribute Chinese cyber attacks through indictments is crucial and positive first step in raising the cost to adversaries. The Intelligence Community should also strive to share as much intelligence information as possible about Chinese cyber operations. In the past, the government has too often watched important intellectual property or data flow out of the country without warning impacted organizations.

RESPONSE TO WRITTEN QUESTIONS SUBMITTED BY HON. TODD YOUNG TO HON. ERIC ROSENBACH

Question 1. Our national security depends in large part on a vibrant, growing, and secure economy. As we continue to face greater international economic competition worldwide, China presents a particular challenge, as all of the panel's testimony has elicited in some form. A failure of the United States to compete economically will undermine the prosperity and security of our Nation.

It is in our national interests of the United States to promote free, fair and reciprocal economic relationships between the United States and foreign individuals and entities. That is why last year, with Senator Cardin as well as Senators Rubio and Coons, I introduced the National Economic Security Strategy Act. This legislation directs the Federal Government—the President in coordination with the National Security Council, the National Economic Council, and the heads of other relevant federal agencies—to periodically submit to Congress a national economic security strategy.

My bill would enhance the ability of the Federal Government to counter the anti-competitive economic behavior, policies, and strategies of foreign individuals and entities. The goal is to ensure Federal policies, statutes, regulations, and procedures

are optimally designed and implemented to facilitate the competitiveness, prosperity, and security of the United States.

Mr. Rosenbach, could you elaborate on your thoughts as to why it is so important for the U.S. to have a comprehensive approach to international predatory economic practices?

Answer. States with authoritarian forms of government—and China in particular—first recognized the strategic importance of information, and have adapted their national laws and policies accordingly. Over the past decade, China has pursued a national strategy to challenge the United States' global leadership in the Information Age through a conscious strategy of state-backed investment, loose consumer data privacy protections, a centralized AI and technology deployment strategy, and intelligence operations to steal crucial data and intellectual property.

The United States, on the other hand, seems to be standing by, beholden to large technology companies focused primarily on connecting more people to generate more data to further bolster their profits. In the absence of a national strategy to protect Americans' data, promote the competitiveness of American firms, and secure our information and technology infrastructure assets, the U.S. risks ceding its leadership role in the future economic, military, and political landscapes.

America needs a whole-of-government strategy to improve national competitiveness in the Information Age. Information geopolitics cuts across all aspects of the economy, society and state security apparatus. Authoritarian governments have adopted a highly centralized, mercantilist approach to protecting, acquiring and using information. Centralization will not be the answer for democracies, but coordination must be. Unprecedented cooperation is required, across economic, social, defense, intelligence, state department and homeland security portfolios. For example, the American government can no longer silo regulatory decisions about information-related companies separate from foreign policy decisions on cyberspace.

Even further, America needs a whole-of-nation strategy that includes coordination with the private sector. The U.S. intelligence community needs to share threat information about foreign intelligence organizations with the social media platforms that so directly influence Americans' economic and political decision. Policymakers must be willing to work with private actors to ensure regulatory red tape does not stand in the way of innovation, and that public-private partnerships continue to create incentives to accelerate technology development. At the same time, American technology firms need to understand, and be held accountable for, their role in protecting national security interests.

Question 2. What are we—the U.S. government—missing in making our policies data-centric?

Answer. The Information Age demands a data-centric security and economic strategy: America needs to develop a data-focused strategy for competitiveness. From a security perspective, a network-centric approach to national security is failing. Focus on the threat of a low probability catastrophic attack on critical infrastructure networks, for example, has distracted leaders from the reality that we are not defending the Nation's most precious resource: information. Likewise, the government has done very little to prioritize the centers of gravity for an economy powered for the Information Age.

The privacy of personal information is also a national security and economic priority. Policies aimed at bolstering U.S. national security and promoting U.S. economic competitiveness must go hand-in-hand with consumer protection. Authoritarian governments may ignore consumer rights in pursuit of acquiring information power, but democracies cannot. Bolstering the global competitiveness of American companies should remain a top priority, but not at the expense of allowing these companies to collect, use, and sell information without user consent or under-invest in cybersecurity measures.

Within the framework of robust national data privacy and security laws, the U.S. government should promote more partnerships with civilian companies and academic institutions to make progress on high-priority AI initiatives. For example, the Defense Innovation Unit—Experimental (DIUx), established by DoD for this purpose, provides a model for incentivizing the private sector to develop technologies with direct national security applications.

Question 3. Mr. Rosenbach—in your testimony you note that while China has an undeniable advantage in data collection due to the nature of its authoritarian government, there are things we can do to keep America competitive. When it comes to deploying next-generation 5G technology, your belief is we must do everything we can to reduce regulatory red tape that slows 5G deployment.

Answer. China's authoritarian system does give it a deployment advantage, but the U.S. can do a lot more to reduce regulatory red tape to expedite deployment of

next-generation broadband infrastructure. Nationwide 5G deployment is a massive effort requiring equipment installation and associated permits and approval processes across thousands of localities. Yet without this foundation, the U.S. risks falling behind in the next generation of wireless-enabled technologies. Policymakers must drive toward regulation that standardizes and fast-tracks local approvals, while giving local authorities the opportunity to provide implementation guidance.

The U.S. should ensure regulation supports the competitiveness of American firms in critical sectors. American firms are currently locked in a tight competition with Chinese powerhouses to determine who will dominate this important area. The U.S. government—and the FTC in particular—should make sure that regulations designed to protect consumers and competition don't inadvertently undermine the competitiveness of American firms relative to Chinese national champions like Huawei.

To promote American competitiveness in 5G technology development and in other critical sectors more broadly, the U.S. must also win the race for talent. The U.S. has a history of prizing and nurturing openness, creativity, and innovation. Our university system is a springboard for raw talent; our legal and government institutions allow new businesses to thrive; and our sophisticated financial system enable the best ideas to be successful. To maintain a competitive edge, the U.S. needs a foundation of policies and practices that continue to attract top talent, like the heads of AI at Apple, Facebook, Microsoft, and Google's cloud computing division, who were all born outside the US. The visa program is a good place to start—at minimum, Congress should ensure that more highly skilled workers are able to obtain H–1B visas. Policymakers should further consider special programs for students and experts in the AI and broader set of STEM fields.

Question 4. Mr. Rosenbach, do you believe the FCC has the required authority today to put the U.S. in a position to win the race to 5G? If not, what additional authorities should Congress give to the FCC to ensure burdensome regulations don't keep us from doing everything we can to win the race to 5G?

Answer. I am not an expert on the FCC, so while I do not have specific recommendations for FCC authority reform, I do support a whole-of-government approach to ensuring American competitiveness in 5G deployment.