S. HRG. 117–305

COUNTERING THE PEOPLE'S REPUBLIC OF CHINA'S ECONOMIC AND TECHNOLOGICAL PLAN FOR DOMINANCE

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

SECOND SESSION

MAY 11, 2022

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.govinfo.gov

U.S. GOVERNMENT PUBLISHING OFFICE
47–983 PDF WASHINGTON : 2022

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

MARK R. WARNER, Virginia, *Chairman*
MARCO RUBIO, Florida, *Vice Chairman*

DIANNE FEINSTEIN, California
RON WYDEN, Oregon
MARTIN HEINRICH, New Mexico
ANGUS KING, Maine
MICHAEL F. BENNET, Colorado
BOB CASEY, Pennsylvania
KIRSTEN E. GILLIBRAND, New York

RICHARD BURR, North Carolina
JAMES E. RISCH, Idaho
SUSAN COLLINS, Maine
ROY BLUNT, Missouri
TOM COTTON, Arkansas
JOHN CORNYN, Texas
BEN SASSE, Nebraska

CHUCK SCHUMER, New York, *Ex Officio*
MITCH MCCONNELL, Kentucky, *Ex Officio*
JACK REED, Rhode Island, *Ex Officio*
JAMES INHOFE, Oklahoma, *Ex Officio*

MICHAEL CASEY, *Staff Director*
BRIAN WALSH, *Minority Staff Director*
KELSEY STROUD BAILEY, *Chief Clerk*

C O N T E N T S

MAY 11, 2022

OPENING STATEMENTS

WITNESSES

COUNTERING THE PEOPLE'S REPUBLIC OF CHINA'S ECONOMIC AND TECHNOLOGICAL PLAN FOR DOMINANCE

WEDNESDAY, MAY 11, 2022

U.S. SENATE,
SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 2:52 p.m., in Room SH–216, Hart Senate Office Building, Hon. Mark R. Warner (Chairman of the Committee) presiding.

Present: Senators Warner, Rubio, Feinstein, Wyden, Heinrich, King, Bennet, Casey, Gillibrand, Collins, Blunt, Cotton, Cornyn, and Sasse.

OPENING STATEMENT OF HON. MARK R. WARNER, A U.S. SENATOR FROM VIRGINIA

Chairman WARNER. Good afternoon. I call this hearing to order.

Welcome to our witnesses.

As I've explained, there are a couple of fairly significant votes this afternoon, so there will be some moving in and out.

But again, to our witnesses, Dr. James Mulvenon, Senior China Analyst; Dr. Dewey Murdick, Director of Georgetown University's Center for Security and Emerging Technology; and Hon. Nazak Nikakhtar, a partner at Wiley Rein and Former Assistant Secretary for Industry and Analysis at the Department of Commerce.

I would start by saying that the Intelligence Committee doesn't actually have that many open hearings, if today's attendance is any indication of why we don't. But the truth is, on this the Vice Chairman and I believe it's really important not just, obviously, for the people who are here but to do this in a public setting to make sure that we are fully aware of the challenges we face from the People's Republic of China, because the nature of this challenge extends far beyond the intelligence and military spheres.

Let me be clear at the outset. When I talk about China, my beef is with the Communist Party of China. It is with Xi Jinping and their authoritarian order. It is not with the Chinese people or in any way the Chinese diaspora, particularly in terms of Chinese-Americans who've made great contributions to our country.

But the PRC poses, I believe, a unique challenge to the United States. Not only United States, but the whole so-called Western liberal international order. No other state actor in recent history has been able to compete with both the West diplomatically, militarily,

and now economically, particularly in our subject today, in technology, at the scale that China can. And that's why for several years now this Committee, on a bipartisan basis, has focused on the technological and economic challenges posed by the PRC. But as strong as we are in this country, we can't do this alone. We need our allies. We also need the American public, including the private sector and our academic institutions and our media outlets to better understand the Chinese Communist Party's efforts to overtake and lead on particularly critical technologies, and the global implications if the PRC is able to do that—of what that would mean for the United States and others if we ceded that territory.

That's why in addition to these open hearings, we also have on a bipartisan basis, again, been hosting what we've called classified roadshows with intelligence, community leaders, industry sectors, academia and others on the threats posed by the CCP's authoritarian regime.

Today's hearing, which will focus on the state of the US-China technology competition, builds on other efforts we have undertaken. Ongoing efforts in terms of these classified roadshows, but other public hearings. One of the more recent ones we had was in August 2021 when we held an open hearing on the counterintelligence threat posed by the PRC. I think for many of us, and I say this as a former telecom guy, the wakeup call for me was with Huawei when several years ago we realized that the PRC had positioned its national champion as a dominant supplier of communications infrastructure across, candidly, much of the globe. And if you actually looked at where Huawei equipment was being sold in the United States and the overlay with some of our anti-ballistic missile installations, it was really chilling. And the truth was, if we had not raised that flag, Huawei and the PRC were poised to cement and dominate the market, not only for 5G, but for next generation wireless services like O-RAN as well.

Truthfully, I think we were caught as a nation and the Intelligence Community, the military, into an industry we were, frankly, caught flat-footed when we realized that there was not only not any American alternate but very few Western technology telecom competitors.

Despite the fact that had Huawei been truly successful, the clear privacy and national security risk presented by that company with its direct ties to its authoritarian regime in Beijing would be a tremendous threat to our whole communications infrastructure. But as we discovered, 5G is just the tip of the iceberg. In the last couple of years, policymakers have realized that the PRC has been diligently working over the past decade to identify a set of emerging and foundational technologies that will confer long-term influence into the entire innovation ecosystem and global supply chains. It is in this context that we realized we needed a national strategy to identify and counter the PRC's ambitions across a set of key technologies—not just 5G, but obviously artificial intelligence, quantum computing, biotechnology, precious metals—and that we need to safeguard our own and our allies' leadership in existing foundational and enabling technologies like semiconductors.

Out of that realization, we've started to act. Legislation currently moving through Congress, like the CHIPS Act and the U.S. Innova-

tion and Competition Act, as well as repeated engagements with the private sector through these roadshows I previously mentioned, are all steps in the right direction. But this belated realization by American policymakers reflects a complacency with our own innovation and, quite honestly, a little bit of inattention to PRC's objectives and their efforts.

For a long time, we thought it didn't matter whether we actually made both the innovation and the products here in the United States. We thought as long as we captured the value in designing and providing services based on those products, we'd basically win out. The conventional view underestimated how effectively one country, in this case the PRC, could exert control over the entire ecosystem by leveraging control over certain key foundational technologies, not only through control of the technologies themselves, but also through the supply chains. And something that I think oftentimes we didn't focus on was those standards setting bodies that often set the rules, standards, protocols for so many technologies. We dominated that. We in America in particular dominated that for decades. In the case of Huawei and 5G, it was the first time we realized not only did China have a leading company, but they were literally setting the rules of the game.

This is not a lesson that we need to learn the hard way once again. If we don't set the standards and protocols for these technologies, our democracies and other allies will not win out; the PRC will. Not only will they set the standards to achieve their illiberal vision of CCP control, but their advantages will translate into military capabilities, geopolitical influence, and economic advantages.

I look forward to the witnesses' testimony on this issue.

For Members' information, today we'll be doing something a little out of the ordinary. Rather than going by order at the time of the gavel, we will be asking questions by order of seniority in five-minute rounds.

With that, I turn to my good friend, the Vice Chairman, Senator Rubio.

OPENING STATEMENT OF HON. MARCO RUBIO, A U.S. SENATOR FROM FLORIDA

Vice Chairman RUBIO. Thank you, Mr. Chairman.

Thank you to all the witnesses for being here today. I think it is an important hearing we are going to discuss. We often talk about China's plans and intentions behind closed doors. But the fact of the matter is that their ultimate goal and what they're trying to do is really not that big a secret. They seek to displace the United States and to become the world's most dominant economic, industrial, technical, and military and geopolitical power. That's their goal. We in this country for a long time had this hope for the better part of 20 years, this consensus, really, that once the Chinese Communist Party in that country became rich, it would become more like us—move toward democracy, have respect for the rules of economic engagement and so forth.

Well, obviously that's not materialized. In fact, they've used the last 20 years to wage an economic war against the United States, stealing jobs, exploiting the free and open market, oftentimes with help by American corporations driven by the short-term profits that

can be gained by having access to the Chinese market. And as part of that goal was to leave us as Americans economically dependent, not just on their massive market, places you want to sell things, but supply chains as well. And we've seen that disruption play out during a pandemic. Imagine in a time of conflict.

And so, they know that once we are dependent on them, our manufacturing base, our supply chains, critical minerals, and not to mention the dangling the promise of access to their massive market, well then our options will be limited and their leverage will be extraordinary.

And they've been able to achieve this through their military-civil fusion strategy, through their national laws that compel the transfer of sensitive information to the government, and frankly, by weaponizing some of our companies against us here in the United States. In many cases, we find that it's American corporations, because they manufacture there or because they want to have access to their market, that are then turned around and become advocates in favor of the Chinese position on any sort of different issue that we face here domestically.

The Intelligence Community—I think at this point leaders on both sides of the aisle have been pretty clear that this is the single greatest challenge this Nation has ever faced. We have never faced a near-peer adversary that poses such a comprehensive challenge the way that China does today. The Soviet Union was a military and a geopolitical rival. They were never an industrial or technical or commercial rival. China is all of that and more. And as I said earlier, if we think having supply chain disruptions as a result of a pandemic shutting down some factories has been bad for our economy, imagine it being shut down deliberately as leverage against us in a time of future conflict, because that's what we can expect to see. It leaves us vulnerable, and it's something we need to begin to address.

I will make one final point and then the two things I hope we can take from this hearing. I think this matters because I think it matters if the most powerful—. Let me put it to you this way. If the most powerful and influential nation on earth is a dictatorship that is willing to enslave its own people in death camps and commit genocide against its population, if that's how they treat their own people and that's the most powerful country in the world, that's not going to be a good world. And that is, unfortunately, what we're headed toward if we don't deal with that. And if anyone has any illusions about the nature of the Communist Party of China, ask the people of China and people living in places like Tibet and Hong Kong and Xinjiang, and they'll tell you what this government is capable of doing.

In closing, what I hope we'll hear today are your views on China's economic and technological plan to dominate key technologies and control critical supply chains. And also, perhaps as part of this hearing, we can begin to think more about how we can dramatically increase our efforts to reduce our economic vulnerability to the Chinese Communist Party.

Thank you for being here with us today.

Chairman WARNER. Again, I thank all the witnesses for being here. I'm not sure who's going to go first, so I'm going to throw it to the panel and whoever is going first, proceed.

STATEMENT OF JAMES MULVENON, Ph.D.,
SENIOR CHINA ANALYST

Dr. MULVENON. Good afternoon.

Senator Warner, Mr. Chairman, Vice Chairman Rubio, other Members of the Committee, thank you for inviting me here today.

I first need to say my name is James Mulvenon. I'm here in my personal capacity. I'm not representing either the company I work for nor any of my Intelligence Community sponsors. They asked me to say that.

For the Committee's reference, the three of us have a rough show-run that we've worked out. I'm going to introduce at a strategic level the key elements of the Chinese strategy and the elements of that strategy, and then pass it to my other colleagues to discuss specific Chinese progress in certain technology areas. And then, clearly, the toolkit that the U.S. Government has for us to be able to deal with these threats—what's working, what's not and how could Congress help us fresh out the toolkit.

The overwhelming strategic point, which just echoes what Senator Warner said in his introduction, is that China does have a deliberate, published national economic and national security strategy to achieve the very levels of domination that Senator Rubio mentioned in his introduction. And as part of that, these strategies are designed to create an unfair, asymmetric environment for U.S. and other multinational companies operating in the Chinese market to force the transfer of technology to domestic national champions who will then turn around and push our companies out of the China market and then compete with them globally.

The main features of this strategy are multifold, but deliberate. First is a focus on industrial planning. We're all familiar that Communist parties like five- and ten year plans, but the Made in China 2025 Plan, the Mid- to Long-Range Science and Technology Plan are dedicated roadmaps for how to achieve their objectives over the next 20 years. I find it notable that whenever we pay too much attention in English to any of these plans, they are suddenly deleted from the Chinese Internet and then it becomes difficult to find them. My question, of course, is what do you have to hide?

That is also followed, as Senator Rubio said, by very dedicated national strategies for what is now more commonly known as military-civil fusion. We've done a lot of work in the last couple of years across the Community looking at this issue and really explicating it.

Finally, there's a level of state subsidy through that industrial planning that disadvantages our companies. And those subsidies are directed primarily toward national champion companies chosen by the parent ministries in China to be the focus of their funding, the focus of their technology development. And then once our companies go to China, they find themselves having to joint venture with these national champions at the direction of the regulator, which then facilitates that technology transfer.

In the last five to ten years, China has also published a blizzard of new laws and regulations, despite not being a rule-of-law country, but a rule-by-law country. But these are codified to be able to use against multinational companies to defend the predatory and extractive practices of the government.

As Senator Warner mentioned, the Chinese for the last 15 to 20 years have used the international standards regime as a trade weapon in order to shape the future of the architecture in ways that benefits their companies like Huawei and ZTE by local directives, Greenfield investment strategies inside the United States once we started to cotton on to the idea that they were trying to force us to do transfers in China, instead decided to come where the technology was, which was in the U.S. And then finally, their global mercantilist policies, which undermine many elements of the international rules-based order that we had put in place since Bretton Woods.

In my own research, I've focused significantly on the illegal technology acquisition side of their strategy. In 2013 with two government employees, I wrote a book called "*Chinese Industrial Espionage*" that detailed in extraordinary detail all of the elements of both the nontraditional collection side that I'm sure the Committee has heard about a lot in terms of their ability to hoover up large volumes of information in the United States and then exploit it back in China. But also their planetary-scale cyber-espionage program as well as their efforts to steal technology here in the United States.

And then finally on the nontraditional side, obviously significant focus on China's 500-plus national, provincial, and municipal talent programs as a way of luring back researchers in the United States and other Western countries with financial incentives in order to transfer that technology. I would only highlight that one little-discussed aspect of the talent programs is that it allows them to have contact with experts who can help them understand the intangible elements of innovation that they can't understand in the stolen blueprint or the stolen source code. It helps them fill in the mortar between the bricks.

I would close by saying that while this Committee deals with a lot of areas of the intelligence challenge that are primarily achieved through national technical means, that this is one of those intelligence challenges that lends themselves very easily to open source intelligence. Not only are all the strategies and documents and regulations that I've mentioned publicly available, but all of the underlying data needed to assess those strategies, whether it's the technical journal articles, the patents, the corporate records, the government and military procurement bidding tenders, are all publicly facing. The bad news, as you can imagine, is that they're all in Chinese, which China regards as its first layer of crypto in terms of being able to disguise what they're doing. Open source intelligence allows us to really get deeply into these issues, as I think my colleagues will confirm.

Let me close my remarks there and I look forward to your questions.

[The prepared statement of Dr. Mulvenon follows:]

Statement before the
Senate Select Committee on Intelligence
"Threats to US National Security: Countering PRC's Economic and Technological Plan for Dominance"

A Testimony by:

James Mulvenon, Ph.D.

March 11, 2022

216 Hart Senate Office Building

Introduction

Chairman Warner, Ranking Member Rubio, and distinguished members, thank you for inviting me to testify today.

My remarks today can be divided into three sections: (1) a summary of the Chinese Communist Party's economic and technological strategies; (2) the role of illicit technology acquisition in those strategies; and (3) the unique value of open-source intelligence to combat these problems.

The Chinese Communist Party's Economic and Technological Strategies

The Chinese government has a comprehensive strategy for national economic growth and technology modernization. This strategy has created an unfair, asymmetric business environment in China, sometimes forcing American companies, which need to be in the China market to grow and prosper, to make suboptimal decisions that are not always in the long-term interests of U.S. national security, but clearly benefit Chinese national security. Although American companies are one of Beijing's highest priority targets in the race to close the technological gap with the United States, the current tech transfer crisis is not entirely their fault. In the China market, American companies confront a comprehensive, state-directed economic and technological development strategy designed to promote technology transfer from foreign multinationals and elevate domestic companies to compete with those multinationals in the global market.[1] This strategy is one personally touted by President Xi Jinping, who declared at a recent Communist Party meeting that the Chinese state must determine which technologies to develop on its own, which to induce or co-opt from abroad, and which to develop in partnership with Chinese entities.[2] Xi's personal vision has been codified into a more concrete strategy with a number of key overt features:

- Promulgation of state industrial planning documents outlining how Beijing would use its substantial regulatory leverage and financial resources to promote technology transfer (e.g., "2006-2020 Mid-to-Long Range S&T Plan" and "Made in China 2025"[3])
- Implementation of the strategy of "military-civilian fusion" that expands "civil-military integration" of defense and civilian industrial bases to facilitate the "construction of a national infrastructure that connects the PLA, state-owned defense research,

---

[1] For an overview, see Jane Perlez, Paul Mozur And Jonathan Ansfield, "China's Technology Ambitions Could Upset the Global Trade Order," *New York Times*, 7 November 2017, accessed at:
https://www.nytimes.com/2017/11/07/business/made-in-china-technology-trade.html?_r=0

[2] https://chinacopyrightandmedia.wordpress.com/2016/04/19/xi-jinping-gives-speech-at-cybersecurity-and-informatization-work-conference/

[3] See U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections*, 2017, accessed at:
https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf

development, and manufacturing enterprises, government agencies under the State Council, universities, and private sector firms."[4]

- Provision of massive state subsidies (e.g., National Integrated Circuit Fund) to benefit Chinese companies, often masked in ways to skirt WTO prohibitions (according to the U.S Chamber's analysis of Made in China 2025, China will "provide preferential access to capital to domestic companies in order to promote their indigenous research and development capabilities, *support their ability to acquire technology from abroad*, and enhance their overall competitiveness"[5]). Other benefits include "fiscal stimulus, tax reductions and holidays, access to low-cost or free land, low-interest credit, easier access to securities markets, patent approvals, discriminatory technical standards, antitrust policy directed against disfavored competitors, privileged government procurement, limits on market access, and other preferential policies."[6]
- Promotion of "national champion" companies (e.g., Huawei) to supplant multinational companies in the China market and globally[7]
- Promulgation of laws and regulations codifying asymmetries in playing field for U.S. companies operating in China using a very broad definition for what constitutes national security (e.g., Anti-Monopoly Law,[8] Cybersecurity Law,[9] Counter-Espionage Law,[10] National Security Law,[11] Counter-Terrorism Law[12])
- The use of a domestic standards regime, especially with respect to information communication and telecommunications, as a trade weapon to advantage Chinese

---

[4] Greg Levesque and Mark Stokes, *Blurred Lines: Military-Civil Fusion and the "Going Out" of China's Defense Industry*, Pointe Bello, December 2016, accessed at: https://static1.squarespace.com/static/569925bfe0327c837e2e9a94/t/593dad0320099e64e1ca92a5/1497214574912/062017_Pointe+Bello_Military+Civil+Fusion+Report.pdf

[5] See U.S. Chamber of Commerce, *Made in China 2025: Global Ambitions Built on Local Protections*, 2017, accessed at: https://www.uschamber.com/sites/default/files/final_made_in_china_2025_report_full.pdf

[6] Scott Kennedy, "Evaluating CFIUS: Challenges Posed by a Changing Global Economy," Statement Before the House Committee on Financial Services, Subcommittee on Monetary Policy and Trade, 9 January 2018, accessed at: https://financialservices.house.gov/uploadedfiles/hhrg-115-ba19-wstate-skennedy-20180109.pdf

[7] James McGregor, *China's Drive for 'Indigenous Innovation: A Web of Industrial Policies*, Washington, DC: US Chamber of Commerce, July 2010.

[8] U.S. Chamber of Commerce, *Competing Interests in China's Competition Law Enforcement: China's Anti-Monopoly Law Application and the Role of Industrial Policy*, accessed at: https://www.uschamber.com/sites/default/files/aml_final_090814_final_locked.pdf

[9] https://www.chinalawtranslate.com/cybersecuritylaw/?lang=en

[10] https://www.chinalawtranslate.com/anti-espionage/?lang=en

[11] http://www.chinalawtranslate.com/2015nsl/?lang=en

[12] https://www.chinalawtranslate.com/%E5%8F%8D%E6%81%90%E6%80%96%E4%B8%BB%E4%B9%89%E6%B3%95-%EF%BC%882015%EF%BC%89/?lang=en

companies (e.g., WLAN Authentication and Privacy Infrastructure or WAPI, draft China CPU/OS/computer standards, and the 5G cellular standard)[13]

- Promotion of "buy local" laws to disadvantage foreign firms, especially in information and communications technologies[14]
- Strategies to attract priority foreign investment in China, especially joint ventures and "greenfield" investments[15]
- Mercantilist investment structures globally designed to create infrastructure path dependencies for Chinese state-owned enterprises ("One Belt, One Road")[16] and quasi-private companies that China aims to ensure will provide the hardware and software that will underpin all critical infrastructure of the future, from power grids to telecom networks to e-payments infrastructure.

These activities have a direct and lasting negative impact on U.S. national security. As the Communist Party seeks to enhance all aspects of its national comprehensive power, U.S. comparative advantages will become even more paramount in sustaining U.S. leadership on the battlefield, including in advanced technologies. For example, the Pentagon's "third offset" strategy seeks to leverage current U.S. commercial technological advantages in key areas, such as artificial intelligence and machine learning, to enhance our war fighting capability vis-a-vis China and a resurgent Russia.[17] Yet if our porous investment security and export control regime is not improved, Beijing may be able to turn these current American advantages into their own by investing in, acquiring, or co-opting critical technology. This will allow China to deny the United States' ability to leverage critical technologies for its national security, and further close the gap with the U.S. in areas of key military systems and applications ranging from hypersonic glide vehicles to AI-enabled cyber defense systems.

---

[13] Dan Breznitz and Michael Murphree, "The Rise of China in Technology Standards: New Norms in Old Institutions," report prepared for the U.S.-China Economic and Security Review Commission, 16 January 2013, accessed at: https://www.uscc.gov/sites/default/files/Research/RiseofChinainTechnologyStandards.pdf

[14] U.S. Chamber of Commerce, *Preventing Deglobalization: An Economic and Security Argument for Free Trade and Investment in ICT*, 2016, accessed at: https://www.uschamber.com/sites/default/files/documents/files/preventing_deglobalization_1.pdf

[15] For the best data on the subject, see the American Enterprise Institute's China Global Investment Tracker at https://www.aei.org/china-global-investment-tracker/ and The Rhodium Group's China Investment Monitor at http://rhg.com/interactive/china-investment-monitor

[16] Christopher Johnson, *President Xi Jinping's "Belt and Road" Initiative: A Practical Assessment of the Chinese Communist Party's Roadmap for China's Global Resurgence,* Center for Strategic and International Studies, March 2016, accessed at: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160328_Johnson_PresidentXiJinping_Web.pdf

[17] https://www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence/

The Role of Illicit Technology Acquisition in CCP Strategies

In 2013, two U.S. government colleagues and I published a book entitled *Chinese Industrial Espionage*, which documented the efforts, both quasi-legal and illegal, used by the Chinese government and state-owned entities to steal U.S. technology, intellectual property, and secrets.[18] For me, this culminated almost two decades of tracking Chinese cyber espionage and the PRC military and defense industrial base's efforts at illicit technology transfer. Beijing's illicit and non-traditional collection activities cover four main areas well known to this Committee:

- Beijing's well-documented, planetary-scale, government-directed cyber espionage program[19]
- Large-scale, government-directed technology espionage[20]
- Non-traditional collection (e.g., the "1000 Talents Program")[21]
- New types of hybrid cyber and human technology espionage (According to the 2016 U.S-China Economic and Security Review Commission report: "China appears to be conducting a campaign of commercial espionage against U.S. companies involving a combination of cyber espionage and human infiltration to systematically penetrate the

---

[18] William Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, London: Routledge, May 2013.

[19] See *Foreign Spies Stealing US Economic Secrets in Cyberspace: Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011*, Office of the National Counterintelligence Executive, October 2011, at https://www.ncsc.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf; ThreatConnect, *CameraShy: Closing the Aperture on China's Unit 78020*, at https://www.threatconnect.com/camerashy/; Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, accessed at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf; Dmitri Alperovitch, *Revealed: Operation Shady RAT*, McAfee, August 2011; McAfee® Foundstone® Professional Services and McAfee Labs, Global Energy Cyberattacks: 'Night Dragon', 10 February 2011, accessed at: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf; Bryan Krekel, Patton Adams, and George Bakos, *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*, (report prepared for the U.S.-China Economic and Security Review Commission by Northrop Grumman Corp), March 7, 2012; and *Operation SMN: Axiom Threat Actor Group Report*, accessed at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[20] Peter Mattis, "Testimony before the U.S.-China Economic and Security Review Commission: Chinese Human Intelligence Operations against the United States," 2 June 2016, accessed at: http://www.uscc.gov/sites/default/files/Peter%20Mattis_Written%20Testimony060916.pdf

[21] William Hannas, James Mulvenon, and Anna Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization*, London: Routledge, May 2013.

information systems of U.S. companies to steal their intellectual property, devalue them, and acquire them at dramatically reduced prices."[22])

Any one of these strategies or policies in isolation would be problematic for the U.S. government and American companies, but their simultaneous and often coordinated implementation with the explicit support of PRC government leadership presents an unprecedented challenge.

The Unique Value of Open-Source Intelligence to Countering the PRC's Strategies

I have spent the last 25 years building teams of cleared linguist-analysts, mainly Chinese and Russian, and cleared technical engineers, performing open-source collection, exploitation, and analysis for the US Government. As Members of the Committee know, some intelligence missions primarily require classified national technical means, while other intelligence missions lend themselves more easily to open-source collection and exploitation. I can confirm that open-source intelligence is particularly powerful for the topics I have been discussing. Most, if not all, of China's national level economic and technological development strategies are openly published, as are the accompanying implementation documents. This is also true of China's "military-civil fusion" strategy, as well as myriad laws and regulations that are promulgated to institutionalize the predatory system. All these documents are published in Chinese, and official translations are rare. Moreover, the core data required to track the implementation of the strategies (procurement bids and tenders, corporate records, investments records, patents, legal proceedings, and even résumés) are all available on public-facing Chinese databases, though again all in Chinese and often requiring moderately sophisticated tradecraft to access in a non-alerting way. With the passage of China's Data Security Law, it has recently become more difficult to access these datasets from outside of China, requiring more sophisticated methods. However, nearly all the information necessary for the US Government to gain deep and operationalizable insight into these CCP strategies and transactions remain available from open sources.

Conclusion

The People's Republic of China, through its economic and national security strategies, poses a serious threat to dominate key technologies and control key supply chains in ways that are inimical to American interests, though focused open-source intelligence could provide us with uniquely valuable and actionable insights. I look forward to your questions and again express my appreciation for the invitation to testify.

---

[22] *USCC 2016 Annual Report*, accessed at: https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf

STATEMENT OF DEWEY MURDICK, Ph.D., DIRECTOR, GEORGETOWN UNIVERSITY, CENTER FOR SECURITY AND EMERGING TECHNOLOGY (CSET)

Dr. MURDICK. Thank you, James.

Chairman Warner, Vice Chairman Rubio, Members of Committee, thank you so much for the invitation.

In 2018, a Chinese state-run newspaper identified nearly three-dozen critical technologies that they believe made themselves vulnerable to potential sanctions and export control. These articles covered a wide range of examples, from the difficulty with producing high-strength steel, which impacts rocket engines and aviation landing gear, all the way to the challenges with building high-resolution LiDAR, the eyes of many unmanned vehicles.

These articles express the feeling that the U.S. and other powers could strangle China at any time. The Chinese are keenly aware of their deficits and are making strides toward achieving technical self-sufficiency. They regularly leverage a wide range of government powers in an attempt to dominate key technical areas and not just the cutting edge ones. Understanding who is leading and who is following in emerging technologies between the U.S. and China requires evaluating the right markers for the right question. I find it helpful to look at what the Chinese compare as their strengths and weaknesses to the U.S. in the emerging technology development. For example, the Institute for International and Strategic Studies at Peking University notes China's own technical strength has been improving progressively in recent years and it has become an influential S&T power. In AI and machine learning, the Chinese consider themselves to be leading in product-driven R&D: areas like facial and speech recognition, computer vision, and training talent at scale. In basic research, the U.S. and China are comparable in their eyes in terms of scientific research, paper publication, and citations. Yet the Chinese acknowledge they lag behind the U.S. in originality and groundbreaking research, and also in their ability to attract and retain top AI talent. The U.S. still has a large lead in AI chips, algorithms, machine learning and other core technologies in promoting military AI applications and application of military technologies and biosynthesis and drug discovery, where they see the U.S. making a lot of advances and breakthroughs.

Furthermore, though the U.S. relies heavily on foreign chip manufacturing, it maintains an overall technical advantage through its possession of key intellectual property and the integration of that intellectual property in advanced semiconductor supply chains. Though China's circuit industry is rapidly developing, it faces foreign dependencies that keep it well behind the United States. This is their self-assessment of where they are.

Beyond AI, the Chinese are also aware of places where they maintain leverage over the U.S. in key parts of the global supply chain. In 2019, a majority of malaria test kits, for example, as well as more than 90 percent of some key antibiotic imports, came from China. The pandemic has demonstrated the massive disruptive effects of foreign dominance of the bio-economic supply chains with a direct impact on U.S. research and medical care. China gaining advantages in key technologies, be it artificial intelligence or semi-

conductors for computing, be it genome editing or quantum technologies, would have considerable implications in global security and potentially even U.S. Intelligence Community operations.

The United States needs to prepare now for the long term. As China's tech ecosystem matures and becomes increasingly innovative, the United States risks being increasingly surprised or even falling behind, because we don't have a comprehensive view of what China and other actors are doing across the technical landscape.

I see three basic classes of tools or responses that, when used together, can achieve the greatest effect. They are: one, run faster. Spur on the innovation system.

Two, slow competitors down—and you'll hear more about this soon. Coordination with our allies is essential, in my opinion, to maximize effectiveness.

And three, monitor the S&T landscape, which is a critical point of success when dealing with a long-term competition with a high-tech peer, which is where I believe we are moving with China. On this last point of S&T monitoring. China's rapid rise in science and technology has been facilitated by a massive and sustained state support that is staffed by more than 60,000 open source collectors and analysts. This allows China to prioritize areas of exploration dynamically and helps ensure the country is not surprised by worldwide innovations. To my knowledge, no part of the U.S. Government, including the IC, has developed a scalable countermeasure to this Chinese approach. We need to embrace this transformative S&T landscape-monitoring mission. When used in combination with run faster and slow them down policy options, it will help maintain leaderships and critical emerging technologies in supply chains now and into the future.

Thank you, and I look forward to the discussion.

[The prepared statement of Dr. Murdick follows:]

Testimony before the Senate Select Committee on Intelligence
Countering the People's Republic of China's Economic and Technological Plan for Dominance

Dewey Murdick, Ph.D.
Director, Center for Security and Emerging Technology (CSET), Georgetown University

May 11, 2022

Chairman Warner, Vice Chairman Rubio, members of the committee, thank you for the invitation.

China is keenly aware of its gaps and is using every means available to close them

In 2018, a Chinese state-run newspaper identified nearly three dozen crucial technologies that relied on specific imports that make China vulnerable to other countries' potential sanctions and export controls. In a series of articles, the full list of which is provided below in Appendix A, the authors covered topics including:

- The difficulty with producing rocket engines and aviation landing gear due to limitations in making high-strength steel;
- The challenges of building reliable high-resolution LiDAR (or light detecting and ranging sensors) that are the "eyes" of many unmanned vehicles; and
- Detailed gaps in China's ability to produce key semiconductor manufacturing equipment components.

These articles expressed the feeling that the United States and other powers could use these and other limitations to "strangle" China at any time.

The Chinese are keenly aware of their strengths *and* deficits, and are making strides toward achieving technological self-sufficiency. They regularly leverage a wide range of government powers in an attempt to dominate key technology areas — not just the cutting edge.

Understanding who is leading and following in emerging technologies between the United States and China requires evaluating comparative success across several key markers of leadership. These include research-driven knowledge creation, financial investment, human talent, intellectual property ownership, market share in technologies, and international standards and norm setting. Using these measures, it is helpful to understand what China sees as its comparative advantages or weaknesses in emerging technology development.

For example, an article published in January by the Institute for International and Strategic Studies at Peking University notes China's own technological strength has been improving progressively in recent years and it has become an influential science and technology (S&T) power. In artificial intelligence and machine learning, the Chinese consider themselves to be leading in product-driven research and development areas like facial and speech recognition, computer vision, and talent training at scale. In basic research, the United States and China are comparable in terms of scientific research paper publication and citation numbers. Yet the Chinese also know they lag behind the United States in original, groundbreaking research and in universities' and employers' ability to attract and retain top AI talent. Further, they view U.S. efforts to coordinate AI technology standards among global democracies as compounding their own problems with internally coordinating standards at different levels of government.

The United States still has a large lead over rapidly-advancing China in AI chips, algorithms, machine learning, and other core technologies; it leads in promoting military AI applications, and it has introduced ML technology in biosynthesis and drug R&D, achieving major breakthroughs. Though the United States relies heavily on foreign chip manufacturing, it maintains an overall technological advantage through its possession of intellectual property and the integration of IP in advanced semiconductor supply chains. Though China's circuit industry is rapidly developing, it faces redundancies and foreign dependencies that keep it well behind the United States. And the same Peking University study cited above also

notes that the technical strength gap between China and the United States in 5G and other communications technologies is narrow.

Beyond AI, the Chinese are also aware of the places where they maintain leverage over the United States in key parts of global supply chains. A December 2020 Congressional Research Service (CRS) report stated that, in 2019, 57.7 percent of U.S. imports of malaria diagnostic test kits came from China, as did more than 90 percent of key antibiotics and their derivative imports. As reported in a recent Nature article, the pandemic demonstrated the massive disruptive effects of China's dominance in bioeconomic supply chains for U.S. research and medical care, including backlogs of medical PPE and laboratory equipment vital to operations like gloves, pipette tips, and bleach for decontamination. Experimental materials including DNA extraction kits and research animals were also interrupted. Labs could not conduct any kind of research during this time, halting or slowing groundbreaking and innovative research.

China gaining advantages in any of these technologies, be it artificial intelligence, semiconductors, genome editing, or quantum technologies, would have implications for global security — and potentially, U.S. intelligence community operations.

The United States has three basic ways to shape its response

The United States needs to prepare now for the long term. As China's tech ecosystem matures and becomes increasingly innovative, the United States risks being surprised (and falling behind) because we don't have a comprehensive view of what China and other actors are doing across the technology landscape. I see three basic classes of responses for the United States and its allies that need to be used together to achieve the greatest effect: *run faster*, *slow competitors down*, and *monitor the entire science and technology landscape* more effectively.

First, the U.S. government could help the nation *run faster*. It could spur on the innovation ecosystem by expanding efforts to buy down risk, investing in innovation incubation, and reducing friction points that might slow U.S.-centric private sector innovation. An increase in funding focused on the transition of research and engineering innovations into American-made products would also yield positive domestic outcomes.

Second, the U.S. government can work with its allies to *slow down* the pursuing competition and *protect* critical technology. The United States should work with like-minded countries to maximize the effectiveness of export controls, sanctions and other related measures, as appropriate. However, these measures will not be effective on their own over time because they can be circumvented, require complicated multi-party coordination, create perverse incentives for tech firms to leave the United States, and spur China to innovate around them. Such methods are most useful when employed selectively in combination with *run faster* and the third option, S&T landscape monitoring.

Third, the United States must improve its monitoring of the science and technology landscape. Doing so is critical to our success in long-term competition with a high-tech peer. Specifically, Congress can support an analytic capability that monitors the S&T landscape and enables rapid adoption of new capabilities that offset Chinese advantages. It also is critical in fast follower situations. China's rapid rise in science and technology has been facilitated by more than 60,000 open-source collectors and analysts. China's large-scale S&T analysis capability has enjoyed massive, multi-layered and sustained state support. The resources devoted to these efforts allow China to prioritize technical areas for exploration and help ensure that the country is not surprised by worldwide innovations.

To my knowledge, no part of the U.S. government — including the intelligence community — has developed a scalable countermeasure to the Chinese approach. Instead, the United States relies on private sector parties to watch the threat and opportunity horizon, and has a limited S&T intelligence analysis capability that typically focuses on foreign threats in a handful of areas without comprehensive context. The United States has made no systematic, continuous, and scalable investment into the wholesale survey and monitoring of the worldwide S&T landscape. This analytic gap directly affects national security and economic competitiveness. And it undermines the country's ability to make informed technology-related decisions.

Analysis capabilities are essential to enable competition with a high-tech peer

CSET and others have proposed options to create this much-needed independent capability that uses unclassified sources to monitor global developments in emerging technologies. In fact, CSET has built a relevant prototype. To be effective, it must sit apart from the intelligence community due to authority and incentive challenges. The U.S. government needs a continuous analysis of the global S&T landscape to support strategic planning and decisions by federal, state, and local authorities in areas such as the following:

- Prioritization of R&D investment and divestment;
- Expert finding, selecting collaborations, and partnerships; and
- Timely insight on the constantly changing targets of unwanted tech transfer.

A well-resourced S&T analysis and monitoring organization with sustained funding:

- Creates an unclassified foundation on top of which more sensitive threat work can be overlaid;
- Functions seamlessly across foreign and domestic technological challenges;
- Assembles a critical mass of resources that are hard to find due to high setup costs, such as technical infrastructure, data resources, expert technical input, and analytic talent; and
- Works to enable innovations to move from research to practice.

We need to embrace this transformative S&T landscape monitoring mission. When used in combination with "run faster" and "slow them down" policy options, it will help maintain U.S. leadership in critical emerging technologies and supply chains — now and into the future.

Thank you, and I look forward to our discussion.

Appendix A: Citation Information for the 35 "Chokepoints" Articles

Article	Citation
(1) Photolithography machines	本报记者高博 [staff reporter Gao Bo], "这些'细节'让中国难望顶级光刻机项背" ["These 'Details' Keep Top Photolithography Machines a Distant Prospect for China"], 科技日报 [*S&T Daily*], April 19, 2018, 1, 3, https://perma.cc/5DGC-8786 and https://perma.cc/BZK5-F8QE.[1]
(2) Microchips	本报记者张盖伦、付丽丽 [staff reporters Zhang Gailun and Fu Lili], "中兴的'芯'病，中国的心病" ["ZTE's Chip Problem Gives China Heart Palpitations"], 科技日报 [*S&T Daily*], April 20, 2018, 1, 3, https://perma.cc/H8XT-6Z6Q and https://perma.cc/E89F-Y9JT.
(3) Operating systems	本报记者高博 [staff reporter Gao Bo], "丧失先机，没有自研操作系统的大国之痛" ["Lost Opportunities: The Pains of a Great Power Without a Domestically Developed Operating System"], 科技日报 [*S&T Daily*], April 23, 2018, 1, https://perma.cc/DL52-V2VL.
(4) Aircraft engine nacelles	本报记者矫阳 [staff reporter Jiao Yang], "居者无其屋，国产航空发动机的短舱之困" ["No Homes of Their Own: The Nacelle Problem of Domestic Aircraft Engines"], 科技日报 [*S&T Daily*], April 24, 2018, 1, https://perma.cc/3GP8-UMDQ.
(5) Touch sensors (for industrial robots)	本报记者张佳星 [staff reporter Zhang Jiaxing], "传感器疏察，被愚钝的机器人'国产触觉'" ["An Oversight in Sensors, a 'Domestic Touch' for Dumbed-Down Robots"], 科技日报 [*S&T Daily*], April 25, 2018, 1, 4, https://perma.cc/A3JG-V8F2 and https://perma.cc/6SQ5-25TP.
(6) Vacuum evaporators	本报记者刘艳 [staff reporter Liu Yan], "真空蒸镀机匮缺：高端显示屏上的阴影" ["Vacuum Evaporator Shortage: A Shadow over High-End Displays"], 科技日报 [*S&T Daily*], April 26, 2018, 1, 3, https://perma.cc/4KMP-NE8P and https://perma.cc/ZU9A-9LAC.
(7) High-end radio frequency (RF) components	本报记者高博 [staff reporter Gao Bo], "射频器件：仰给于人的手机尴尬" ["RF Components: For Mobile Phones, an Embarrassing Reliance on Others"], 科技日报 [*S&T Daily*], May 7, 2018, 1, 4, https://perma.cc/6CJH-HRYM and https://perma.cc/5UQ2-J6CB.
(8) Primers and reagents used for iCLIP technology (for RNA manipulation)	本报记者张佳星 [staff reporter Zhang Jiaxing], "'靶点'难寻，国产创新药很迷惘" ["'Targets' Are Elusive, Leaving Domestic Production of Innovative Drugs in a Fog"], 科技日报 [*S&T Daily*], May 8, 2018, 1, 3, https://perma.cc/6JF4-4VJ5 and https://perma.cc/C9UE-M4TG.
(9) Heavy-duty gas turbines	本报记者瞿剑 [staff reporter Qu Jian], "'命门火衰'，重型燃气轮机的叶片之殇" ["'Weakness between the Kidneys'—The Blade Wounds of Heavy-Duty Gas Turbines"], 科技日报 [*S&T Daily*], May 9, 2018, 1, 4, https://perma.cc/H9SV-LDWU and https://perma.cc/WW9D-RSM8.

[1] Most of the "chokepoints" articles published by Chinese state-run newspaper *Science and Technology Daily* (*S&T Daily*, 科技日报) in 2018—profiled in the upcoming CSET report "Chokepoints: China's Self-Identified Strategic Technology Import Dependencies"—begin on page one and continue onto a subsequent page. In these cases, we provide two URLs. The first one links to a PDF of page one of the relevant issue of *S&T Daily*, a page that includes the first half of the "chokepoints" article among other articles. The second PDF is of the page of the newspaper that contains the second half of the "chokepoints" article in question.

(10) LiDAR	实习记者崔爽 [reporter intern Cui Shuang], “激光雷达昏聩，让自动驾驶很纠结” [“LiDAR Dimness Leaves Autonomous Driving in a Tangle”], 科技日报 [*S&T Daily*], May 10, 2018, 1, 3, https://perma.cc/SCA7-XVBN and https://perma.cc/KRK3-P5LA.
(11) Airworthiness standards	本报记者矫阳 [staff reporter Jiao Yang], “适航标准：国产航发又一道难迈的坎儿” [“Airworthiness Standards: Another Difficult Hurdle for Domestic Aircraft Engines”], 科技日报 [*S&T Daily*], May 11, 2018, 1, 3, https://perma.cc/669C-55H8 and https://perma.cc/FZ7U-AR3W.
(12) High-end capacitors and resistors	本报记者高博 [staff reporter Gao Bo], “没有这些诀窍，我们够不着高端电容电阻” [“Without This Know-How, High-End Capacitors and Resistors Will Remain Beyond Our Reach”], 科技日报 [*S&T Daily*], May 14, 2018, 1, 4, https://perma.cc/57QK-KFUJ and https://perma.cc/FBN7-2ADB.
(13) Electronic design automation (EDA) software	本报记者俞慧友 [staff reporter Yu Huiyou], “核心工业软件：智能制造的中国‘无人区’“ [“Core Industrial Software: China’s ‘Uncharted Territory’ in Smart Manufacturing”], 科技日报 [*S&T Daily*], 1–2, May 17, 2018, https://perma.cc/7GW3-J2T5 and https://perma.cc/4U7J-RHV9.
(14) High-end indium tin oxide (ITO) sputtering target materials	本报记者赵汉斌 [staff reporter Zhao Hanbin], “烧不出大号靶材，平板显示制造仰人鼻息” [“Unable to Sinter Large-Size Targets, Panel Display Manufacturing Depends on Others for Survival”], 科技日报 [*S&T Daily*], May 18, 2018, 1, 4, https://perma.cc/DXH8-XXGN and https://perma.cc/J9LC-RTL4.
(15) Core algorithms (for robotics)	本报记者杨仑 [staff reporter Yang Lun], “算法不精，国产工业机器人有点‘笨’“ [“With Inept Algorithms, Domestically Produced Robots Are a Bit ‘Slow’“], 科技日报 [*S&T Daily*], May 22, 2018, 1, 3, https://perma.cc/QP2T-RBCN and https://perma.cc/EY6D-UWJP.
(16) Aviation-grade steel (for landing gear)	本报记者孙玉松 [staff reporter Sun Yusong], “航空钢材不过硬，国产大飞机起落失据” [“Weak in Aviation-Grade Steel, Large Domestic Aircraft Lack Support for Takeoff and Landing”], 科技日报 [*S&T Daily*], May 23, 2018, 1–2, https://perma.cc/PT8S-6AKK and https://perma.cc/73ST-RYWR.
(17) Milling cutters	本报记者华凌 [staff reporter Hua Ling], “为高铁钢轨‘整容’，国产铣刀难堪重任” [“For High-Speed Railway Track ‘Facelifts,’ Domestic Milling Cutters Are Not Up to the Task”], 科技日报 [S&T Daily], May 24, 2018, 1, https://perma.cc/W4VP-4YAR.
(18) High-end bearing steel	本报记者王延斌 [staff reporter Wang Yanbin], “高端轴承钢，难以补齐的中国制造业短板” [“High-End Bearing Steel, a Difficult Shortcoming for Chinese Manufacturing to Overcome”], 科技日报 [*S&T Daily*], May 25, 2018, 1, https://perma.cc/26AR-FFKY.
(19) High-pressure piston pumps (for hydraulic machinery)	本报记者王海滨、通讯员王玉芳 [staff reporter Wang Haibin and correspondent Wang Yufang], “高压柱塞泵，鲠在中国装备制造业咽喉的一根刺” [“High-Pressure Piston Pumps: A Thorn in the Side of China’s Equipment Manufacturing Industry”], 科技日报 [*S&T Daily*], May 28, 2018, 1, 3, https://perma.cc/XA2S-QBGQ and https://perma.cc/WV9R-NN3Q.
(20) Aviation design software	本报记者张晔 [staff reporter Zhang Ye], “航空软件困窘，国产飞机设计戴上‘紧箍咒’“ [“Aviation Software Plight Has Domestic Aircraft Design under a ‘Skull-Squeezing Curse’“], 科技日报 [*S&T Daily*], May 30, 2018, 1, 3, https://perma.cc/RU6C-MTQS and https://perma.cc/U9HU-YC5V.
(21) High-end photoresists (for photolithography)	本报记者过国忠 [staff reporter Guo Guozhong], “中国半导体产业因光刻胶失色” [“China’s Semiconductor Industry Losing Its Luster Due to Photoresists”], 科技日报 [*S&T Daily*], May 31, 2018, 1, 3, https://perma.cc/MYL5-PYGZ and https://perma.cc/KD25-QMZW.

(22) High-pressure common rail direct fuel injection systems (for low-emission diesel engines)	本报记者江东洲、刘昊 [staff reporters Jiang Dongzhou and Liu Hao], “高压共轨不中用，国产柴油机很受伤” [“When High-Pressure Common Rail Is No Good, Domestic Diesel Engine Production Suffers”], 科技日报 [*S&T Daily*], June 4, 2018, 1, 4, https://perma.cc/T7JN-4GU7 and https://perma.cc/R83U-KFA4.
(23) Transmission electron microscopes (TEM)	本报记者张佳星 [staff reporter Zhang Jiaxing], “我们的蛋白质3D高清照片仰赖舶来的透射式电镜” [“High-Definition 3D Photographs of Our Proteins are Dependent on Foreign Transmission Electron Microscopes”], 科技日报 [*S&T Daily*], June 6, 2018, 1, 4, https://perma.cc/HX2Z-BF6V and https://perma.cc/6YPW-346K.
(24) Main bearings for tunnel boring machines (TBM)	本报记者矫阳 [staff reporter Jiao Yang], “自家的掘进机却不得不用别人的主轴承” [“Chinese-Made Tunnel Boring Machines Have to Use Main Bearings from Others”], 科技日报 [*S&T Daily*], June 7, 2018, 1, 3, https://perma.cc/SD3Z-E622 and https://perma.cc/QJA5-WMUM.
(25) Microspheres	本报记者高博 [staff reporter Gao Bo], “微球：民族工业不能承受之轻” [“Microspheres: The Unbearable Lightness of National Industry”], 科技日报 [*S&T Daily*], June 12, 2018, 1, 3, https://perma.cc/TF8V-L8ZX and https://perma.cc/P27W-8LSP.
(26) Underwater connectors	本报记者陈瑜 [staff reporter Chen Yu], “水下连接缺国产利器，海底观测网傍人篱壁” [“With No Domestic Producers of Underwater Connectors, Seafloor Observation Network Depends on Others”], 科技日报 [*S&T Daily*], June 13, 2018, 1, 4, https://perma.cc/K8ZS-6JWZ and https://perma.cc/G93B-6SH6.
(27) Key materials for fuel cells	本报记者张盖伦 [staff reporter Zhang Gailun], “少了三种关键材料，燃料电池商业化难成文章” [“Without Three Key Materials, Fuel Cell Commercialization Will Be Hard to Achieve”], 科技日报 [*S&T Daily*], June 14, 2018, 1, 3, https://perma.cc/EQ5E-GYGV and https://perma.cc/6NAR-HB27.
(28) High-end welding power sources (for underwater welding robots)	本报记者叶青、龙跃梅 [staff reporters Ye Qing and Long Yuemei], “国产焊接电源‘哑火’，机器人水下作业有心无力” [“Domestic Production of Welding Power Sources ‘Misfires,’ Frustrating Underwater Robot Operations”], 科技日报 [*S&T Daily*], June 20, 2018, 1, 4, https://perma.cc/UZG7-NBU7 and https://perma.cc/47XR-D898.
(29) Lithium battery separators	本报记者孙玉松 [staff reporter Sun Yusong], “一层隔膜两重天：国产锂电池尚需拨云见日” [“One Layer of Separators, Two Very Different Environments: Domestic Lithium Battery Production Still Waiting for the Clouds to Part”], 科技日报 [*S&T Daily*], June 21, 2018, 1, 3, https://perma.cc/DN9Q-C6T6 and https://perma.cc/42QZ-EYNV.
(30) Components for medical imaging equipment	本报记者张佳星 [staff reporter Zhang Jiaxing], “拙钝的探测器模糊了医学影像” [“Dull Detectors Blur Medical Imaging”], 科技日报 [*S&T Daily*], June 25, 2018, 1, 4, https://perma.cc/H62R-UUH7 and https://perma.cc/6SZ3-XU3T.
(31) Ultra-precision polishing techniques	本报记者张景阳 [staff reporter Zhang Jingyang], “通往超精密抛光工艺之巅，路阻且长” [“In Ultra-Precision Polishing Techniques, the Road to the Top is Long and Rocky”], 科技日报 [*S&T Daily*], June 26, 2018, 1, 3, https://perma.cc/N6V6-FETT and https://perma.cc/LLZ2-2G7H.
(32) Epoxy (for high-end carbon fiber)	本报记者李禾 [staff reporter Li He], “环氧树脂韧性不足，国产碳纤维缺股劲儿” [“Insufficient Resiliency in Epoxy Means Domestic Carbon Fiber Lacks Strength”], 科技日报 [*S&T Daily*], June 27, 2018, 1, 4, https://perma.cc/2TVR-8PZK and https://perma.cc/SU6R-E4Y5.

(33) High-strength stainless steel (for rocket engines)	本报记者付毅飞、实习记者于紫月 [staff reporter Fu Yifei and reporter intern Yu Ziyue], "去不掉的火箭发动机'锈疾'" ["The Intractable 'Rust Disease' of Rocket Engines"], 科技日报 [*S&T Daily*], June 28, 2018, 1, 3, https://perma.cc/KH74-9FKL and https://perma.cc/TTV7-CY7R.
(34) Database management systems	本报记者高博 [staff reporter Gao Bo], "数据库管理系统：中国还在寻找'正确打开方式'" ["Database Management Systems: China still Looking for the 'Right Way to Open'"], 科技日报 [*S&T Daily*], July 2, 2018, 1, 4, https://perma.cc/MDR9-JJCG and https://perma.cc/3ZEP-2DZX.
(35) Scanning electron microscopes (SEM)	实习记者陆成宽 [reporter intern Lu Chengkuan], "扫描电镜'弱视'，工业制造难以明察秋毫" ["Scanning Electron Microscope 'Visual Impairment' Makes Minute Observation Difficult for Industrial Manufacturing"], 科技日报 [*S&T Daily*], July 3, 2018, 1, 3, https://perma.cc/VWV2-AFDP and https://perma.cc/9LVG-V9ES.

Appendix B: Recommended Reading

Zachary Arnold and Melissa Flagg, "A New Institutional Approach to Research Security in the United States" (Center for Security and Emerging Technology, January 2021). https://cset.georgetown.edu/publication/a-new-institutional-approach-to-research-security-in-the-united-states/

Tarun Chhabra, William Hannas, Dewey Murdick, and Anna Puglisi, "Open-Source Intelligence for S&T Analysis" (Center for Security and Emerging Technology, September 2020). https://cset.georgetown.edu/publication/open-source-intelligence-for-st-analysis/

CSIS Technology and Intelligence Task Force, "Maintaining the Intelligence Edge: Reimagining and Reinventing Intelligence through Innovation" (Center for Strategic and International Studies, January 2021). https://www.csis.org/analysis/maintaining-intelligence-edge-reimagining-and-reinventing-intelligence-through-innovation

Ryan Fedasiuk, Emily Weinstein, and Anna Puglisi, "China's Foreign Technology Wish List" (Center for Security and Emerging Technology, May 2021). https://cset.georgetown.edu/publication/chinas-foreign-technology-wish-list/

Melissa Flagg and Paul Harris, "System Re-engineering: A New Policy Framework for the American R&D System in a Changed World" (Center for Security and Emerging Technology, September 2020). https://cset.georgetown.edu/publication/system-re-engineering/

William Hannas and Huey-Meei Chang, "China's STI Operations" (Center for Security and Emerging Technology, January 2021). https://cset.georgetown.edu/publication/chinas-sti-operations/

Will Hunt, "Sustaining U.S. Competitiveness in Semiconductor Manufacturing" (Center for Security and Emerging Technology, January 2022). https://cset.georgetown.edu/publication/sustaining-u-s-competitiveness-in-semiconductor-manufacturing/

Ben Murphy, "Chokepoints: China's Self-Identified Strategic Technology Import Dependencies" (Center for Security and Emerging Technology, May 2022). Forthcoming

Alex Rubin, Alan Omar Loera Martinez, Jake Dow, and Anna Puglisi "The Huawei Moment" (Center for Security and Emerging Technology, July 2021). https://cset.georgetown.edu/publication/the-huawei-moment/

Wang Jisi, Zhao Jianwei, Hu Ran, Zhang Chengyang, and Zhang Yike, "Sino-U.S. Strategic Competition in the Technology Domain: Analysis and Outlook" (Institute for International and Strategic Studies at Peking University, January 2022). http://cn3.uscnpm.org/model_item.html?action=view&table=article&id=27016

STATEMENT OF HON. NAZAK NIKAKHTAR, PARTNER, WILEY REIN LLP; FORMER ASSISTANT SECRETARY FOR INDUSTRY AND ANALYSIS, U.S. DEPARTMENT OF COMMERCE

Ms. NIKAKHTAR. Thank you, Dewey.

Senators, Committee Members, and staff, thank you for the opportunity to speak today. And thanks for everything that you do for America.

As a lawyer, economist, law school professor, and former government official. I've been on the front lines of the China economic challenge for decades. I set up the China/Non-Market Economy office at the Commerce Department nearly 20 years ago and audited Chinese companies for the U.S. Government. Recently, I served as both Assistant Secretary for Trade and CFIUS and Acting Undersecretary for Export Controls. Now back in private practice, I represent global industries that are fighting back against predatory practices that are weakening critical supply chains.

It is from all of these vantage points that I offer my views today. These views and opinions expressed are mine only.

In my written testimony, I described China's deliberate predatory tactics to weaken the economies of the United States and our allies. To be clear, this is not an issue of trade or protectionism. China has publicly stated that its goal is to weaken U.S. and other countries' supply chains to the point where we are helpless. Obviously, we need a strategy that protects ourselves from harm. We've seen China's stranglehold over its trading partners in Africa, Latin America and South America through the One Belt/One Road debt trap. How do we avoid a similar fate? Through the rigorous use of our laws and the creation of new laws where there are gaps.

First and foremost, we absolutely need outbound investment reviews that are currently absent from law. Joint ventures, as you heard, are happening all the time in China where U.S. companies are collaborating with the Chinese military to develop dangerous technologies and manufacturing know-how, when technology is developed abroad that falls outside of export control jurisdiction. Plus, the movement of supply chains outside of the United States to adversary nations is generally unregulated, like critical lifesaving medical equipment. Without medicine and supply chains to build our defense systems, how will we survive under attack? This gives our adversaries the ultimate trump card.

Second, we need an export control system configured to allow us to run faster, while at the same time blocking China's ability to benefit from our technology. China's military advancements in hypersonic weapons were facilitated by the transfer of U.S. technology. One company's short-term profits years ago now threatens global security. Our export system failed. We need to fix it.

Third, we need to control the export of sensitive data that can be weaponized by our adversaries to conduct massive surveillance and develop dangerous AI-enabled weapons. Data transfer needs to be regulated through new laws on export controls; so does sensitive research at universities.

Fourth, when we authorize the transfer of sensitive technology to China through export licenses, supercomputer enabling technology, for instance. Today we can't even be sure that our technology is not being used for military purposes when it goes to China and not

being used for weapons of mass destruction. This is because China restricts our ability to conduct end-use checks—and has for a long time in China. That's a big problem if we're allowing exports of critical technology to China today.

Fifth, we need national security reviews of Greenfield investments. If you heard, through the CFIUS process, China buys land here and conducts surveillance, connects to our energy grid, accesses our control technology from within our own borders, and wipes out our domestic industries by underpricing from within our own borders. This is a problem.

Sixth, any revenue loss from sales to China through export restrictions, make no mistake, can be regained from investing domestically and in our allies' markets. We need investments and safe locations to strengthen our supply chains. Consider the U.S. to be an emerging market, not China.

Seventh, we need laws to address China's additional trade-distortive practices where we currently have no laws. Overcapacity in fiber optic cables—this is the infrastructure of 5G and China's running overcapacity. The economic harm caused to businesses from cyberattacks and the displacement of businesses from global markets due to China's predatory pricing behavior around the world.

To address this, we need additional Section 301 investigations into these practices to recoup the economic loss to U.S. businesses resulting from these harms. If the investigations result in tariffs, then we ought to shift the tariff responsibility onto the Chinese exporter and away from American importers. Americans should not be paying for China's predatory behavior.

And finally, we should use the 301 tariffs collected to create an innovation fund dedicated to capitalizing high technology in critical industries. In other words, use the tariff revenue paid by China to build out our critical supply chains.

In sum, remember, the more we invest in China's non-market economy, the more we move production to China to avail ourselves of its cheap prices, forced labor, and other non-market distortions. The more we buy cheap Chinese products rather than goods from market economies, the more we allow distorted, non-market forces to capture a greater share of the global market. In this way we are accelerating the demise of capitalism and the market based system. We need to reverse this.

Thank you and I look forward to your questions.

[The prepared statement of Ms. Nikakhtar follows:]

May 11, 2022

Statement of Hon. Nazak Nikakhtar

Partner, International Trade and National Security Practice Chair, Wiley Rein LLP
Former Assistant Secretary for Industry & Analysis, Under Secretary for Industry & Security*
U.S. Department of Commerce

Testimony Before the Senate Select Committee on Intelligence*

Threats to U.S. National Security:
Countering the PRC's Economic and Technological Plan for Dominance

Senator Warner and Senator Rubio, Committee experts, policy advisors, and staff, thank you for the opportunity to speak about the growing challenges posed by the People's Republic of China ("PRC") to U.S. and global national security and economic security interests, and the appropriate U.S. Government response.

My name is Nazak Nikakhtar, and it is an honor to appear before you today. I am an international trade attorney and Chair of the National Security practice at the Washington, DC, law firm of Wiley Rein LLP. I am also a trade and industry economist, a former Georgetown University adjunct law professor, and recently completed my second tour of duty in the U.S. Government. Twenty years ago, I began my career as an analyst at the Department of Commerce's Bureau of Industry and Security and subsequently at the International Trade Administration, where my colleagues and I witnessed from the frontlines the predatory economic tactics used by our trading partners to erode our industries. In 2004, I helped establish and lead the Commerce Department's China/Non-Market Economy Office and, for several years thereafter, I audited numerous foreign (including Chinese) companies and their affiliates for the Department. In 2018, I returned to the Commerce Department to serve as Assistant Secretary for Industry & Analysis and, in 2019, I simultaneously served, performing the non-exclusive functions and duties, as the

**Performing the non-exclusive functions and duties of Under Secretary while also serving as Assistant Secretary.*

The views and opinions expressed in this testimony are mine only and do not represent the views of Wiley Rein LLP or any of the firm's clients.

Under Secretary for the Bureau of Industry and Security. It is from all of these vantage points that I offer my testimony and observations today about the risks to U.S. national and economic security, as well as the gaps in U.S. laws that must be closed to adequately mitigate these risks. There are many.

I. THE EROSION OF SUPPLY CHAINS AND THE RESULTING ECONOMIC AND NATIONAL SECURITY THREATS

Only recently, in 2017, the U.S. Government began to aggressively confront the challenges posed by the PRC's predatory economic practices. These challenges had been ignored for decades and, as a result, over the course of the past 40-plus years, the United States continuously lost capabilities in sector after sector in manufacturing, technology, and services that are essential to our national security. In goods alone, the offshoring of manufacturing has created supply chain vulnerabilities across hundreds of critical products, ranging from semiconductor and electronics manufacturing to the development of active pharmaceutical ingredients. This has led to job losses of between 3.4 to 3.7 million between 2001 to 2018.[1] In key sectors such as communications equipment, electronics, and computer technology, we ceded up to 40% to 60% of the domestic market share to Chinese imports, and globally the PRC has captured extensive market shares in those sectors as well.

Let me be clear on two key points. First, these are not incidental consequences of open and free trade. These are the very perverse and adverse consequences of one country exploiting open borders to cripple other nations' economies. Our economic losses have resulted from the PRC's deliberate attempts to hollow out our industries in order to create dependency on their own

---

[1] Robert Scott and Zane Mokhiber, *Growing China Trade Deficit Cost 3.7 Million American Jobs Between 2001 and 2018*, Economic Policy Institute (Jan. 30, 2020), available at https://www.epi.org/publication/growing-china-trade-deficits-costs-us-jobs/.

distorted market. The weaker our industries become – semiconductors, telecommunications, critical minerals and rare earth elements, high-capacity batteries, and pharmaceuticals and medical equipment – the more our national security is at risk.[2] Without access to secure supply chains, we are unable to sustain our economies, and we are unable to develop the weapon systems necessary for national defense. The result is that our military will have a "one strike" capability. This is also true for our allies and the rest of the world.

Second, the economic facts before us should make abundantly clear that the PRC government has waged an economic war against the rest of the world aimed at eroding non-Chinese supply chains so that no country is able to depend on itself or its allies for the essential items it needs. The PRC's end game is to render the rest of the world dependent on it, and today this plan is succeeding. At present, we depend on the PRC for 80% of our critical minerals,[3] 20-23% of our semiconductor chips (92% on Taiwan for our most advanced chips),[4] 60% of our consumer electronics including telecommunications equipment,[5] 75% of our lithium-ion battery cells,[6] and 100% for many of our pharmaceuticals and medical supplies. The greater our dependence grows, the more vulnerable and fragile we become. This is not a sound strategy.

---

[2] President Biden's 2021 supply chain Executive Order lists these critical sectors. *Executive Order on America's Supply Chains*, The White House (Feb. 24, 2021), available at https://www.whitehouse.gov/briefing-room/presidential-actions/2021/02/24/executive-order-on-americas-supply-chains/.

[3] *A Federal Strategy to Ensure Secure and Reliable Supplies of Critical Minerals*, U.S. Department of Commerce (2019), available at https://www.commerce.gov/sites/default/files/2020-01/Critical_Minerals_Strategy_Final.pdf.

[4] *Strengthening the Global Semiconductor Supply Chain in an Uncertain Era*, Boston Consulting Group and Semiconductor Industry Association (Apr. 2021) at 5, 35, available at https://www.semiconductors.org/wp-content/uploads/2021/05/BCG-x-SIA-Strengthening-the-Global-Semiconductor-Value-Chain-April-2021_1.pdf ("BCG/SIA 2021 Report"); *Taking Stock of China's Semiconductor Industry*, Semiconductor Industry Association (July 13, 2021), available at https://www.semiconductors.org/taking-stock-of-chinas-semiconductor-industry/.

[5] BCG/SIA 2021 Report at 28.

[6] Gavin Thompson, *Batteries with Chinese Characteristics*, Wood Mackenzie (Feb. 10, 2021), available at https://www.woodmac.com/news/opinion/batteries-with-chinese-characteristics/; *Protecting Americans' Sensitive Data From Foreign Adversaries, Exec. Order No. 14034 of June 9, 2021*, 86 Fed. Reg. 31,423 (June 11, 2021), available at https://www.govinfo.gov/content/pkg/FR-2021-06-11/pdf/2021-12506.pdf.

To be clear, we have not yet felt the full adverse effect the PRC's control over our supply chains and economies yet. Not because control does not exist, but rather because the PRC government has chosen not to exercise it yet. When will that time come? When the PRC knows that we are too weak to respond – perhaps when it displaces the U.S. dollar from the global currency market, or when it fully indigenizes leading-edge semiconductor development such that it no longer needs U.S. technology. This time horizon is only a few years away. This is becoming an immediate threat.

As a nation, we tend to downplay these risks because we steadfastly hold onto the belief that the United States' economy is strong and resilient, and so it will be immune from external threats. The prevailing argument – that U.S. purchasing power will continue to keep the PRC dependent on the United States and prevent it from harming U.S. interests – is terribly misinformed. We source from the PRC not because we choose to but because we have little other option. Today's economic reality is that United States and the rest of the world have absolutely no choice but to import heavily from the PRC because this is where supply chains for the most critical products reside. The current trade deficit with the PRC, which stood at $355.3 billion in 2021, underscores this point.[7] The coronavirus pandemic highlighted supply chain reality. And the farther our supply chains migrate into the PRC, the greater our dependence will become.

As our import dependence on PRC-origin goods expands, we need consider the following question: Will the PRC government guarantee to the rest of the world fair and equitable access to its supply chains? The answer is a definitive "NO." We have already witnessed instances of the PRC's stranglehold over its trading partners. For example, the debt-trap deliberately created by

---

[7] The deficit with China increased $45.0 billion to $355.3 billion in 2021. Exports increased $26.6 billion to $151.1 billion and imports increased $71.6 billion to $506.4 billion. *U.S. International Trade in Goods and Services, December 2021*, U.S. Department of Commerce Bureau of Economic Analysis (Feb. 8, 2022), available at https://www.bea.gov/news/2022/us-international-trade-goods-and-services-december-2021.

the PRC's One Belt One Road scheme where African and South American countries, who were once lured by the PRC government's promises for substantial investment, have now been forced to give up their most valuable national assets (*e.g.*, mines, roads, and ports) in repayment.[8] These countries are now at the PRC government's mercy and, so far, their only recourse is to ask the United States and other countries for assistance. We – the United States, our North America allies, European and Asian partners – are all nearing this dangerous tipping point as well.

For those of us who have studied the PRC in-depth for decades, this is precisely the PRC government's end game: to deplete other nations of the resources necessary for self-defense by creating supply chain weaknesses and economic dependence. This PRC strategy, coupled with reports of the PRC government's endless intimidation of Taiwan, Japan, Australia, South Korea, and Lithuania, and the government's repeated threats of military attacks against the United States and its allies must make absolutely clear that we are not dealing with a friendly nation. The PRC government is a threat, and both the Trump and Biden Administrations have designated the PRC government as a "foreign adversary" along with the governments of the Republic of Cuba, the Islamic Republic of Iran, the Democratic People's Republic of Korea, the Russian Federation, and Venezuela's Nicolás Maduro Regime.[9] This designation means something.

To be clear, the United States, Europe, and the rest of the world are already in a very vulnerable position with respect to critical minerals and semiconductors supply chains. Without access to these goods, we have very little leverage over the PRC government, and our military capabilities are severely limited. This, then, leads to the obvious question: if the PRC government

---

[8] Jeremy Mark, *China's Real 'Debt Trap' Threat*, Atlantic Council (Dec. 13, 2021), available at https://www.atlanticcouncil.org/blogs/new-atlanticist/chinas-real-debt-trap-threat/.

[9] *Securing the Information and Communications Technology and Services Supply Chain*, 86 Fed. Reg. 4,909, 4,911 (Dep't Commerce Jan. 12, 2021), available at https://www.govinfo.gov/content/pkg/FR-2021-01-19/pdf/2021-01234.pdf.

were to restrict global access to its critical mineral exports, as well as its own and Taiwan's semiconductor supply chains, what would be the economic impact and how would we respond?

The economic impact to the United States will be in the trillions. Compounded by the economic impact across the rest of the world – the result will be catastrophic. Almost everything we manufacture or consume today, and all of our technological advancements, depend in some way on Chinese-processed critical minerals or Chinese and Taiwanese semiconductor supply chains. Without access to these materials, the global economy will come to an abrupt halt.

As to how we would respond, our response would be ineffective. Realistically, it will take a minimum of three to five years to scale production of critical minerals mining, extraction, and processing capabilities to wean dependence off the PRC. Additionally, it will take at least 10 to 20 years to recreate the vast semiconductor ecosystem that currently exists in the PRC and Taiwan, including the development of upstream raw material and chemical supply chains, as well as the back end assembly/testing/packaging capabilities, which are presently concentrated in the PRC and Taiwan.[10] During this transition period, our countries are vulnerable.

This is the point that most policymakers fail to realize. The PRC is leveraging its near monopoly over critical global supply chains to secure its ambitions for economic and military hegemony. We need to quickly reverse our vulnerabilities, and I urge the Commission and Congress to act before it becomes too late.

II. THE UNITED STATES MUST RETHINK ITS APPROACH TO NATIONAL SECURITY AND TRADE LAWS

For years, I have described the predatory economic tactics that the PRC government has systematically used to weaken our industries and economy, and I have often stressed that we do

---

[10] BCG/SIA 2021 Report at 19.

not adequately leverage our laws to counter these security threats. Appended hereto is my prior testimony on this topic. Today, however, my goal is to offer perspectives on how to cure our vulnerabilities in order to better protect our economies and technologies. The recommendations I provide may not all be easy. They will require sacrifices. But if we, as a nation, are resolute, we may be able to solve our weaknesses before it is too late.

Success will depend on open trade and reliance on the comparative advantages of the United States and our allies. Success will depend on our ability to work together to reconfigure supply chains out of the PRC. And success will depend on forging greater economic ties between like-minded partner countries. For the United States, the economic impact of moving our supply chains out of the PRC is approximately 1% of U.S. gross domestic product in the short-run. If we do this in concert with our European, Japanese, and South Korean allies, the economic impact is significantly lessened. After three to five years, any negative economic impact will turn into substantial gains for the United States and those gains will grow significantly. Overall, the benefit to the free world of disentangling from a predatory actor will be immeasurable.

A. Deterring Invasion of Taiwan

At the outset, one of the most immediate threats to global security is the PRC government's potential move on Taiwan, whether by military force, legal decree, or another mechanism. The PRC government's objective in obtaining control over Taiwan is to gain control over the island's semiconductor and electronics industries, and thereby gain almost absolute control over the global economy. In other words, control over Taiwan will allow the PRC government to bring the global economy to its knees.

Importantly, however, the United States still controls one of the most powerful weapons of the global economic order – the U.S. dollar. The dollar's special status as the global currency gives our nation unrivaled sanctioning power. Given that access to dollars is a near-necessity for

multinational businesses and global financial institutions, the United States is able to impose significant economic damage by denying certain entities or governments access to the dollar. Indeed, the sanctions that are currently pummeling the Russian currency, banks, and the internal economy are a vivid demonstration of the power of the U.S. dollar. Coupled with sweeping European sanctions, the United States and its allies are capable of imposing significant costs to the PRC economy through comprehensive financial sanctions on PRC banks should it take control of Taiwan.

It should be noted that the PRC government is now hastening efforts to reduce reliance on the U.S. dollar to protect itself from potential U.S. sanctions. It is simultaneously working to displace the dollar from serving as the global currency in favor of the Yuan. But it will take years for the Yuan to gain any significant foothold in the global economy. Until then, and while the dollar still maintains substantial influence, the U.S. Government should be prepared to use this economic lever as deterrence.

B. The U.S. Government Needs A Legal Mechanism to Recognize PRC Entities' Ties to the Central Government

Over the course of the past 10 years, the PRC government has steadily increased its control over Chinese companies. And by doing so, it has coerced companies to aid the central government in growing its military base, technological capabilities, and surveillance activities. It is well documented that the PRC government mandates and coerces – through law, administrative guidelines, and regulations – entities to transfer sensitive information, trade secrets, and intelligence information to the central government. In addition, PRC laws require that entities conform their practices to advance the Chinese Communist Party's ("CCP") military and

surveillance interests.[11] Moreover, the PRC's Military-Civil Fusion strategy demands that entities cooperate with the People's Liberation Army ("PLA") to advance the military strength and ambitions of the PRC government for global power. All Chinese entities, even those enterprises that still remain ostensibly private and civilian, are legally obligated to serve the state and the leadership of the central government such that Chinese entities have limited autonomy over their business decisions. The PRC government's routine installation of CCP officials inside private firms ensures compliance with the party's mandates.

The reality today is that Chinese entities operate in a military-driven ecosystem that is centrally coordinated by the CCP to advance the country's weapons capabilities, intelligence operations, and security apparatuses. The legal framework through which the PRC government forces entities to contribute to the modernization and expansion of the CCP's military industrial complex continues to expand rapidly and, therefore, poses a significant threat to the national security, foreign policy, and economy of the United States.

In light of the foregoing, it is surprising that the U.S. Government does not have a consistent legal framework across all federal agencies for finding affiliation between Chinese commercial entities and the PRC central government. In fact, it never has. Crippled by this lack of comprehensive legal framework, the U.S. intelligence community has been hampered in both its offensive and defensive capabilities, the U.S. Department of Defense is limited in the types of companies it can eliminate from supply contracts, and U.S. Government agencies are unable to

---

[11] USCBC, *Fact Sheet: Communist Party Groups in Foreign Companies in China*, China Business Review (May 31, 2018), available at https://www.chinabusinessreview.com/fact-sheet-communist-party-groups-in-foreign-companies-in-china/.

legally prohibit procurement from CCP affiliates or prohibit U.S. investments in PLA affiliates.[12] However, if the U.S. Government had an actual legal framework to determine whether companies are (1) controlled by the PRC government, or (2) affiliated with the PRC government, it could do more to protect U.S. industries, economy, and national security from their malign activities.

Accordingly, U.S. Government should develop a comprehensive, consistent, and complementary legal standard for evaluating the extent to which commercial and non-commercial PRC entities are controlled by or affiliated with their provincial or central governments. The lack of framework has, to date, significantly impeded the U.S. Government's analysis in export controls, foreign direct investment screenings (discussed further below), intelligence community risk assessments, federal government acquisitions, and supply chain vulnerability analyses. This shortcoming ought to be remedied, and the solution is quite simple. Congress should, by legislation, adopt the longstanding legal definitions of affiliation that exist in U.S. trade laws, through statute, regulations, and case precedent, and apply these definitions to augment the legal authorities currently existing across all federal agencies. The trade laws extend the definition of affiliation beyond ownership interests to the broad range of ways in which foreign governments are able to exercise influence over corporate entities' business operations such that the entities lose autonomy over key decisions. These trade laws have been upheld by U.S. courts for decades, are consistent with the United States' obligations under the World Trade Organization ("WTO") agreements, and will therefore withstand judicial scrutiny. It is axiomatic that the application of a comprehensive legal standard such as this would improve each federal agency's ability to maximize the use of its own existing authorities where a determination of affiliation is needed.

---

[12] *E.g.*, through the U.S. Department of the Treasury's Chinese Military Industrial Complex companies. *See Non-SDN Chinese Military-Industrial Complex Companies List (NS-CMIC List)*, U.S. Department of the Treasury (Dec. 16, 2021), available at https://home.treasury.gov/policy-issues/financial-sanctions/consolidated-sanctions-list/ns-cmic-list.

Further, a consistent legal approach such as this would promote uniformity and predictability across the U.S. Government agencies' legal authorities and provide better clarity to businesses seeking regulatory approvals from various agencies.

C. The United States and Its Allies Should Rely More Heavily on Export Controls

The PRC's growth has been driven in significant part by U.S. companies as well as firms in allied nations racing to transfer technology to Chinese counterparts – many of which are controlled by the PRC government – in exchange for temporary access to the PRC market. The fact that the PRC government restricts access to its domestic market in exchange for technology transfer to individual companies confirms the extensive collusion and connection between PRC companies and their central government.

This technology-transfer trend has accelerated over the course of the past two decades and has resulted in so much technology transfer to the PRC that the PRC is now technologically neck-in-neck with the United States in many important sectors (*e.g.*, telecommunications and computers), and vastly ahead in others (*e.g.*, hypersonic weapons, artificial intelligence, genomics, and robotics). This is incredibly alarming. In order to solve this problem, we need to revise our current strategy.

1. The Need for a "Block" and "Run Faster" Approach

At the outset, the United States' export control community has traditionally pursued a competition strategy of "run faster" when it comes to developing export control policies.[13] The theory behind this strategy is that, by permitting exports of critical technologies to PRC entities, U.S. firms will gain access to the revenue needed in order to invest in next-generation technologies and stay ahead in the technology race. But this strategy has failed over the years. Although it

[13] It is important to emphasize that export controls are not prohibitions on exports per se. They simply subject exports to a license review process.

takes our firms years, even decades, to develop new technologies, we are handing over these technologies to the PRC virtually overnight, allowing them to bypass the extended technology-development lead times and costs (including trial-and-error) that innovators endure. In other words, our strategy has been to place the painstaking technology development burden on our own businesses, and then allow the rapid transfer of the resulting technology to adversaries enabling them to "run faster" than us. Two examples demonstrate the danger of the 'tech transfer for revenue' approach.

ASML is the Dutch photolithography company that developed the highly-advanced and one-of-a-kind extreme ultraviolet ("EUV") lithography tool that produces the most leading edge semiconductors in existence today. This tool was developed, in part, using U.S.-controlled technology. ASML is the only firm in the world that is capable of making these sophisticated machines,[14] and it has taken ASML 20 years to develop this tool with billions of dollars in investments.[15] If the PRC semiconductor industry were to acquire this machine, it would be able to reverse engineer it in three years, giving it a substantial boost in semiconductor development and solidify its position as a global leader. Indeed, the PRC semiconductor industry in 2020 surpassed Taiwan for the second year in a row in global semiconductor chip sales.[16] With this added EUV capability, along with the downstream assembly/packaging/testing ecosystem that the

---

[14] Sam Shead, *Investors are Going Wild Over a Dutch Chip Firm, And You've Probably Never Heard of It*, CNBC (Nov. 24, 2021), available at https://www.cnbc.com/2021/11/24/asml-the-biggest-company-in-europe-youve-probably-never-heard-of.html.

[15] Matthew Gooding, *ASML Might Be The Most Successful Tech Company You've Never Heard Of*, Tech Monitor (Aug. 6, 2021), available at https://techmonitor.ai/technology/future-of-asml-photolithography-semiconductor-chip-euv.

[16] *China's Share of Global Chip Sales Now Surpasses Taiwan's, Closing In on Europe's and Japan's*, Semiconductor Industry Association (Jan. 10, 2022), available at https://www.semiconductors.org/chinas-share-of-global-chip-sales-now-surpasses-taiwan-closing-in-on-europe-and-japan/.

PRC government has developed, the PRC will be positioned to dominate the global chip industry likely by 2025.[17]

In comparison, the United States is lagging behind; we do not have the capability to produce all of the semiconductors required for our defense capabilities, let alone a substantial portion of our economy. We produce neither all of the upstream raw materials necessary to manufacture the chips, nor do we maintain an assembly/packaging/testing ecosystem to operationalize the chips. This is the fundamental problem. It will take 10 to 20 years to rebuild an on-shore and complementary near-shore semiconductor ecosystem to cure the United States' and our allies' dependence on the PRC and Taiwan. The PRC, by contrast, is only a few years away from independence.

The second example is the well documented PLA's advancements in hypersonic weapons, which was facilitated by the transfer of U.S. semiconductor technology to the PRC. To be clear, one U.S. company's technology transfer allowed the PRC military to race ahead of the United States, and that company's realized short-term profits now threatens our national security and the world's security.

Clearly, we need a different strategy – one that both blocks technology transfer and allows us to run faster. This means that we need more aggressive export controls on transfers of critical technology through the denial of export licenses to adversaries in the PRC. We also need to augment investments in U.S. innovation, as discussed further below.

---

[17] Tim De Chant, *The Chip Choke Point*, The Wire China (Feb. 7, 2021), available at https://www.euvlitho.com/Blogs/The%20Chip%20Choke%20Point%20-%20The%20Wire%20China.pdf; Robert Castellano, *3 Headwinds Facing ASML's Non-EUV Business in China*, Seeking Alpha (Mar. 22, 2021), available at https://seekingalpha.com/article/4415477-three-headwinds-facing-asml-s-non-euv-business-in-china, Misha Lu, *Is Huawei Making its Own Lithography Equipment*, Tech Taiwan (June 9, 2021), available at https://techtaiwan.com/20210609/huawei-duv/.

2. Controls on Emerging Technologies

Although the Export Control Reform Act of 2018 ("ECRA") legislated the protection of "emerging technologies" through the use of export controls,[18] the debate continues in the U.S. Government as to the most effective way to implement ECRA's mandates and restrict such exports. At the outset, there is widespread recognition that emerging technologies are most vulnerable to foreign acquisition when they are at the nascent stages of development. Congress recognized this reality when it used the term "emerging" in ECRA. Indeed, at the nascent stage of development, the full range of applications that may arise from new technologies are seldom identified. Because Congress recognized this uncertainty, it instituted regulatory controls over their exports given that the same technologies that wield the power to drive significant advancements in the commercial sector may also be exploited for both known and yet-to-be known dangerous uses by foreign adversaries. Artificial Intelligence is a perfect example of this intersection.

My understanding is that the U.S. Government appreciates the enormous difficulty associated with the task of identifying "emerging technologies" for export controls when those technologies and their applications are constantly evolving. The Government further recognizes that, in order to move forward with controls, it must decide between two very different types of regulatory approaches. The first option is to wait until "emerging" technologies develop into somewhat better understood, more "mature" technologies in order to be more precisely defined for controls (in much the same way that most technologies are identified on export control lists). Alternatively, the U.S. Government has the option of acting more swiftly by delineating and controlling broader categories of technologies as "emerging technologies" under ECRA.

---

[18] Export Control Reform Act, H.R. 5040, 115th Cong. § 106 (2018).

I do not believe that the U.S. Government has abandoned either option to date, even though there are downsides associated with each. The former approach, whereby "emerging technologies" are narrowly defined, risks additional delay in instituting controls that are presently needed. Moreover, by attempting to define technologies that are not yet fully understood with a high degree of specificity, the Government may inadvertently omit necessary technologies from control. A too-narrow definition also increases the likelihood of circumvention by technology developers who may be able to reconfigure their technologies in minor ways in order "design out" from the scope of controls. On the other hand, the alternative approach of adopting a broader definition of "emerging technologies" – while it allows for the more expeditious implementation of licensing requirements – runs the risk of regulating more exports than necessary to protect national security. To the extent the U.S. Government adopts either option, it should consider imposing licensing requirements for only exports of emerging technologies to entities and/or countries that pose the most significant national security risks. To the extent that the acquisition of emerging technologies by U.S. allies does not pose risks, allies could be exempt from licensing requirements. This approach additionally eases the licensing burden on federal agencies and U.S. businesses.

3. Exports to Countries that Do Not Permit Adequate End-Use Checks

The U.S. Government also needs to better control technology transfers to countries with inadequate "End-Use Checks," like the PRC. End-use checks are mechanisms by which U.S. Government officials conduct on-site audits of foreign recipients' ("end users") use of controlled items to determine whether the items are being used in accordance with the terms and conditions associated with the U.S. Government's export authorization.

Today, in order for the U.S. Government to conduct an end-use check of any PRC entity, it must notify the PRC government of its intent and seek the government's authorization in advance

of the actual check. Often, end-use checks are not permitted for weeks. This affords the PRC government ample time to tamper with the end user's records in order to obfuscate any evidence of export control violations. The PRC government and its companies are notorious for falsifying records and diverting exports of controlled items to unauthorized end users within the PRC (*e.g.*, the PLA, military end users) and countries abroad (*e.g.*, Iran). The U.S. Government needs to take this reality into account.

If the U.S. Government does not have full confidence in its ability to conduct thorough and transparent end-use checks in the PRC, then it should not authorize exports of sensitive items to the PRC at all. At a minimum, the Government ought to adjudicate export licenses to the PRC under a "presumption of denial" evaluation criteria rather than the current "case-by-case" criteria, which is normally enjoyed by firms in nations that authorize end-use checks by U.S. officials and otherwise fully comply with U.S. export laws. The PRC should not be subject to the same license review criteria as fully-cooperating partners. This policy needs to change.

4. Entity List License Review Criteria

The U.S. Government should also update its Entity List policy. The Entity List (found in Supplement No. 4 to Part 744 of the Export Administration Regulations ("EAR")[19]) "identifies entities for which there is reasonable cause to believe, based on specific and articulable facts, that the entities have been involved, are involved, or pose a significant risk of being or becoming involved in activities contrary to the national security or foreign policy interests of the United

[19] 15 C.F.R. § 744.16, available at https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744/appendix-Supplement%20No.%204%20to%20Part%20744.

States."[20] Where the U.S. Government determines that reasonable cause exists, it may include a parent company, as well as its affiliates, on the Entity List.[21]

For items subject to the EAR, the entity listed companies are generally prohibited from receiving U.S. exports absence a license from the U.S. Commerce Department, and the majority of export licenses to Entity List companies are subject to a "presumption of denial" license review policy. The legal threshold for including entities on the Entity List is by design a flexible standard so that the U.S. Government has improved ability to curtail these entities' harmful actions through export licenses.[22]

Today, there are a number of entities on the Entity List where U.S. exports are subject to an export license review policy of "case-by-case" or "presumption of approval," rather than the "presumption of denial" policy. These more lenient license review criteria obviate the punitive impact of a company's designation on the Entity List. It makes no sense to place a PRC entity on the Entity List for having engaged in malign activities if, through the designation, the entity is able to benefit from the same or better export-license adjudication procedures than non-harmful actors.

Congress has, in the past, requested license review and approval statistics for PRC companies on the Entity List and has been surprised by the large number of export licenses approvals to Entity Listed companies. This is the reason.

---

[20] *Clarification of Entity List Requirements for Listed Entities When Acting as a Party to the Transaction Under the Export Administration Regulations (EAR)*, 85 Fed. Reg. 51,335 (Bureau of Indus. and Sec. Aug. 20, 2020), available at https://www.govinfo.gov/content/pkg/FR-2020-08-20/pdf/2020-17908.pdf.

[21] 15 C.F.R. § 744.11(b).

[22] Company-specific Entity Listings are not a substitute for item-specific export controls. An Entity Listing regulates exports of many items to a specific entity (*e.g.*, SMIC, Huawei), whereas the control list designation regulates exports of a particular item to all entities in various countries. These authorities are not substitutes and should not be used interchangeably.

5. Unilateral Versus Multilateral Controls

It is also worth pointing out that the notion of consistently favoring a multilateral approach for export controls over a unilateral approach may not always be justified and may ultimately impede the implementation of much-needed controls to safeguard national security. The reality is that not all countries are able to move in lock-step with the United States by imposing controls at the same speed, same scope, same manner, and at the exact same time.

Most countries' economic exposure to the PRC and geopolitical vulnerabilities are far greater than the United States', and these exposures necessitate a different approach to controls. For example, Europe is far more economically entangled with the PRC, and South Korea and Japan are far more geographically vulnerable. In light of this reality, it makes little sense for the U.S. Government to continuously demand multilateral export restrictions and expect allies to consistently act in unison in order for it (the U.S. Government) to act. Again, this delays the implementation of controls to protect U.S. national security.

Where the United States has the will and ability to impose controls in advance of its allies, it should do so and with faith that our allies will likely follow our lead. This is exactly what happened when the United States imposed restrictions on U.S. exports to Chinese telecom giant Huawei Technologies Co., Ltd. ("Huawei") several years ago. Had the U.S. Government pursued export restrictions multilaterally, the restrictions would never have been imposed.

For reference, in May 2019, the United States placed Huawei on the Entity List for its violation of U.S. financial sanctions against Iran.[23] The U.S. business community responded with outrage because it argued that foreign countries would increase sales to Huawei and displace U.S.

---

[23] *Addition of Entities to the Entity List*, 84 Fed. Reg. 22,961 (Bureau of Indus. and Sec. May 21, 2019), available at https://www.govinfo.gov/content/pkg/FR-2019-05-21/pdf/2019-10616.pdf.

business opportunities. Businesses, in effect, complained that America's allies would work against U.S. interests. But that is not what happened. In fact, the exact opposite occurred.

Soon after the U.S. Government placed Huawei on the Entity List and restricted exports to Huawei under a "presumption of denial" export license review policy,[24] America's allies began pulling back sales to Huawei. Not because they were legally obligated to do so, but because it was the correct course of action. Yet they did not pull back publicly. Each country, given its own unique economic and political circumstance, retreated from Huawei in its own manner, most often quietly and without any public fanfare. In fact, the United States' unilateral action caused a multilateral ripple effect among our allies, and by our giving them "top cover," our allies followed suit. The result, of course, was the crushing defeat of Huawei's smartphone business.[25]

This example illustrates that, when coordinating export controls with allies, we need not always move in in perfect synchronicity. The United States should, whenever necessary, act to protect its national security interests and be assured that our allies will follow, albeit at their own pace and through their own legal mechanisms.

6. Closing the Fundamental Research Gap in Export Controls

Further, our adversaries are exploiting research in our universities to obtain cutting-edge technology, and our universities are in turn freely transferring technology to high-threat actors using the "fundamental research" exception of the export control rules. The EAR currently defines fundamental research as:

---

[24] The license review policy was subsequently changed in August 2020 to a "case-by-case" license review criteria for most exports.

[25] Rob Thubron, *Huawei experiences largest-ever revenue fall as sanctions crush its consumer division*, Tech Spot (Aug. 6, 2021), available at https://www.techspot.com/news/90696-huawei-sees-largest-ever-revenue-fall-sanctions-crush.html.

> {R}esearch in science, engineering, or mathematics, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons.[26]
>
> "Technology" or "software" that arises during, or results from, fundamental research and is intended to be published is not subject to the EAR.[27]

These exceptions permit the flow of cutting-edge research and development in critical technologies – for example, artificial intelligence ("AI"), leading edge semiconductor design and production, lithium-ion batteries, robotics, genomics – to high-threat actors. This is another gaping hole in our laws that needs to be closed.

U.S. universities ought to be subject to export control licensing requirements before engaging in such technology transfer, and there are steps that the U.S. Government can take to regulate this flow of information. An immediate step is to issue notices to universities (via a Presidential Proclamation or a Federal Register notice) providing that licenses would be required for sharing controlled technology with non-U.S. persons. The legal mechanism here is the "is-informed" process, which is a "stop gap" measure where the U.S. Government informs the entity/entities (universities in this case) of a license requirement in advance of a formal rule change. Subsequently, the U.S. Government should revise its definition of "fundamental research" in the EAR to make it more restrictive. Fundamental research should be treated no differently than controlled technology; once basic research evolves into the type of know-how matching control levels, licenses should be required. Indeed, the U.S. Government maintains the authority to change its own regulations to keep pace with new national security threats. It must do so now; time is overdue.

---

[26] 15 C.F.R. § 734.8.

[27] *Id.*

7. Export Controls on Data

In today's high-technology ecosystem, there is no reason why we are not controlling through export controls data transfers to foreign adversaries, especially when it is public knowledge that our data are being used and misused by our adversaries to build dangerous AI capabilities and massive surveillance machines. Similarly, U.S. businesses should not be placing data storage centers in the countries of our adversaries or allowing them to have any control over our domestic data storage systems. Some of these transactions would never come under the review of the Committee on Foreign Investment in the United States ("CFIUS") (falling below the regulatory thresholds or developments through greenfield investments), so we need independent legal authority to deal with this risk. The proposed outbound investment review legislation discussed below would help regulate the transfer of data storage centers abroad. Export controls are additionally needed to regulate the export of sensitive data.

8. Secondary Sanctions as a Tool

Secondary sanctions should also be leveraged as a viable economic tool. The U.S. Government and Congress receive substantial information on a regular basis – whether through intelligence reporting or public news outlets – of sanctions violations by PRC entities. Under U.S. laws, violations of U.S. sanctions are punishable by the imposition of secondary sanctions. Yet, the U.S. Government has, to date, been reluctant to punish PRC companies for such violations. Presumably, the reason for this is the extent of American companies' financial exposure to the PRC.

Herein lies the irony of the U.S. Government's policies. The U.S. Government, on one hand, is unable to hold PRC entities accountable for undermining U.S. national security interests and, on the other hand, permits businesses to transact with harmful entities even though doing so

fuels the PRC's growth. Our refusal to impose secondary sanctions also emboldens PRC entities to continue undermining U.S. interests.

Our policies need to change. Secondary sanctions need to be used to address activities that undermine U.S. national security interests.

9. Revenue Substitution – Away from the PRC and Towards Allies

Finally, we should dispel the prevailing notion that U.S. businesses need revenue from sales to the PRC in order to invest in next-generation technologies and survive economic competition. Indeed, any revenue lost from sales to the PRC may be replaced (and even augmented) by increasing sales within the United States and to nations of allies. It makes no sense to invest in the supply chains of an adversary instead of our own. We must build our own supply chains, as well as our allies', in order to achieve much-needed redundancies in our most critical supply lines. Furthermore, redundancy is essential where supply chains are most vulnerable. The U.S. Government should support investments to build supply chains domestically and with allies.

D. Regulating Foreign Direct Investment ("FDI") Flows

The U.S. Government needs to better regulate FDI flows that harm U.S. economic and national security interests.

1. Delayed Reviews of FDI in Existing Critical Technology Businesses

The Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA") represented a major milestone in protecting national security by granting to CFIUS enhanced authority to protect "critical technologies" from foreign acquisition through FDIs. However, nearly four years into its enactment, the U.S. Government has not yet been able to fully utilize this new authority. This is because FIRRMA's definition of "critical technologies" rests in large part on ECRA's identification of "emerging technologies," and until the U.S. Government makes progress on this issue, gaps in our national security laws persist.

Here too, the question of whether to narrowly or broadly define "emerging technologies" (as explained above) has important implications in the context of reviews of FDI transactions. On one hand, a broader definition would subject a wider range of transactions to FIRRMA authority, thereby giving the U.S. Government increased visibility into U.S. FDI activities and greater authority to restrict those that threaten national security. On the other hand, it is argued that increased regulatory oversight will deter FDI flows into the United States. To address this latter concern, the U.S. Government could consider limiting mandatory filing requirements to only those entities and/or countries that pose the most significant threats to U.S. national security. This would decrease regulatory burdens on U.S. businesses and ultimately reduce the volume of transactions subject to review by federal agencies. A broader definition applied to a narrow set of countries is the most effective and efficient national security approach.

Whichever option the U.S. Government pursues has serious implications. But the ultimate point here is that the U.S. Government needs to make substantial progress in its identification of "emerging technologies" under ECRA and "critical technologies" under FIRRMA. Movement on these fronts will give businesses some clarity going forward and enable the U.S. Government to better exercise the legal authorities it possesses to protect national security. The exercise of those authorities has, for nearly four years, languished.

2. Merits of Outbound Investment Reviews

In much the same way that FIRRMA and its predecessor, the Foreign Investment and National Security Act of 2007, imposed national security reviews on inbound FDI transactions, Congress is now considering similar legislation for outbound investments to high-risk countries. New legislation would call for CFIUS-type reviews of U.S. asset flows to foreign markets for national security risks. Even though this outbound investment review screening mechanism is one

of the most important pieces of legislation before Congress today, it is one of the most contentious.[28]

To the extent there is any question as to whether such investment review mechanisms are warranted, we should be clear about how urgent the situation has become. At the end of 2020, U.S. investments in in PRC companies totaled by capital investment type (public and private equity):

- U.S. Entity List Companies: $48.6 Billion
- PRC State-Owned Enterprises: $152 Billion
- PRC Military End User and Chinese Military Companies: $54 Billion
- Telecommunications: $43 Billion
- Robotics: $1.3 Billion
- Biotechnology: $50.4 Billion
- Artificial Intelligence: $221 Billion
- Surveillance: $3.8 Billion
- Aerospace and Defense: $1.3 Billion
- Semiconductors: $21 Billion
- Pharmaceuticals: $31 Billion

In total, U.S. financial investments in Chinese domiciled companies totaled over $2.3 trillion in market value of holdings at the end of 2020. Compounding this fact is the <u>additional</u> transfer of our technology and supply chains, and the outbound investment screening legislation is a key step to solving this problem. We need this law.

Before I explain the merits of this proposed legislation, it is important to level-set, as there has been extensive misinformation about this law. The proposed legislation is not in any way an

---

[28] To lessen the burden on U.S. businesses in filing notices of such transactions for federal agency review and to ease the workload for U.S. Government agencies adjudicating such transactions, the scope of reviews could be limited to outbound transactions involving foreign countries that pose the most significant national security threats.

overreach by Congress to interfere in the free market – far from it. Rather, the proposed legislation is essential to protecting U.S. national security interests that are currently unprotected. To be clear, businesses are primarily motived by revenue, and that is their strong suit. Yet, this fact should not cause them to be unregulated, especially when profit seeking interests undermine U.S. national security. It is the Government, not business, that is charged with protecting national security, and to the extent transactions strengthen adversaries in dangerous ways, the Government must intervene. We have, for centuries, regulated the transfer of defense articles to foreign adversaries. Today, in much the same way, we need to regulate the transfer of technology, economic flows, and supply chain capabilities to them. These are the new weapons of modern economic warfare and our strategic capabilities should not fall into the wrong hands.

As a nation, we need to come to terms in particular with our technology transfer to the PRC. Make no mistake, the PLA's hypersonics advancements were fueled by U.S. chip technology. One company's short-term profits have now threatened to erode the United States' and the world's national security and economic stability. That makes no sense. Our data and technology transfer have also enabled the PRC to race ahead with AI, where reports are starting to surface that Chinese enterprises are using our software and phone apps to track and monitor our movement and behavior data.

As Joseph Stalin is rumored to have said: "We will hang the capitalists with the rope they sell us." Whether this quote is accurate or not, it is illustrative of what is happening today. We have had decades of unregulated supply chain and technology transfer to the PRC that has systematically eroded our own supply chains and rendered us dangerously dependent on the adversary. This is not a good national security strategy. We need a new strategy.

As I mentioned, there is currently no legal authority that reviews these types of transactions for national security risks – namely, joint ventures between U.S. and foreign firms abroad, the acquisition by U.S. firms of shares in companies abroad, or the transfer of a skilled work-force abroad. Such business transactions are frequent and, in the countries of foreign adversaries where the government regularly coerces businesses to act in ways that undermine U.S. national security interests, the risks are serious.

There are four key ways that business transactions are able to undermine U.S. national security interests by transferring to the foreign country/business the following:

> (1) transfer of emerging uncontrolled technology,
>
> (2) transfer of operational know-how that may fall below export controls but nevertheless confers critical know-how to build and/or operate very sensitive machinery (e.g., for nuclear reactors),
>
> (3) transfer of engineers that will develop technologies abroad and so will fall outside the jurisdiction of U.S. export controls (this also results in a "brain drain" in the United States), and
>
> (4) movement of critical manufacturing capabilities and supply chains abroad, such as lithium-ion batteries, active pharmaceutical ingredients, semiconductor manufacturing operations, and medical supplies including personal protective equipment ("PPE").

The foregoing should illustrate that this is a zero sum game; our adversaries' gain is our loss, and our gain is their loss. We need to be clear about this reality. The more we invest in a government-run, command-style non-market economy that is designed to undermine our markets, the more we move production to the PRC to avail ourselves of its cheap prices, forced labor, and other non-market distortions, and the more we purchase cheap goods from PRC businesses rather than goods produced in market economies, the more we allow non-market forces to capture a greater share of the global market. In this way, we are accelerating the demise of capitalism and the market based system. We need outbound review and restrictions as a measure to protect

national security. That is Congress's responsibility and I commend you for not losing sight of this objective. Congress should pass this legislation as it is a national security imperative.

3. Reconsidering CFIUS Mitigation Agreements with the PRC

The U.S. Government's CFIUS "mitigation agreement" policy also warrants reconsideration in light of the PRC government's laws mandating that Chinese and foreign companies transfer sensitive intellectual property, proprietary commercial secrets, and personal data to the central government and the PLA. Among the relevant PRC laws are:

- **National Security/Intelligence Laws:** mandating the transfer of data, information, and technology to the PRC authorities.[29]
- **Cybersecurity Law:** mandating that network operators cooperate with public security organs. [30]
- **Cryptography Law:** eliminating "core function exemption" for products with encryption as general features. [31]
- **Data Security Law:** empowering CCP authorities to demand data from companies and requires companies to "favor economic and social development in line with the CCP's social morality and ethics." [32]
- **Export Control Law:** prohibiting exports of "important data," essentially any information outside of China, even if that data originated from a foreign country, including a U.S. business.[33]

These laws appear to apply to all companies operating in the PRC, regardless of nationality and, in some instances, they also appear to have extraterritorial application, reaching to corporate

---

[29] *Data Security Business Advisory: Risks and Considerations for Business Using Data Services and Equipment from Firms Linked to the People's Republic of China*, U.S. Department of Homeland Security (Dec. 22, 2020) at 6-7 ("DHS Advisory"), available at https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

[30] Lauren Maranto, *Who Benefits from China's Cybersecurity Laws?*, Center for Strategic & International Studies (June 25, 2020), available at https://www.csis.org/blogs/new-perspectives-asia/who-benefits-chinas-cybersecurity-laws.

[31] DHS Advisory at 8-9.

[32] *Id.* at 7-8.

[33] Ck Tan, *China's Export Control Law to Become 'Key Dynamic' in U.S. Relations*, Nikkei Asia (Dec. 1, 2020), available at https://asia.nikkei.com/Economy/China-s-export-control-law-to-become-key-dynamic-in-US-relations.

operations abroad. In the CFIUS context, these laws likely trump the U.S. Government's mitigation agreements.

In reviewing transactions for national security risks, CFIUS commonly enters into agreements with parties in order to mitigate any national security risk resulting from the transfer of information, data, or technologies from the United States to the foreign acquirer. However, when the foreign acquiror is a PRC entity that is also subject to its own governments' data transfer requirements, that entity cannot logically be expected to abide by both the U.S. mitigation agreement and the conflicting PRC government laws. In other words, when a conflict exists between CFIUS's prohibitions on information transfer and the PRC's mandate for data transfer, there is simply no way to adhere to both requirements.

Of course, the PRC government has levers to compel cooperation with its own laws instead of the United States' requirements. One example is the PRC government's nationwide social credit rating system that applies to all corporations for the purposes of detecting misconduct and non-compliance with PRC government rules.[34] The "Corporate Social Credit System" has implications for companies with respect to proprietary technical information, sensitive personal data, and surveillance information. Companies may be given low scores if they fail to transfer their data to the PRC government as part of their obligations. Failing to score well, by non-compliance with the PRC government's policies or demands, may subject companies to myriad sanctions, including higher taxes or permit difficulties, or a blacklisting which could mean financial ruin for that entity.

---

[34] *See, e.g.*, *China's Corporate Social Credit System*, Congressional Research Service (Jan. 17, 2020), available at https://crsreports.congress.gov/product/pdf/IF/IF11342; Kendra Schaefer, *China's Corporate Social Credit System: Context, Competition, Technology and Geopolitics*, Trivium China (Nov. 16, 2020), available at https://www.uscc.gov/sites/default/files/2020-12/Chinas_Corporate_Social_Credit_System.pdf.

The European Chamber of Commerce describes this credit rating system as potentially amounting to "life or death" for companies.[35]

The U.S. Government and Congress must account for the PRC's enormous control over companies and evaluate the effectiveness of the CFIUS agreements. Until the U.S. Government is able to resolve the conflicts described above, it should not permit mitigation agreements for any PRC transactions.

4. The Need for National Security Reviews of Greenfield Investments

Unregulated greenfield investments in the United States also pose very real risks to our national security interests. While CFIUS jurisdiction currently extends to certain real estate transactions that are located within certain geographical areas, for example, certain pre-defined military installations,[36] "greenfield" investments are not broadly subject to CFIUS jurisdiction. This is an enormous gap in our regulations.

Today, malign actors are able to acquire real estate in the United States and use this asset to harm the U.S. interests in a variety of significant ways. Examples include (1) the disruption of regional economic commerce by interfering with critical supply chains (*e.g.*, agriculture, transportation, telecommunication); (2) the displacement of U.S. manufacturers through economic distortive trade activities (underpricing or overproduction to eliminate competition); (3) the acquisition of sensitive personally identifiable information about the general population (*e.g.*, genetic, biometric data); (4) the use of soft power and political propaganda to undermine U.S. democracy (*e.g.*, political promotion programs and media); (5) mass surveillance of U.S.

---

[35] *European Chamber Report on China's Corporate Social Credit System, A Wake-Up Call for European Businesses in China*, European Chamber of Commerce (Aug. 28, 2019), available at https://www.europeanchamber.com.cn/en/press-releases/3045/european_chamber_report_on_china_s_corporate_social_credit_system_a_wake_up_call_for_european_business_in_chin.

[36] 31 C.F.R. §§ 800.213, 802.212.

populations (through the establishment of hotels, medical, and service oriented businesses); and (6) the disruption of the energy grid through the transmission of malicious code (*e.g.*, through malicious software in electric vehicle charging stations or smart homes that connect to the grid). These are just a few examples.

President Biden has already warned the American public that the PRC government has been conducting large-scale cyberattacks against the United States.[37] Indeed, some of these threat vectors are coming from within our own boarders. In 2014, the China Rail Rolling Stock Corp. ("CRRC"), a PRC state-owned enterprise, built a passenger rail assembly plant in Springfield, Massachusetts. Over time, this investment destroyed U.S. competition in the rail car market. The CRRC now has passenger rail cars in the U.S. North East, Midwest, and West Coast and it is able to leverage these assets to conduct massive surveillance operations over major U.S. populations and control the movement of the public. Presently, the CRRC controls more than 83% of the global rail market, and the company has publicized its aim to dominate the remainder of the world market as well.[38]

Of course, FDI is capable of delivering enormous benefits to an economy. But the U.S. Government must be aware of the risks posed by malign investors as well. The time is ripe to expand CFIUS jurisdiction to greenfield investments. Even though the U.S. Government will never be able to entirely eliminate all threat vectors from its borders, it must do a better job of addressing the range of threats that exist right now.

---

[37] Sean Keene, *Biden Administration Blames China For Microsoft Exchange Email Hack*, C Net News (July 19, 2021), available at https://www.cnet.com/news/privacy/biden-administration-blames-china-for-microsoft-server-hack/.

[38] David C. Lester, *Rail Security Alliance Expresses Concern about CRRC to U.S. Dept. of Defense*, RT&S (June 9, 2021), available at https://www.rtands.com/passenger/rail-security-alliance-expresses-concern-about-crrc-to-u-s-dept-of-defense/.

E. The Chips Act

The Chips Act is a crucial first step to growing the domestic semiconductor manufacturing base in order for the United States to become self-sufficient in semiconductor manufacturing capability and the associated intellectual property. The majority of this capability currently resides in the PRC, Taiwan, and Southeast Asia. Presently, there are quite a number of rumors concerning potential beneficiaries of the Chips Act using financial awards to not only invest in U.S. manufacturing facilities, but also to funnel the corporate capital otherwise saved to investments in China and other geographically vulnerable regions in Southeast Asia. This is an enormous problem. The Chips Act is necessary to strengthen U.S. supply chains and thereby avoid risks associated with our adversaries' growing stranglehold over this sector. It would be antithesis to the object and purpose of the Act to fund domestic industries while allowing the same beneficiaries to double-down on Chinese investments and undermine U.S. national security. There ought to be guardrails put in place in any forthcoming appropriations language.

Further, lawmakers should be mindful of the fact that creating a resilient U.S. supply chain for chips is a an enormously complex endeavor, as secure supply chains outside of the PRC and Southeast Asia are needed for a range of semiconductors products (e.g., logic, memory, analog, digital, and mixed-signal) at varying nodes (180 nm, 7 nm, 5 nm, etc.). In total, this comprises hundreds and thousands of discrete semiconductor chip types with unique chip designs. Additionally, investments are also needed for the development of next-generation lithography technology to manufacture leading edge chips in the United States. As the PRC is endeavoring to acquire current technologies, we need to stay steps ahead.

Moreover, we need to build resilient supply chains for the backend and highly-technical assembly, packaging, and testing capabilities. We also cannot lose sight of the upstream supply chains required to manufacture both the semiconductor chips and the wafer fabrication

equipment themselves, including as raw materials certain critical minerals (e.g., gallium, germanium), chemicals (e.g, hydrofluoric acid), superabrasives (e.g., diamond powder), etc. Most of these supply chains – for both the United States and our allies – reside in the PRC and Southeast Asia.

Finally, the U.S. military needs to ensure that we have robust domestic capabilities – from raw materials, wafer fabrication equipment, to backend assembly, testing, and packaging – to manufacture the semiconductors needed for defense applications, in the event that access to the South China Sea is blocked and armed conflict ensues. Without a strong upstream and downstream military supply chain, our armed forces will only have one-strike capabilities. This is a dangerous position to be in.

F. Trade Remedy Laws Must Be Improved to Protect Injured U.S. Industries

Substantial improvements must also be made to existing U.S. trade remedy laws to better protect injured U.S. industries and provide American businesses with the support needed to re-grow.

1. The PRC's Distortion of the Surrogate Country and Surrogate Value Methodology

From the early 2000s, following the China's 2001 accession to the WTO, the PRC government began an aggressive push to erode U.S. industries through predatory pricing practices. Trade with the PRC increased over the years, and the number of trade disputes grew exponentially.

Presently, the United States has over 223 trade remedy cases against the PRC versus a total of 441 cases against all other nations combined.[39] This is astounding, and the level of harm inflicted by PRC exporters through their underpricing behavior is the most significant of any other

[39] United States International Trade Commission Website, available at https://www.usitc.gov/.

trading nation. What is more, the number of complaints against the PRC continues to increase well into the its third decade of WTO accession. This tells us something very important: that the PRC is continuing to take advantage of the multilateral trading system in order to displace competitors from the global market.

While the United States currently maintains a robust set of trade remedy laws (antidumping and countervailing duty laws) to offset unfair trade and "level the playing field" for domestic manufacturers, many of the policies that the U.S. Government pursues to carry out these laws need to be updated to address the PRC's growth.

One of the most compelling areas for change is the manner in which the U.S. Government selects "surrogate" countries in dumping proceedings to value goods produced by the PRC. Because the PRC is a non-market economy, the U.S. Government relies on third country prices, or "surrogate country" prices to value the cost of production in the PRC (which is then compared to U.S. prices to measure unfair dumping). However, because PRC goods have penetrated global markets so aggressively, it is nearly impossible to find a surrogate country that has not been adversely affected by the PRC's predatory pricing. Prices around the world have been depressed so extensively that virtually all benchmark prices in trade cases are now understated and inadequate for measuring underselling by the PRC.

The result is that the tariffs ultimately imposed by the U.S. Government on Chinese imports to offset dumping are inadequate to "level the playing field," and consequently proper relief is denied to American firms. The U.S. Government must update its tools to more effectively prevent harms to the domestic industry. The present system is failing.

2. Section 301 Investigations to Address Additional Predatory Economic Practices and Creation of An Innovation Fund

Finally, Section 301 of the Trade Act of 1974, as amended, provides a remedy against country-specific unfair trade practices, and action is permissible if the United States Trade Representative determines that U.S. rights under a trade agreement are being denied, or a practice by a foreign country violates or is inconsistent with a trade agreement, or is unjustifiable and burdens or restricts U.S. commerce.[40] If such a finding is made, Section 301 authorizes the U.S. Government impose a range of remedial trade measures, including but not limited to the imposition of tariffs on goods imported from the foreign country.

It has been rumored that the United States may be considering, in addition to the current Section 301 tariffs on PRC goods for intellectual property theft (*i.e.*, tariffs ranging from 7.5% to 25% on specific imports),[41] tariffs in response to the PRC government's use of industrial subsidies. That is, a new Section 301 investigation would be launched to determine whether such industrial subsidies have harmed U.S. interests.

Beyond IP theft and industrial subsidies, there are numerous additional ways in which the PRC is undermining U.S. national security and economic security interests. The PRC focuses on areas where existing laws are inadequate or altogether nonexistent: global overcapacity, covert cyberattacks, market access restrictions (in China), and the exploitation of assets in the U.S. market.[42] Here too, USTR should conduct Section 301 investigations on these practices and

---

[40] Section 301 of the Trade Act of 1974, as amended (19 U.S.C. § 2411).

[41] Section 301 tariffs were imposed by the United States on imports from the PRC to recoup the approximately $50 billion a year economic harm to the U.S. economy caused by the PRC's intellectual property theft. *See Section 301 Tariffs on Goods from China: International and Domestic Legal Challenges*, Congressional Research Service (April 5, 2022), available at https://crsreports.congress.gov/product/pdf/LSB/LSB10553.

[42] For example, PRC entities underselling through physical presence in the U.S. market where existing trade remedy tools that are specific to countering unfairly priced imports (e.g., antidumping and countervailing duty laws) would not apply, and where Federal Trade Commission anticompetition laws do not probe national security threats for action.

impose import-restrictive measures to recoup the value of economic harm caused to U.S. businesses.

Moreover, if affirmative determinations of harm are made as a result of the Section 301 investigations and additional Section 301 tariffs are imposed on imports, then the U.S. Government should consider shifting the tariff payment responsibility onto PRC exporters rather than U.S. importers. Currently, U.S. Customs and Border Protection requires that the "importer of record" (which may be the U.S. importer or foreign exporter) pay tariffs on imported goods. However, often for the payment of Section 301 tariffs, PRC exporters pressure U.S. importers to bear the costs. If, however, the responsibility for the Section 301 tariffs were legally placed on the PRC exporter, it would relieve the U.S. importer of this financial burden. Through a Presidential Proclamation, the U.S. Government could legally require PRC exporters to be liable for 301 tariffs.

Furthermore, the U.S. Government should consider using the tariff revenue collected to create an "Innovation Fund" dedicated to capitalizing high-technology U.S. industries. The fund should ideally be used to assist U.S. manufacturers and innovators, including high-end semiconductor technology companies and infrastructure companies, obtain a strong foothold in the U.S. market through augmented research and development investments and facility builds. The U.S. Government has collected well over $100 billion in Section 301 tariffs since their original imposition in 2018, and these tariffs, in addition to any new ones, should be directed at growing and catalyzing U.S. innovation and industry growth. The revenue stream certainly exists, and so the U.S. Government should leverage this opportunity to support the nation's industrial and engineering advancements.

III. CONCLUSION

I would like to conclude with a one final note. The world may very well be on the brink a new national security crisis. In order for the United States to lead and defend our nation and our allies, we must have a robust economy, a strong manufacturing base, and the protection of critical assets and technologies. Our vulnerabilities are currently significant, and we need to quickly make important decisions to solve them. Time is not on our side and the challenge ahead of us is enormous.

I look forward to your questions.

ATTACHMENT

July 30, 2020

Statement of Nazak Nikakhtar
Assistant Secretary, International Trade Administration, Industry & Analysis
U.S. Department of Commerce

Before the
Senate Committee on Commerce, Science, and Transportation
Subcommittee on Security
"The China Challenge: Realignment of U.S. Economic Policies to Build Resiliency and Competitiveness"

Good morning. Chairman Sullivan, Ranking Member Markey, and Members of the Subcommittee, thank you for providing me the opportunity to testify today regarding the United States' economic relationship with the People's Republic of China (PRC). We are at historic cross-roads in the U.S.-China relationship, as the steps we take now will chart the course for U.S. economic and technological leadership, and will shape the landscape for the democratic world for decades, and possibly centuries to come.

The Department of Commerce's International Trade Administration is responsible for strengthening the competitiveness of U.S. industry in the United States and global marketplace, increasing investments in America, monitoring compliance with U.S. trade agreements, and enforcing U.S. trade laws. At Industry and Analysis (I&A), we are, in particular, responsible for working with businesses to develop international trade and investment strategies for a range of industries from the manufacturing sector to the financial services sector, including industries that are critical to the United States' national security interests. I&A also leads the Commerce Department's participation in the Committee on Foreign Investment in the United States (CFIUS), a committee that reviews certain specific foreign investments and real estate transactions in the United States for their impact on U.S. national security.

Today, I would like to speak about challenges to the United States' national security industries and set the stage for the successful commercial growth of our most critical sectors. In 2017, the U.S. Government began, for the first time, to confront head-on the challenges posed by China's predatory practices. Those challenges had been ignored for decades and, as a result, over the course of the past 40-plus years, the United States has continuously lost capabilities in sector after sector in manufacturing, technology, and services that are essential to our national security. In goods alone, the offshoring of manufacturing has created supply chain vulnerabilities across hundreds of critical products, ranging from semiconductor and electronics manufacturing to the development of active pharmaceutical ingredients. This has led to job losses of between 3.4 to 3.7 million between 2001 to 2018.[1] In key sectors such as communications equipment, electronics and computer technology, we ceded up to 40 percent of

[1] Scott, Robert; Mokhiber, Zane, Economic Policy Institute, "*Growing China Trade Deficit Cost 3.7 Million American Jobs Between 2001 and 2018*," (Jan. 30, 2020) https://www.epi.org/publication/growing-china-trade-deficits-costs-us-jobs/; *also* Census Data and Department of Commerce calculations.

the domestic market share to Chinese imports, and globally China has captured 40 percent of market share in those sectors as well.

To underscore with examples of where that leaves us, the United States does not have the domestic supply chains required to manufacture many key electronic components for our telecommunications systems, or many active pharmaceutical ingredients for medicines to serve America's health needs. Nor does the United States process the rare earth elements that produce magnets that are essential for military and weapons uses, as processing is now dominated by China. Even the more mature steel and aluminum industries have been experiencing existential challenges, as global overcapacity continues to weaken American firms. Where the United States was once the undisputed leader in technological innovation and industrial advancements across the board, it is now struggling to remain competitive in many key industries.

There are two classes of state actors in the global economy. The first class is comprised of nations that generally adhere to their obligations under the rules and principles of the global economic and trading system, as enshrined in international organizations such as the United Nations, International Monetary Fund, Organization for Economic Cooperation and Development, and the World Trade Organization (WTO). The second class is comprised of nations that either do not adhere (or selectively adhere) to these rules and norms, or actively circumvent them. While both classes of nations can introduce distortions into the global economic order – for example, through corporate subsidies and discriminatory nontariff barriers – the distortions can be managed when dealing with rules-based state actors and market-oriented economies. Here, international agreements may provide viable legal mechanisms to address non-competitive, market-distorting behavior, and states have historically adhered to their binding commitments or improved their practices when compliance fell short.

The Chinese Communist Party (CCP), on the other hand, does not just fall within this second class of state actors. It is also, by far, the most distortive economic actor that the global trading system has ever encountered. Not only are the current rules of international trade and monetary policy largely ineffective when dealing with China but, as a non-market economy under the tight control of the CCP, the government of the People's Republic of China flagrantly flouts those rules when it believes it is in its interest to do so, and shows no intention of reforming to a market-based system or adhering to its international obligations when those rules frustrate its national industrial goals. And because of China's size and scale, it has been able to weaken international supply chains and disrupt the global economy significantly. In this respect, the threat from China is formidable, and it is the largest threat the United States has encountered to date.

But we need to remember that this threat is nothing new, it has its roots in the Cold War. Khrushchev famously said "We," meaning the Sino-Soviet bloc, "declare war upon you," the United States, "in the peaceful world of trade. We will declare a war; we will win over the United States." Again, quoting from the Prime Minister of the Soviet Union, "We," again referring to the Communist states, "value trade less for economic reasons and most for political reasons." The hearing transcript for the Trade Act of 1962 includes these powerful statements. Perhaps in response to this threat, in the "Statement and Purpose" subsection of the Trade Act of 1962, 19 U.S.C. 1801, Congress explicitly enacted into law the goal of Chapter 19; it is *inter*

alia, "through trade agreements affording mutual trade benefits" to "prevent Communist economic penetration." This provision is still valid today precisely because the threats continue today. And after 1979, when the United States formally normalized trade relations with China, the PRC government accelerated its plan to augment global economic and military strength in a quest that it concedes will ultimately lead to a great power struggle against the United States.

The PRC government's weapon of choice is predatory economic tactics, and it has successfully used such tactics to disrupt global supply chains and weaken the technological advancements of the United States and its Western allies. China has transformed itself into the epicenter of global commerce, has centralized manufacturing and research and development (R&D) hubs within its own borders and, with this, it has accumulated the power to influence all economies that are dependent on it.

CHINA'S USE OF PREDATORY ECONOMIC TACTICS TO CAPTURE CRITICAL SUPPLY CHAINS AND TECHNOLOGY

In order to understand the PRC government's predatory economic strategy, it is important to understand the specific trade tools that it deploys. Indeed, China's most effective tools, by design, are those that are governed by weak or non-existent international rules and disciplines. To understand a "strategic competitor" or an "adversary," one has to understand their tactics. To counter those tactics, we need to consider how our laws need to be strengthened.

Case in point: China's economy has grown in large part because of the massive subsidies it provides to industries, and the lack of transparency on the subsidies it provides results from its failure to notify them completely to the WTO, as well as the absence of effective WTO rules governing the types of market-distorting industrial subsidies used in China.[2] It is difficult to legally challenge what we do not know about or what the rules do not cover. Moreover, China leverages its self-designated developing country status to avoid complying with existing WTO rules and obligations, and WTO rules are generally silent on how a member state can challenge another country's self-designated status.

Next, the PRC government takes advantage of the absence of applicable international rules over state-owned enterprises (SOEs) to funnel massive amounts of capital and other resources to SOEs with the well-publicized intent of dominating strategic sectors worldwide. The PRC government also distorts prices and costs throughout its economy (e.g., land and property, energy, wages, and raw materials) through direct price controls and to export undervalued goods and services worldwide, thereby weakening the competitive positions of

[2] Examples include Chinese government subsidies that constitute unlimited guarantees to corporations, subsidies to insolvent or ailing enterprises lacking credible restructuring plans (also known as "zombie" companies), subsidies that encourage global overcapacity, subsidies to firms unable to obtain long-term financing from independent commercial sources that are operating in sectors or industries in overcapacity, and direct debt forgiveness.

market-based firms. Dangling possible access to China's large consumer market and making available cheap labor, goods and services are also how China lures foreign manufacturing capacity and technological know-how into its own borders. And as the CCP controls the government of a sovereign state, it knows full well that its non-market economic system is unaffected by legal challenges or the prospect thereof by the rest of the world; even possible losses of legal challenges at the WTO may not be incentive enough to compel China to reform a system that has served it so well and eroded the competitive positions of its adversaries so quickly.

Just as alarming, the PRC government takes advantage of the dearth of rules governing global overcapacity to flood world markets with distortedly low-priced goods. In 2019, China's overcapacity significantly depressed global prices in the fiber optical cable market. Its strategy is to eliminate competitors and obtain absolute control over this critical 5G infrastructure asset. The PRC government has previously deployed the same strategy in the steel and aluminum sectors, among many others, and the same strategy will create excess capacity in new sectors in the future. And notwithstanding the fact that the 2020 coronavirus pandemic has dramatically reduced demand for steel and aluminum products worldwide, China has once again ramped up steel and aluminum production and dramatically increased inventories, contributing to drastic global price depression. This illustrates the national security threat to our steel and aluminum industries and why the President imposed Section 232 tariffs to address the impact of overcapacity and the threat posed by steel and aluminum imports. Outside the United States, however, the global surge continues and China's actions are still destabilizing the global steel and aluminum industries.

The PRC government is further exploiting opportunities abroad to monopolize strategic ports and mines (among other assets). State-backed Chinese investors own 10 percent or more of equity in ports in Europe, and it has major deals in Greece, Italy, Spain, France, the Netherlands, and Belgium. This is in addition to a growing number of investments in more than 40 ports in North America, South America, Eastern Europe, the Middle East, Africa, Central Asia, South and Southeast Asia, Australia, and the Pacific. The PRC government is similarly increasing control of the raw materials necessary for manufacturing high-technology products (*e.g.,* phones, vehicles, advanced energy storage systems, and magnets) that are sourced from a small number of countries, and for which substitutes are unavailable. Operating in niche markets with limited transparency, often in politically unstable countries, Chinese firms continue to capture supplies of cobalt, graphite, lithium, nickel, niobium, and platinum, to name just a few. Because these minerals and metals are finite assets that cannot be replaced, China is able to exert influence over the rest of the world by withholding access to these assets to compel nations to bend to its will.

Additionally, in its never-ending quest for technological superiority and control over key positions in the industrial value chain, the PRC government regularly has supported or directed the theft and misappropriation of U.S. technology and intellectual property (IP). Monetary damages accrued to the United States are estimated to range from $50 billion to as high as $600 billion annually. Moreover, by making short-lived market access promises to cutting-edge technology companies, the PRC government pressures the most technologically-advanced firms to transfer IP and sensitive data to it. The PRC government ultimately uses the IP it extracts from companies to displace them from the market. China's increased dominance in key

segments of the industrial value chain further cements its technology transfer approach. Even where Chinese firms are perceived to "collaborate" in technology development, take for example Huawei's announcement that it plans to build a $1.2 billion optical fiber research facility in the United Kingdom, the gains are only one sided.[3] Chinese companies will, as directed by the PRC government, benefit from scientific research and collaboration with international scientists abroad, resulting in some cases in the repatriation of technology to generate overcapacity to eliminate competition and obtain a monopoly position. In sectors like 5G, where optical fiber cables provide the infrastructure for an impending technology revolution, the national security implications are obvious.

It is also reported that the Chinese government, this year, is implementing a nationwide credit rating system for all corporations – foreign-owned or Chinese-owned – operating within China. Companies handling sensitive personal data and proprietary technical information will be required to transfer that data to the Chinese government. The European Chamber reports this credit rating system as amounting to "life or death" for companies. [4]

China's engagement in international standards as a way to influence the global technology market also is of great concern, but it is often not fully understood. To illustrate this attempted influence, take for instance the fact that, from 2011 to 2019, the number of Chinese-led technical committees in the International Organization for Standardization, one of the largest international standards setting organizations, increased by 75 percent.[5] Further, China has strategically increased its participation in the International Telecommunication Union (ITU), an agency of the United Nations responsible for coordinating telecommunications operations and services, with the hopes of expanding its influence around the globe. In fact, in key technology working groups of the ITU, China alone comprises 40 percent of participants.[6] Moreover, China's press into international standardization ranges from introducing weak proposals into the standards development process, flooding the organizations with low-quality proposals that detract from and take resources away from sound proposals, to making financial contributions as a way to wield power over those organizations and to punish member companies and countries

---

[3] Gold, Hadas, CNN, "*Huawei to Build $1.2 Billion Cambridge Facility as It Faces Uncertain UK Future*,"(June 25, 2020) https://www.cnn.com/2020/06/25/tech/huawei-cambridge-uk/index.html.

[4] European Chamber of Commerce, "*European Chamber Report on China's Corporate Social Credit System, A Wake Up Call for European Businesses in China*," (Aug. 28, 2019), https://www.europeanchamber.com.cn/en/press-releases/3045/european_chamber_report_on_china_s_corporate_social_credit_system_a_wake_up_call_for_european_business_in_china.

[5] Kamensky, Jack, China Business Review, "*China's Participation in International Standards Setting: Benefits and Concerns for U.S. Industry*," (Feb. 7, 2020) https://www.chinabusinessreview.com/chinas-participation-in-international-standards-setting-benefits-and-concerns-for-us-industry/.

[6] Department of Commerce calculations.

that do not side with its agenda. Indeed, China's participation in international organizations has become a vehicle to advance its One Belt One Road Initiative, and the more influence China has over standards development, the more likely this initiative will succeed.

Additionally, China uses other international organizations to advance its global ambition, including the Belt and Road Initiative. To illustrate, it has been reported that the head of the UN Department of Economic and Social Affairs used his position to discriminate against people and organizations who were drawing attention to the CCP's repression of the Uighur ethnic group. The World Health Organization's capture by the Chinese government, by failing to alert countries to the rapid transmission of the coronavirus, is yet another recent example. Even more to the point, if the Chinese government is currently threatening to retaliate against Nokia and Ericsson for the EU's possible move to ban Huawei from their 5G systems,[7] imagine the types of influence that China could wield if it is able to dominate global standards organizations and the standards themselves.

Finally, it is worth emphasizing that because China is a sovereign state, foreign laws can never be sufficient to fully address its conduct. In fact, the PRC government takes advantage of the United States' lack of an extradition treaty with it to advance cyberattacks on sensitive U.S. assets. The attacks not only obtain proprietary trade secrets from companies and sensitive personal information about American citizens from servers, but these attacks also target crucial weapons systems and sensitive military technology (well-documented examples include attacks that extracted sensitive information about U.S. submarines, cryptographic systems, the F-35 Joint Strike Fighter, and anti-ship missiles that are crucial for deterrence and developing countermeasures). China's medium of cybertheft also includes stealing computer software source codes, design technology, and technical product specifications. And the PRC government continues to violate its 2015 bilateral commitment to the United States in which it had vowed to refrain from stealing and misappropriating U.S. IP.

The tactics used by the PRC government over the course of the past 40 plus years have enabled the country to move its economy from the 12th largest in the world ($191 billion gross domestic product, GDP (current prices), in 1980) to the second largest ($14 trillion GDP (current prices) in 2019); become the second largest foreign holder of U.S. debt at $1.09 trillion in 2019 (the first largest being Japan holding $1.27 trillion), and grow as the world's largest exporter of goods. Indeed, the United States' largest bilateral trade deficit is with China ($345.6 billion in deficit in goods in 2019). In addition, China today holds uniquely powerful positions in the most critical supply chains in the world including rare earths elements, medical equipment and supplies, pharmaceuticals, and electronics.

The past policies of the United States did not effectively impede or curtail China's rise as a predatory economic actor. To build our seemingly efficient supply chains, we flocked to China

[7] Lin, Liza; Woo, Stu; Wei, Lingling, "*China May Retaliate Against Nokia and Ericsson If EU Countries Move to Ban Huawei*," Wall Street Journal (July 20, 2020), https://www.wsj.com/articles/china-may-retaliate-against-nokia-and-ericsson-if-eu-countries-move-to-ban-huawei-11595250557.

as the low-cost producer of virtually every link in the chain, allowed the PRC government to build reserves of U.S. dollars which it used to devalue its currency, traded our most sensitive intellectual property in exchange for short-term market access and profits, and did not adequately use legal enforcement tools to protect our industries. Our motives were short-sighted, and we failed to sufficiently anticipate the vulnerabilities that this trading relationship would create.

As a result, we willingly transferred our debt and exported our manufacturing capabilities (and jobs) to a non-market economy where market principles, transparency, and predictability do not exist. By doing this, we created a global economy where distorted prices and non-market conditions are allowed to proliferate. We also put China in control of our revenue stream. This vulnerability is often not discussed among policymakers, but it is important to emphasize: within our highest-technology sectors, substantial revenue comes from U.S. exports to China. This means that China, by controlling America's revenue stream, also controls America's ability to earn income and fund R&D. This is an extraordinary vulnerability that, if unaddressed, will be used by the PRC government to further halt America's technological progress.

RESHORING CRITICAL SUPPLY CHAINS

Traditionally, economists have viewed calls for countries to pursue policies aimed at protecting national security production capacity skeptically. They argued that a nation could, in a globalized world, always turn to other countries if the domestic supply chains eroded at home. However, what we have learned from the coronavirus crisis is that borders do matter because any state has the sovereign right, and ability to, restrict exports to the rest of the world. Indeed, the PRC government strategically withholds exports: (1) as a bargaining chip to extract concessions from trading partners; or (2) to punish trading partners that do not bend to its will. Even our allies introduced earlier this year – at the height of the pandemic – emergency export restrictions over much needed medical equipment in order to provide for their own citizens to the detriment of neighbors in need.

These facts should serve as an important reminder to the United States that the security of domestic supply chains is essential, and it must be regained because the basic political and economic unit should *always* remain the nation-state. Indeed, the protection of American citizens requires that the United States' vulnerable supply chains be strengthened, and a major component of supply chain resiliency must be reshoring. But how can the United States reverse the excessive offshoring that has occurred over the course of the past 40 years?

The problem is complex, but it can be solved through a whole-of-Government approach. That is, if we collectively are prepared to tackle difficult policy questions, even those that may run counter to long-held economic biases. To the extent that those biases once formed policies that incentivized critical industries to offshore, then logically they need to be revised or reversed.

Understanding what has led to the degradation of our supply chains, then it stands to reason that a comprehensive reshoring strategy must remedy those causes. At the outset, the United States must systematically and routinely identify all products, goods, and technologies that are critical to national security to address the country's dependency on imports from strategic competitors, whether in a time of war, cyber-attack, pandemic or other national

emergency. This Administration – my office in particular on behalf of the White House – has begun doing this. We need to continue this on a permanent basis. An additional component here is measuring the flow of technology if it is now as equally as important, and in many instances more important, than the traditional "national security good."

A second essential component of a reshoring strategy is incentivizing inward investments in domestic manufacturing and R&D activities. We have begun doing this to boost innovation and economic growth through tax cuts. A whole-of-Government approach, in partnership with Congress, will continue to make this effort successful.

Third, we have in our arsenal of tools powerful U.S. Government procurement authority, including the Defense Production Act authority, to provide capital to new American investments and also as a tool to generate demand, through U.S. Government purchases, for national security-related items that are produced within the United States. Reliance on Government procurement authority is what will compel many companies to take a leap of faith and re-invest in the United States. This is an important tool that we are using and should be empowered to use even more.

Fourth, it is, of course, axiomatic that U.S. investments must be encouraged to grow to commercial scale in order to compete against more mature foreign competitors. Further, an industry's commercial viability will generate robust upstream and downstream supply chains, draw in new market entrants to enhance production efficiency and moderate prices, attract greater private sector investments, and encourage competition to accelerate R&D. These are the fundamental building blocks of a resilient domestic supply chain.

Finally, we have the ability to increase exports of all U.S. firms – including those that re-shore to the United States – through trade agreements. We have begun to increase exports thorough the U.S.-Mexico-Canada Trade Agreement and the U.S.-Japan Trade Agreement, and we should continue to encourage greater exports through new trade deals.

With the support of Congress, we can build the strongest supply chain in the world, enhance our comparative advantage with allies, and create an ecosystem where market-based principles prevail and market distortions are eliminated. We have begun doing this; we can do more together, which is why this hearing is so important.

CONCLUSION

Historically, through times of adversity, the United States has led the world out of war and economic turbulence into recovery. And now too, the world will look to the United States to lead the way in solving today's supply chain challenges. It should not be forgotten that the global economy of the 20th century was developed by the United States and, although China is aggressively seeking to shape the global economic order of the 21st century, it is not too late to act. While the United States remains the largest economic power in the world (a status that is not guaranteed as China's exponential growth continues), it has the ability and leverage to act in coordination with allies. Time is of the essence, and our supply chain vulnerabilities are too great to await another national security crisis that may expose this country to even more devastation and destruction.

Chairman WARNER. I want to thank all three witnesses. And I want to point out a couple other quick things and then get to my question.

One, I think we also do need to acknowledge while China has picked national champions, they have combined the best of both systems to a level. They do have a ferocious startup industry in China, oftentimes supplemented by their $500 billion in intellectual property theft each year. And so, they have that ferocious competition until that national champion emerges. I think we need to be clear-eyed about our potential competitor here.

This brings back two points that maybe I should have made in my opening comments. I remember, and it was driven a lot by this Committee, when we woke up about 5G and Huawei and tried to finally get all the right people who we thought in the room from USG, we had I think three intelligence agencies. We had DOD, we had Commerce, we had State, we had NTIA, we had OSTP. And for those who might be watching this, these are all relatively large organizations with all these acronyms. We had the FCC. And it was absolutely clear that these people had never been in the same room talking about taking on a question like how do we give up the spectrum that's going to license 5G, how we think about making competition with our allies, how we address what was happening with Huawei.

That is a preface. And the other preface before my first question is if you then look at the technologies where we need to be competitive against China, we all have I think marveled sometimes at the game plans that they've laid out. And as I think Dr. Mulvenon said, James said, that they'll put this out until the West discovers it and suddenly they disappear from the websites. But I just know within recent years when I've asked the intel community, what are the key technologies we ought to be competing with? We got one list from the ODNI, a somewhat overlapping but not entirely the same list from CIA. Commerce has got a different list. The White House through OSTP may have another list. So if we can't figure out who to get in the room or what is even the major focus areas of our attention. Senator Cornyn really took the lead on helping move forward this idea around semiconductors. I'm not sure we'd have been making the progress even on semiconductors but for COVID because of the immediate shortages we were seeing.

The first question I would ask is for the whole panel. Ms. Nikakhtar, you seem to have looked at this from a trade standpoint, but if you were going to structure, make a change in government on how we would put the right people in the room to make these honest assessments, because I remember from the fact that our intel community can't even look, frankly, at what was happening domestically. They can look abroad, but they can't look here domestically. How do you get the right folks in the room? And I'd ask the whole panel on that.

Is there a new structure they've put together? Is it a working committee? What's the structure to make that happen?

Ms. NIKAKHTAR. Honestly, the National Security Council is a wonderful body. And this is the convening body that brings everybody together, and they do a good job at bringing everybody together. The fundamental problem, because I've been at these meet-

ings in various positions, is that not every agency, not every bureau within an agency is like minded. And so you have bureaus within an agency trying to torpedo one another. And I personally don't know how to solve that. I wasn't born in this country, but if I were a Cabinet member, I would make sure—I mean, if I were President, I would make sure that I had every single Cabinet member likeminded, every Cabinet member ask their staff, what is your forward-leaning China strategy? That way you can convene everything at——

Chairman WARNER. You think it has to come from them. What about your colleagues? What do you guys think?

Dr. MULVENON. It's early days, but I am hopeful about the Agency's new Transnational Technology Mission Center, at least as a locus for doing these types of strategic-level assessments on technology. I share your frustration. I'm old enough to remember the 1996 Militarily Critical Technologies List when it was published by the Pentagon, which for a brief moment in time was a definitive, governmentwide list that we could all use to then assess technological progress and make export control decisions. But then the promise was that it was going to be updated and then it never was.

One suggestion, Senator, that I've heard that I think makes some sense is given that many people in the Intelligence Community in a sense are cutoff from the high tech industries and may not be as current as they should be. That partnering with organizations like the National Academy of Sciences for those studies makes more sense because of their networking connections.

Chairman WARNER. Dr. Murdick?

Dr. MURDICK. Lists are always problematic, especially in a dynamic space of emerging technologies where they're always changing. And I think to be able to build this kind of capability, you need a systematic analytic capability that covers both domestic and foreign capabilities. We don't really have a place in the U.S. Government for that kind of capability. And to be able to answer the kind of questions you need, you need to be able to have people who can go deep enough to actually answer the substantive questions, not just from a who do we partnership perspective, from a state perspective, or from commerce, or from DOD. I think you need to have, what I would call, an independent capability within the government that you can regularly turn to and they can coordinate with all the rest of the U.S. Government entities and even take money for it for analysis tasks, but actually get at this analytical capability. And I think the reason I encourage this is even just watching how China has made their advance. Obviously, we don't want to mirror China, but they have put a tremendous amount of resources in—. Sixty thousand people is not a small number of people to actually look at what's happening worldwide from the S&T space. And I think that that analytic capability is essential. And I think there's a variety of ways to do that to be able to move the things forward.

Chairman WARNER. On the next round, I'm going to come back and ask, as we think about this with our allies around the world, should that be in a more formal alliance or organization structure or should it be one off?

I will remind Members before I go to Senator Rubio that today we are doing something slightly different than normal. We are going to go by order of seniority.

With that, Senator Rubio.

Vice Chairman RUBIO. Thank you.

Let me just start. I'm going to ask a question at the front end, but I want you to answer at the end, to just give you a couple of minutes to think about it. As an example, I know we're all aware of the chips. We're all involved in semiconductor vulnerabilities and the like. But there's a bunch of pretty startling vulnerabilities that we have on the supply chain that are really critical beyond textiles and things of this nature. One, as an example, I think the figure is right, about 90 percent of our key antibiotics are sourced from manufacturing. And what I'm going to ask you to think about in the next couple of minutes while I go through these other two questions, is if you can give me another example of something like that that maybe is not as broadly known, but that's a key vulnerability that we never want to have to depend on them for.

Here's the first question. I don't know who wants to take it. Maybe all three of you do. It's been publicly reported now that as the iPhone 14 comes out that Apple is thinking about using a memory chip made by a product that is from a company that is not just a Chinese-government-owned entity, state-owned business, but it has close ties to the military. So an American goes to buy or we broadly sell in this country to see an iPhone 14 that has that memory chip in it. Beyond being annoying, right, that we're getting it from them, what is the actual vulnerability that that creates for us on a mass scale? The memory chip?

Ms. NIKAKHTAR. Let me start by answering that. You first, Senator, asked for different types of technologies. Seventy-seven percent of the lithium ion battery cell capacity is located in China. Chemicals, nobody talks about chemicals. The ability to make chemicals for semiconductors, for a whole bunch of things also resides in China. A whole bunch of things. But I want to get to the second point of your question. In that example, Senator, that you mentioned, it was actually that the U.S. company in China who's hiring American tech engineers to then go to YMTC to make those chips for it. Obviously, there's threats of backdoor, but the threat that nobody's really talking about is the brain drain that this is creating in the United States—the lack of innovation.

These are companies—I think you had alluded to it, Senator, earlier in your opening statements, which is every time we try to stop this, it's the U.S. companies that are lobbying for the CCP and doing the CCP's bidding.

Vice Chairman RUBIO. The second question is, and we've seen the vulnerability of Americans' genetic information, whether it's housed in our research and medical systems, whether it's what you voluntarily turned over because you want to know where your ancestors came from or whatever it might be. I think data, obviously, is probably the most valuable commodity in the world. And the Chinese can compel the biological data of the largest population in the world. And then they can combine that with whatever they buy and/or access through different ways beyond the privacy concern.

Because the individual may not want their stuff out there in the hands of anybody, much less a foreign government.

Why do they want that genetic information? Obviously, it has to do with biologics. It has to do with biomedical research and development. But what are the advantages of being in possession of a vast dataset of genetic information, not just on the people in their own country, but so many different countries around the world, particularly the United States?

Dr. MULVENON. Before the pandemic, I would have said that we were primarily concerned with organizations like the Beijing Genomic Institute and others because of their unethical practices, because of their connections to the military, because of their connection to the military's biological warfare programs in the PLA. After the pandemic, once we realized that the hyper-globalized model of pharmaceuticals was broken, and that things would not just seamlessly move across borders wherever there was market demand, but in fact national interests had come back to the fore. Clearly having that huge store of data in a lower-ethical-standard environment, to be clear, than the United States, in terms of research ethics on genetic data, means that they would be able to, on the positive side, use their supercomputing capacity to more quickly identify and develop vaccines and pharmaceuticals. But also then, unfortunately, on the offensive side, be able to then figure out how to mutate and be able to modify those genomics.

And so as we move to a world in which we become more and more biological- and machine-integrated as humans, understanding how to make those modifications, particularly their focus on CRISPR and other technologies and the unregulated use of CRISPR in China to do gene modification—that's a very heady and dangerous mix, Senator.

Dr. MURDICK. Senator Rubio, you asked a really interesting question and one that is actually very hard to answer because we're still doing a lot of basic research and it's unclear exactly where everything will be opening up. But let me give one scenario.

Personalized medicine is increasingly learning how to treat the individual and how to work with the individual's whole system. And the more diverse that that data is, the more that they will be able to move beyond what is a much-less-diverse genetic pool in China and to be able to now see what's happening in the U.S. There are a number of examples that will drive innovation. And the more they have this data, the more they'll be able to make breakthroughs in innovation. And I think that's one of their goals: they want to be a competitor and actually make a lot of innovation. And by having access to genomic data at the scale from around the world, it will open up new vectors of innovation that I think will make competition that we can't even imagine in this room right now.

Chairman WARNER. Senator Feinstein.

Senator FEINSTEIN. Just for a moment. My experience with China goes back to when I was mayor of San Francisco. And one of the things I wanted to do was establish a relationship with the Chinese city. We picked Shanghai. Wang Daohan was mayor. We established a relationship. Then Jiang Zemin became mayor. He became president of the country.

In the meantime, trade ideas went back and forth between our two cities. We took Chinese students; we had all kinds of exchanges going on, and I felt it really worked. Now what I see today is all of that kind of thing is gone and the people-to-people relationship which is so intrinsic to friendship and progress and faithful trading has changed to a much more hardened situation.

And I really very much regret that because I will never forget. Those of you that knew Jiang Zemin when he was president of the country know he also sang. And it was the kind of relationship where you could sit down with a group of people, have dinner. He would sing a few songs and it was amazing. And now all that is different.

How do we bring personal relationships back into the equation?

As I review my material, it's all hard edged, it's all companies, it's all economy. But relationships matter. And I deeply believe that. If any of you, you must know China, have ideas, I would certainly welcome them.

Ms. NIKAKHTAR. Senator, maybe I can start. I agree with you, relationships matter. But then how do you foster relationships in a country that's closely monitoring the information that its population gets and is engaging in a propaganda of how the United States is bad? I think that maybe back in time there was opportunity to grow and foster this relationship. But we're now competing with the CCP and its massive propaganda machine and I think our efforts will be exploited and I just don't think the CCP wants that.

Senator FEINSTEIN. You don't think China can change from where it is today?

Ms. NIKAKHTAR. I always think countries——

Senator FEINSTEIN. If it was changed in the past as it has.

Ms. NIKAKHTAR. Yes, I was born in Iran and Iran was very different then than it is today.

Senator FEINSTEIN. Iran isn't China.

Ms. NIKAKHTAR. Right, countries can change for better or for worse. I think under this current CCP leadership with President Xi, China will not change. It's only going to get more and more combative with the United States.

Senator FEINSTEIN. Well, I'll tell you, I would like to do my utmost as a United States Senator from California to try and restore the roots of friendship that once existed and enabled the beginning of the entire trade agenda. If anybody has any thoughts, I would welcome them. I listened carefully to what you said and I understand that a hardness has entered into this relationship, and I think all of us ought to try to change it because this is a huge country with smart people and a dynamism that can make the world better if we're able to make the contacts, the agreements, and the changes to bring it into the modern day without negative influence.

I just wanted to say that. Thank you very much.

Dr. MURDICK. I just wanted to add one thing. You asked for ideas and I think that's really where we're going to have to continue to look, because there are challenges on the ground. However, I just wanted to add from a more encouraging perspective two points.

One, if you view China as purely out to destroy us, that's all they want to do, I think that mind view actually limits options. I actually don't think their sole purpose is to destroy us. They want respect. They want a place at the table. They want to be able to remove the vulnerabilities they feel like they have. I'm not saying these are benevolent, by the way, but I think viewing them as a competitor and viewing that there are things that will be worth working on together and there are things that are not worth working on together.

The challenge, however, in this is two parts and one of them is people-to-people interactions that building trusting relationships, but the other is a dearth of information. If you don't have solid information on what China is doing, it's easy to get sucked into a discussion that you're underprepared for and you're actually not realizing what's actually happening. And I think the U.S. Government can raise the bar, if you may, and understand more about China by investing more in our analysis capability, and then arm people who are engaging personally so that they aren't going to get swept in the wrong way, because they don't understand the context and can negotiate through a strength of knowing and power. And I do believe that those personal relationships ultimately will make a difference. But I would encourage that those relationships to be well-informed.

Senator FEINSTEIN. Thank you.

Chairman WARNER. Senator Collins.

Senator COLLINS. Thank you, Mr. Chairman.

Ms. Nikakhtar, first let me thank you for your very powerful testimony and your very specific recommendations. I was also pleased to hear the discussion of the supply chain for pharmaceuticals. This is an issue I've been very concerned about ever since the FDA testified that 72 percent of the facilities making active pharmaceutical ingredients are located in either India or China. We simply are very vulnerable in that area.

Let me move to my question. Of the $107 billion in total exports to China in 2019, I am told that all but $500 million were exempt from export controls or did not require an export license in the first place. I think that's absolutely stunning. That is less than one-half of one percent of all exports from our country to China that are subject to any form of effective export control oversight. That seems to me to be potentially extremely harmful to our national security, economic and technological advantages, that the United States has traditionally enjoyed.

As a former implementer of policy at the Commerce Department, where do you think we have not effectively used existing tools to protect our national economic security interests against the PRC?

Ms. NIKAKHTAR. Thank you for the brilliant question. I'm going to add a statistic on to what you said, which I found very disturbing. I think it was about 2018 or 2019. Ninety-nine point one percent of the export licenses were either granted or returned without action, meaning the agency took no position. Ninety-nine point one percent. Of what is controlled and you actually have to get a license for: Ninety-nine point one percent.

The other point I want to make is, and I find this very troubling. I do this because I just want to help this country protect its na-

tional security interests. The back end of the early 2010s, there was export control reform in the government and export control rules on dual-use items were pretty much loosened to create gaps in the laws to allow these exports. You have definitional issues. You have areas where just licenses are exempt. That needs to be reformed again given current threats. And I would support anybody's effort who really wants to help me and maybe others to sweep through these regs and then recommend some solid changes.

Senator COLLINS. Thank you so much.

Dr. Murdick, China's Ministry of Foreign Affairs is undertaking a very aggressive diplomatic effort in international organizations to establish favorable worldwide technology standards that China wants that are favorable to the PRC and its values. On a scale of one to ten, how effective has our State Department and other diplomatic arms of NATO and the West been at pushing back at these efforts?

Dr. MURDICK. Just a brief comment on history. The standards efforts that China is engaged in trying to implement now, in the push that they've had, was motivated by what they perceived as a very effective U.S. effort. In aerospace and a variety of other places, the standards that we helped influence in GPS and other places were a gold standard. They said, wow, we really want to do the same thing. So first of all, we motivated them by our success to try to do something similar. They're working very hard. It's hard for me to provide a number and I'm not trying to avoid the question in that sense, but I'm not actually sure how I would characterize it with a number. I think it's too soon for me to be able to judge what is the success. I think it's an ongoing dynamic space and it depends on the particular industry and the particular standards bodies where we've been more successful and where we haven't been as successful. But I do want to lay the foundation that a lot of the foundation is based on previous U.S. successes in the standard space.

Not exactly the answer you're probably looking for, but it's the best I can do right now.

Chairman WARNER. Senator Heinrich.

Senator HEINRICH. Dr. Murdick, you've said that the U.S. Government needs an analytic capability to survey and monitor the global science and technology landscape that we currently don't possess. If I could put you in charge of just such an effort, what would it look like? How would you structure it? Where would it fit into the current USG org chart?

Dr. MURDICK. Obviously, political reality will temper this, but I'm going to go ahead and speak from an idealist perspective.

From my perspective, an organization that does this type of analysis needs to be independent. They need to be able to receive money from all over the government. They need to have a seat at the table in terms of decisionmaking. But their primary goal is to do analysis. I think there are Federal elements here, but there are also regional elements. Just having everyone sitting in the U.S. capital region is probably not a great idea because there's innovation happening all around America. And both the information that this group would need as well as the results of some of the findings would be relevant to the sector.

It's probably the majority—or half, let's say—of the staff would be in the D.C. area. The rest would be throughout the U.S. And I think it would probably have, I don't know, maybe a number of hundreds of analysts and data collectors. They would bring the data together. They would be able to provide analysis on S&T challenges. They would be able to have a monitoring situation so that you could answer questions and be alerted when things are changing. And that this information would be available to U.S. policymakers and as appropriate to the public and industry as well as relevant. I think the U.S. can learn, actually, something from the Chinese implementation of this in terms of the scale of investment. And we're not talking about more than, I don't know, could be a couple hundred million dollars. We're not talking about a colossal—. We're not launching multiple satellite constellations here. We're talking about a reasonable and consistent and sustained development that has an analytic capability that looks at both foreign and domestic. It provides strategic input. It provides input on where unwanted tech transfer is happening. And it provides the kind of information that's actionable and useful to policymakers.

In a thumbnail, that is a few thoughts I have.

Ms. NIKAKHTAR. I'd like to quickly add to that. I would take a little bit from what Senator Warner had also asked. There are two lists in the government. There's the emerging technologies list that just came out from the White House. And then it's BIS's, I think 2019 or 2020, foundational technologies list. You combine those two, you've got a pretty darn good list of where we need to focus on. And then the National Labs. Our National Labs know stuff about what we're doing, our competitive advantage. And our adversaries, what they're doing, how far they are in terms of even commercializing their R&D. I think the National Labs are a completely underutilized crown jewel in American policymaking, and I think we really need to leverage them.

Senator HEINRICH. I agree with you, although in the fact that I interface with those labs all the time, sometimes pulling that information out of the labs in a usable way for the government and particularly for policymakers can be quite challenging.

Let me ask you about export administration regulations and the current definition of fundamental research.

Ms. Nikakhtar, you've talked a lot about that and you write that the exception of fundamental research is a gaping hole right now. Can you give us some context for why that gaping hole exists in the first place and what we need to do to change it?

Ms. NIKAKHTAR. Yes. Basically, the rule is pretty squishy and it basically says that if the building blocks essentially are built from fundamental research, then pretty much what generates from it is also this fundamental research. And if you might have the intent of publishing it at some point then it's exempt from export controls. I mean, we're lawmakers. When you leave squishy things like that, can anybody exploit it? Absolutely. And the reason why I'm completely nervous about this is because I've got a friend who's doing some critical semiconductor research in Silicon Valley. And he calls me and he goes, there's a prominent university in California who has these Chinese nationals coming in and doing research on the

next generation of semiconductor technology. And my response is, oh my gosh, of course this is because of the fundamental research exception because this is how it always gets used. And then he's like, what's the fix? And I said, issue an "is informed" letter to the universities to say cut it out for these technologies and then go back and change the definition of fundamental research. And I don't need to tell you guys, but an agency's regulations belongs to the agency, they can change it any time they want. Why wouldn't they do it? Over.

Senator HEINRICH. Okay. Thank you.

Chairman WARNER. And one of the things, I think, Senator Heinrich, when you asked that question, as we've seen on the intel side, you've got some pretty good folks who do some pretty good research in issue areas. But at least the folks on the Intel Committee, they can't even look at what we're doing domestically. How we figure out where that's located and letting them have a full 360 would be really important.

Senator BLUNT.

Senator BLUNT. Thank you, Chairman.

Dr. Murdick, we're in conference right now on a bill regarding largely competition with China. Most of us, if not all of us, are free-market thinkers in terms of how things should sort out. But clearly, what is the best way to compete with a country that largely subsidizes and moves quickly in technologies without either regulation or without having to have total outside financing to be your competitor? Do you think it's reasonable that in these areas like chips that the United States makes a government-taxpayer-funded commitment to bring that industry back here?

Dr. MURDICK. With respect to competition with China, I just wanted to have one meta comment or high-level comment, which is the U.S. strength is because we have a highly distributed system. We do not run a command economy. We have a lot of innovators working, a lot of people moving. There are times when we get the need for the government to step in to correct subsidies that are happening within China or other places. So I do think it makes sense to step in when it's been very clearly identified. We've lost a core capability of chip manufacturing. It needs to be done in a way that enables the diverse and distributed innovation system to flourish. We can't put it under a thumb or put it in a constraint in a cage that tries to control too much of how it happens. But I do think that we clearly have identified there's a gap here. We can bring back a manufacturing capability if correctly executed, that will enable us to bring that competition back.

Now, there are a number of other areas that will also need this kind of attention. And that's why I mentioned that we need to be monitoring and dynamically watching the situation because it's a very fast and rapidly moving space. And it moves at a speed outside of lawmaking in its traditional form.

Senator BLUNT. You're saying we don't want to find out that suddenly we're behind like we might have a few years ago in 5G, for instance?

Dr. MURDICK. Yes, exactly. And I think there are very discrete and clear things that we can do to make sure that that information is flowing. To Senator Warner's last point, we don't have a good

foreign-domestic, red-blue analytic view that we have wonderful intelligence assets that can find very pristine and immaculate information that will help. But that needs to be contextualized effectively with an unclassified base that these pristine and exquisite sources can augment insight. I do think we have the opportunity to do this, if that's helpful.

Senator BLUNT. Alright.

Dr. Mulvenon, do you want to add anything to that? This idea of how we compete with countries that are highly subsidized?

Dr. MULVENON. Well, I think the first thing I would say, Senator, is that we shouldn't compete alone. That in particular one of the things that I support about the current Administration's policies is the emphasis on a coalition of the willing in particular tech areas, looking at how we can bring together countries with similar value systems, democratic countries, similar legal systems, and break down some of the barriers that we have between us. A very good example of that is in 5G. We are all aware of the fact that for a long time Huawei was the only company that really had an end-to-end offering from handsets to servers and base stations. But the obvious industrial coalition between companies like Cisco and Juniper and Nokia and Ericsson would have fallen afoul of antitrust regulation unless the U.S. Government effectively moved to break down those barriers, so that there could be an alternate 5G end-to-end offering to compete head-to-head with Huawei. That is a solvable policy problem, particularly given the likeminded countries that we're dealing with.

So, I would just say not competing alone, but using our OECD allies, and I'm including the South Koreans, the Japanese, the Singaporeans, the Taiwanese, all of our European friends. We obviously have a lot of work to break down a lot of our barriers, common data privacy protections first—.

Senator BLUNT. Let me see if I can get one more question in here for Ms. Nikakhtar.

I was interested in the discussion Senator Collins had about pharmaceuticals. One question that's come up that I wonder about is the United States, with vaccines, obviously, a big thing now. Do we have the capacity within our own system to produce and deliver end-to-end vaccines without dependence on China, particularly, or outside the United States supply chains?

Ms. NIKAKHTAR. Thanks for that question.

There are a lot of pharmaceuticals and active pharmaceutical ingredients that we can actually make in the United States if we use our current facilities and we're able to retool and re-shift so we can produce them. I think the first step is to look at what our manufacturing companies, our pharmaceutical companies, not just what they make today, but give them a survey of all these active pharmaceutical ingredients and say what can you do with the facilities you have? What's the lead time? What's the cost? And okay, now that I can solve that in a case of emergency, what can I actually now not make in the United States and maybe Canada? And then, how do I solve for that?

Senator BLUNT. That sounded like a no, but we could get there.

Ms. NIKAKHTAR. No. Exactly. That's right. No, but we can get there.

Senator BLUNT. Alright. Thank you, Chairman.

Chairman WARNER. I think we've seen in the midst of COVID where something like 80-plus percent of the APIs were coming from either China or India.

Senator King.

Senator KING. Thank you.

First, Dr. Mulvenon, I absolutely agree. I think it's a huge mistake to not take advantage of our allies. And if you add the EU and us and Japan and South Korea and Australia and other countries, we're bigger than China. We have a bigger market and a lot of intellectual horsepower, so I think that ought to be part of the strategy. And having uttered that word strategy, it strikes me that what we're doing here today is we're throwing darts at a policy dartboard. And this whole thing started with your discussion of the detailed strategy and doctrine that the Chinese had developed. I believe we need to do that same kind of thinking. Our policy toward China is all over the place. It involves trade, it involves intellectual property theft. We haven't even mentioned the word military here today—enormous military competition. And I feel that there's no comprehensive or cohesive or comprehensible overall strategy.

Dr. Mulvenon, I just served on a commission on cyber, a national commission. It involved Members of Congress, private sector, and members of the executive. And I found it a very useful exercise to be assigned to think about a large issue in a comprehensive way.

Do you think that we ought to be thinking about having a national strategy to deal with China?

Dr. MULVENON. Well, we do have elements of a national strategy. I wish it was more explicit. Obviously, we were all disappointed that Secretary Blinken got COVID last week, because he was going to articulate for the first time, I think, the comprehensive nature of the strategy. And I think that is coming eventually. The Indo-Pacific framework that was published gives us a lot of clues.

But I would say the following. Industrial policy is a 16-letter word, not a four-letter word. We've had a lot of really successful industrial policy——

Senator KING. I agree with that, by the way. And in facing a rival like China, we've got to get over our aversion to the idea of industrial policy, which indeed we are on the CHIPS Act. That's industrial policy.

Dr. MULVENON. Well, I mean if you go back to the Eisenhower Interstate System, there are ways in which we can have market-based policy solutions that are industrial policy that are not socialism, to be fair. And semiconductors in particular, which is a major focus of mine, I agree with General Selva when he was the vice chair of the Joint Chiefs he said, we can't protect everything. He said, I want to protect semiconductors because that's the hill I want to die on. Because it's the foundational technology under all of the other advanced technologies.

Senator KING. And that is something that we are taking an active role in. But I think that your example of the scientists working on advanced semiconductors, who are Chinese nationals—I mean we've got to just be more sensible about this.

Let me ask a broader question. China had this explosion of economic growth and now they seem to be re-imposing the old central planning. Everything is controlled from the government. Is there a danger that they will not kill, but stifle the golden goose by re-imposing a state central planning dead hand of government on what was really a capitalist explosion?

Dr. MULVENON. I agree with you, Senator. I have been, frankly, stunned by the retrogression in Chinese economic development over the last decade because private sector enterprises, private enterprises accounted for a huge majority of the amazing growth of the Chinese economy between 1978 and the late aughts. But the current regime is clearly focused on re-centralization of planning, re-emphasis on state-owned enterprises, and frankly, a squelching of entrepreneurship. The recent crackdown on the tech companies that were outside of government control. And to Senator Warner's point, it's no accident. The last time I was in China, you went in a bookstore and there was a whole section of the bookstore with books of some variation of a title of Where is China's Steve Jobs? And the idea was that they were looking for innovators, but——

Senator KING. He's probably in jail somewhere.

Dr. MULVENON. Or forced under common prosperity to give away millions of dollars of his hard-earned money. But the idea was that the political and legal and intellectual property milieu in which you have to innovate in China does not encourage mavericks to rise up through the system, as I think that Jack Ma and others have discovered in the last two years.

Senator KING. I don't think we can rely on that to save us, but I do think it's a factor in what's going on now.

I have this feeling—I serve on the Armed Services Committee—and of these two heavily armed blind giants stumbling toward one another in a conflict that neither one wants and it would be catastrophic for both. But there needs to be some discussion about where we want to go. The old saying is if you don't have a destination, you'll never get there. And I think we need to have a better definition of where we want to get and have a more comprehensive thought about how we want to deal with China on a whole series of levels.

Thank you, Mr. Chairman.

Chairman WARNER. Senator Cornyn.

Senator CORNYN. Thank you, Mr. Chairman, for this hearing. This is exactly the sort of hearing we need to be having, an open session so that not just the Committee can hear, but the American people can hear and be better informed about the competition that we're having with the PRC and the Chinese Communist Party.

Ms. Nikakhtar, I was happy to see that you cover in your written testimony the importance of an outbound screening mechanism. And I'd like to get you to talk about that first, and then maybe have the other witnesses talk about it as well. As you noted, Senator Casey and I have a piece of legislation called the National Critical Capabilities Defense Act. But some of the figures that you mentioned here, Mr. Mulvenon, I think from these figures that we see here in this testimony, it looks like U.S. venture capitalists have funded the rise of the Chinese economy. And we know they don't play by the same rules that we do and they don't follow the

law. They shamelessly steal secrets and they coerce American investors into joint ventures, steal their IP and their know-how. And of course, that was part of what we tried to address in the CFIUS reforms. But we also tried to include an outbound screening mechanism to see what American companies were doing investing in China and its impact on the United States, not only from an economic standpoint but from a national security standpoint.

And I want to thank Senator Casey for working with me on this, and I with him. Thankfully, the House COMPETES bill has a piece of that in it. And I think it provides us an opportunity in the conference committee that a number of us are on to try to include this in that final conference report.

But Ms. Nikakhtar, you mentioned in your testimony that this could be one of the most important pieces of legislation before Congress today. And the numbers that you mentioned here totaling $3.5 trillion in market value of holdings by U.S. financial investments in China in 2020. Of course, we know this is a part of the CHIPS Act. The semiconductor bill is going to be focusing on providing incentives for re-shoring of semiconductor manufacturing. But these companies are global companies. And I for one, and I bet I'm not alone, don't want to see those companies using some of these taxpayer dollars that we're trying to provide to incentivize reshoring of semiconductor manufacturing to enhance their investments in the PRC, which is exactly where we are and who we are competing against.

Maybe you can start and talk about why you think this is important and then hear from the other witnesses.

Chairman WARNER. Before the witness starts, I just want to indicate that because of the voting, I'm going to run and vote and come right back and we'll move down the line. But I think Senator Cornyn's got a very good question.

Vice Chairman RUBIO [presiding].

Ms. NIKAKHTAR. Senator, your question is about the outbound legislation, right? And the importance of that?

Senator CORNYN. It was about the outbound screening mechanism and the National Critical Capabilities Defense Act.

Ms. NIKAKHTAR. Okay. Perfect. I just wanted to make sure.

No, like I said and you pointed out, it's one of the most important pieces of legislation because this is a gap in the laws. We have the limits of export control jurisdiction. What is that? U.S.-origin items and then certain items produced from technology. But this doesn't involve the movement of plants abroad. This doesn't involve the companies that are forming joint ventures or just like building facilities in China and then developing technology in China. Even if they avail themselves of the CHIPS Act money—and I know the CHIPS Act is so, so important—there's got to be guardrails so they don't double down and make more investments in China because of the revenue saved because we gave them taxpayer dollars for subsidies.

Back to the outbound legislation. Right now, legally, we actually do not have the ability to stop this flow of dangerous capabilities to our adversaries. We're not talking about the rest of the world. We're talking about the adversaries.

And I just wanted to give you some really, really critical examples of where export controls—. We don't control these things. We don't control lifesaving medical cancer detection equipment. Semiconductor capabilities, even those that are below controls, what good is it to move things abroad when we can't even make any of those in the United States? High-capacity batteries. We are struggling to make lithium ion battery cells in the United States because we've moved everything over to China. Materials, chemicals, critical material chemicals. People don't adequately understand how much of the chemicals that we're enabling China to produce. Active pharmaceutical ingredients, we already talked about that. I can go on for hours listing technologies. We certainly don't have that time, so I'll stop there.

But I really want to say, look, by moving the supply chains there, we've become hostage to our adversaries. Businesses will not protect national security. That is not their job. That's the government's responsibility. And thank you, thank you, thank you for identifying this gap in the law and developing a legal mechanism to fix it.

Senator CORNYN. Can I let the other two witnesses comment briefly?

Vice Chairman RUBIO. Yes, you can.

Dr. MULVENON. Senator Cornyn, you may remember actually a member of your staff invited me to testify before Senate Banking. And I think I was the only person on the panel in favor of FIRRMA against the venture capitalists and the other corporate types. And I was very happy that it passed. Of course there were some pieces missing from the original legislation, in particular monitoring of JVs in China, and the outbound investment.

I fully support the legislation and the concept paper, which I read first, about the legislation. And the two things I like best about it are, first, the way you parameterized the first tranche of outbound investment that would be subject to the regulation, clearly delineating what was subject to it and what wasn't. And also, your point that we shouldn't wait for allies. That we needed to be able to make a lot of those moves unilaterally first and let our allies catch up with us. And I think those are the two strongest parts of the bill.

Vice Chairman RUBIO. And I'm sorry to interrupt. I promise, we will get back to that second answer, Senator. But we're running out of time on this vote and I want to make sure Senator Bennet gets to vote.

Senator BENNET. I really appreciate that, Mr. Chairman. Thank you very much. We're running out of time on the vote.

I wanted to come back to Dr. Murdick's red-blue analogy in terms of our analytic capabilities. And it hopefully suggests a way forward. Senator Sasse and I have been working on several bills to better position ourselves for the competition and better direct our investments. In the last year's Intelligence Authorization Act, we advanced a national technology strategy which we continue to push forward. We're currently working on a bill to establish the capability to conduct technology net assessments in order to determine U.S. leadership on critical technologies relative to other countries, particularly China. What we found through our work on this Com-

mittee is that while the Intelligence Community looks at what China and other countries are doing on emerging technologies, no one in the government, as we were talking about earlier, is really looking at how such trends compare to the U.S. private sector activity.

Our new Office of Technology Net Assessment would review U.S. competitiveness and technologies critical to economic and national security based on a fusion of intelligence, including open-source intelligence and commercial data.

Would a capability like this help us determine where we need to direct investment and answer some of the questions we're asking today and protect leadership and technologies that matter most to U.S. economic and national security, do you think?

Dr. MURDICK. Clearly, the net assessment type model is quite exciting and has a lot of potential. And I think that pursuing that kind of approach makes a lot of sense. I think it's important, wherever this capability is, that they have the authorities and incentives to be able to answer the questions in a full way. Authorities, meaning that they can get at both the red and blue like you were highlighting.

I think that's a central point. And also the incentives. The U.S. tends to use open source as a complement for SIGINT and HUMINT and other sources. And I think other models are using the open source as a first resort and then laying on top of that the classified sources. I think to get another assessment, it's important that you look at the big picture first and then fill in the pristine information on top of it. And so it's a methodological—in making sure those incentives are honored.

Senator BENNET. We'd like to work with you on that. And with the last couple of minutes remaining though, thank you for your testimony. I think it really is important and I'm very, very pleased that Senator Cornyn said what he said about the importance of doing this in public.

I think it is very clear too, having been on this Committee now for however many years it is, that our failed experiment of prioritization and making stuff as cheaply as possible in China has been just that, a catastrophic failure for the United States of America. And it's going to require something totally different for us to compete.

I wonder with a couple of minutes left, what does that industrial policy look like? How do we do it in a way that harnesses the imagination of the capitalist system that we have, as opposed to the way that the Chinese are doing it? And finally, how are we going to know that we're actually succeeding so when people are sitting at that table at some point in the not-too-distant future, they're actually telling a story about how we're outcompeting rather than have our lunch eaten by Beijing?

I don't know who would like to start, but I'd be happy to hear all of you or any of you. Thank you.

Ms. NIKAKHTAR. I can. Go ahead.

Dr. MURDICK. Just very briefly. I'll be short, though. This is a good time to re-engineer our innovation system and to be able to think about—. There is a good friend of mine who wrote a paper dealing with the system, re-engineering of the American R&D sys-

tem. There are options and ways to be able to take the strengths of the U.S. system and be able to effectively engage in a way that recognizes the government authorities that we actually have—where we actually have authorities, where we can engage and where we should be letting the innovation system work in that beautiful American way of it's hard to predict.

Just a very small comment. I'll let you go deeper.

Ms. NIKAKHTAR. Thank you.

Look, representing industries, folks are really excited about this potential for industrial policy and many of us have been champions of it for a long time. What you see is you were getting a lot of excitement. You've got companies with really exquisite IP, clean rare earths processing, for example, that actually have the IP, but they've never really had the financial means to get this launched.

There's a lot of IP that's in the works that this is also catalyzing. Catalyzing is the key word. But I think to make this successful, these companies are still reluctant to make the investments in the United States because they're like, I'm going to be displaced by cheap Chinese stuff because China is configured to outcompete all the time. They're really freaked out about that.

We've got to think of a mechanism that once our industries through our industrial policy are growing, we're able to really cut out unfair predatory competition.

And then finally to your last point, how do we know that we're succeeding? When the world starts buying our goods and not the Chinese goods.

Vice Chairman RUBIO. Senator Casey, you voted already?

Senator CASEY. I did.

Vice Chairman RUBIO. Okay.

Senator CASEY. Mr. Chairman, thank you very much. I want to thank our witnesses. I'll focus my question and some comments before it on Ms. Nikakhtar. In particular, I'll be quoting you in reference to some of the areas of questioning that Senator Cornyn raised on outbound investment.

I wanted to start by way of a predicate quoting the 2022 Annual Threat Assessment. It says in pertinent part, quote, "Beijing's willingness to use espionage, subsidies, and trade policy to give its firms a competitive advantage represents not just an ongoing challenge for the U.S. economy and its workers, but also advances Beijing's ability to assume leadership of the world's technological advancement and standards." End quote.

In your written testimony, you note, quote, "U.S. financial investments in Chinese-domiciled companies total over $2.3 trillion in market value of holdings at the end of 2020." This is on page 24 of your testimony when you make that statement. And then you have just above it, a list of the capital and investment types. It's just breathtaking. It's everything from telecommunications to robotics, biotechnology, AI, surveillance, semiconductors, pharmaceuticals. It goes on and on. That gives people a good sense of the challenge we have.

Later in your testimony, you say, and I'm quoting here, "We have for centuries regulated the transfer of defense articles to foreign adversaries. Today in much the same way, we need to regulate the

transfer of technology, economic flows, and supply chain capabilities to them." Unquote.

And as Senator Cornyn mentioned, we have the National Critical Capabilities Bill and you talk about that in your testimony as well, in some of your earlier testimony.

I guess a two-part question. One is, what are the limits of existing regulatory tools, including export controls? That's question one.

Question two is why is an interagency outbound investment review mechanism necessary to win the competition with regard to the Chinese government?

Ms. NIKAKHTAR. Thanks for a really thoughtful question.

First, what are the limitations of existing regulatory tools? I think we have a lot of gaping holes in our export control system and I think we really need to tighten those up. Greenfield investments. I mean, gosh, what an incredible way that we're allowing domestic investments to be exploited.

Really, the transfer of sensitive data—data centers—not to the rest of the world, but to adversaries who we know are going to take the data from our data centers and use it for their AI machine. That's another area. And then certainly the outbound investment mechanism because—. We talked about the limits of export controls. So when you have these facilities in foreign countries and you develop the technologies there, release technologies there, aren't critical manufacturing capacities there, we empower them and not ourselves in the United States.

But another point that your thoughtful question had me realize is that China has all these national security laws that actually have companies that are in China, transfer data to them whenever the CCP wants. And then, they have the corporate credit system, like the social credit system but for corporations. It even applies to foreign corporations in China, that if you don't act anytime that the CCP wants to enable them and to act in their best interests, they can take all these adverse actions that the EC Chamber of Commerce, European Chamber of Commerce, basically said that it amounts to life or death for a company.

And we're allowing our companies with critical capabilities to go over there. It makes no sense. And again, I really want to stress that it is not businesses' responsibilities to take care of national security. It is all of yours. And then, thank you for what you doing. Remind me of the second question.

Senator CASEY. Why would this outbound investment mechanism be necessary?

I know you've said it. I would just like you to restate it.

Ms. NIKAKHTAR. Like we said. China has made abundantly clear. This isn't McCarthyism. China's made it abundantly clear that it is holding our supply chains hostage to gain leverage, not only for the United States but the rest of the world. That's why we need this legislation. Thank you.

Senator CASEY. Thanks very much. Thank you, Mr. Chairman.

Vice Chairman RUBIO. Senator Sasse.

Senator SASSE. Thank you, Chairman. Thanks to all three of you. This has been an informative hearing. Obviously, in the SCIF we cover topics like this regularly, but it's clear that the American peo-

ple broadly don't understand these issues. And corporate America certainly doesn't.

I've become increasingly concerned as I learn more and more about how premier U.S. law firms ostensibly represent private, in scare quotes, Chinese companies, where American lawyers work on cases in what feels a lot like a revolving door of senior government officials leaving Administrations going out and being hired at law firms. And then a lot of their clients become these Chinese fake private companies. As Chairman Warner says again and again, our beef is not with 1.4 billion Chinese people created in the image of God. It's with the Chinese Communist Party and their malevolence and their export of surveillance-state autocracies and their genocide in Xinjiang and more and more.

Could you walk the American people through how China uses former U.S. Government employees and particularly those who've had access to our government secrets?

Ms. NIKAKHTAR. Yes, it's really terrifying. What is the Stalin quote? We'll use the rope that the capitalists sell us to hang them. There's debate on whether that's a quote or not. But the true thing is that it's money. It's money, money, money. When the Chinese companies dangle money in front of folks who've been in the government and have access to exquisite data and know how the ins and outs of the government work, know how to exploit regulations, it's really hard for people to say no to money.

And so you see this revolving door and then there's various reasons why people go into the government. But one of the key reasons is to get a better job on the way out. When the CCP exploits that with being able to pay a lot of your bills—all your legal bills. And when there's this rat race within law firms, who can generate more revenue and with status within the firm, who can generate revenue.

How do you resist that temptation? The way my firm does it is we bring trade cases against China, so there's an inherent conflict of interest. So, I don't have that. But most, as you pointed out, law firms don't. And so then how do you resist all of these temptations and these expectations of you that you're supposed to generate revenue, when the Chinese make it so easy?

Senator SASSE. And what is the Chinese government via these companies seeking advice about from these law firms? Is their goal better governance compliance?

Ms. NIKAKHTAR. Yes, it's twofold. It's just lobbyists. Lobbyists. Just pepper the government with lobbyists, so they can just hear, hear, hear from an echo chamber. And the other one is they hire people who know people in the government and then know how to manipulate the laws. The more you know the intricacies of the laws, the more they're interested in you because you can build in nuances to basically create backdoors for them to circumvent the laws.

And that's what they're looking for.

Senator SASSE. Anything the two of you want to add to this?

Dr. MULVENON. Senator, it certainly is a function of our open system, which is in stark contrast to the opacity, of course, that our companies face on the Chinese side. And perhaps that's worthy of some mention. All of the proliferation of documents that I men-

tioned, many of which are unpublished. Our companies will go into meetings with ministry regulators in China and the regulator will push and draft unpublished regulation across the table for them to read and to be enforced. And they ask, can I keep a copy of it? And they said, no, that's just an unpublished draft and pull it back. They don't even have the ability then to seek remedy with the U.S. Government or with other people who could help them in those situations. Not to mention the fact that, of course, while there have been some improvements in the intellectual property courts in China, the court system itself is not an independent branch of government. It is fundamentally dominated by the Chinese Communist Party. And the judges in those courts are first and foremost responsible to the Communist Party discipline before the legal discipline.

That is just one of these unbelievable asymmetries between the two sides and further creates that asymmetric environment for our companies.

Dr. MURDICK. I'll take on one small part of this. One of the challenges in working in the government is you have limited time to think and you don't have a lot of space to do that thinking. You tend to rely on what's being said outside, because you need someone who has had time to be able to draft out, particularly in emerging technology spaces because these are very complex. They're technical—technically hard to understand. There's a lot of players involved. It's important to get that information.

And I think that information dearth that we've put on Senators and Congress, individuals, as well as Executive Branch, actually puts you at an increasing disadvantage because you're actually dependent on people outside, who might actually have a conflict of interest, to inform you on what to do. And therefore, coming back, I do think there is an opportunity to increase this analytic insight so that you can be informed by sources that conflict of interest is more clearly controlled.

Senator SASSE. I know I'm nearly out of time. It's been reported that there are currently 20 former Senators and Congress people that lobby extensively on behalf of the Chinese government and Chinese fake private corporations. Is there any reason why that is in the interest of the United States citizenry or governance?

Ms. NIKAKHTAR. I've thought a lot about this, and I really want to answer this question because I don't understand what their end game is. If you're taking money from the CCP and you're lobbying on their behalf, at some point somebody's going to have to win this conflict. And if we lose, where are you going to run? Where are you going to hide? You've actually enabled this to happen. And when China is the dominant power and we become a vassal state, it's affected you too. I just fundamentally do not understand why these people are trading in their future, their children's future, for a few dollars today.

Senator SASSE. Thank you.

Vice Chairman RUBIO. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman.

First question for you, Ms. Nikakhtar. I'm very troubled about the use of the $10 trillion private equity industry to mask investments by Chinese-government-linked actors in critical infrastruc-

ture and technology. And you may be aware that as Chairman of the Senate Finance Committee, I've been working on legislation that would close disclosure loopholes for private investment vehicles like hedge funds, private equity, and venture capital firms.

In your view, would there be a national security interest in fully understanding who is behind these funds that are acquiring companies with critical technology?

Ms. NIKAKHTAR. A hundred percent.

We've got to explore all of the disclosure loopholes and close those. And then when we trace the financing back, it has to go back to the ultimate beneficial owner. And I think companies do not do adequate due diligence to figure this out. And I think sometimes our intelligence communities fail to do that.

Senator WYDEN. Would it be fair to say you believe legislation requiring disclosure of beneficial ownership of these very large investment vehicles would make the CFIUS review process more thorough and efficient?

Ms. NIKAKHTAR. Yes, Senator, I do. And I would actually take it a step further. I actually think that companies that do business of a certain dollar amount with the CCP need to disclose that to the government, too, so we really understand what these transactions are that companies are making. So, yes. And then again, I would take it a step further.

Senator WYDEN. It'd be fair to say between the two questions I asked and the additions you just made, where you said you'd go further, you think to a great extent, we're just pretty much in the dark with respect to anything resembling useful, fulsome information about these funds?

Ms. NIKAKHTAR. As the former head of CFIUS at the Commerce Department, yes, we were completely in the dark. Our Intelligence community didn't have adequate information. And I was frequently in the office until three in the morning using any open source information I could to get to the ultimate beneficial owner. So, yes.

Senator WYDEN. That really is what you are left with is just flailing about trying to find open source, when, if we had government doing its job and insisting on disclosure and insisting on accountability, you would have that information. Is that fair to say?

Ms. NIKAKHTAR. Flailing about, yes. Sometimes I found really good data, yes. And a lot of sleepless nights, yes.

Senator WYDEN. Very good. You clearly have the expertise to use open source information. I don't think it should come to that. I think we ought to be adopting the suggestions.

Ms. NIKAKHTAR. You're absolutely right. It was just tongue-in-cheek. It was never through open source, the exact type of information I need to take it across the finish line. You're absolutely right.

Senator WYDEN. Very good.

Dr. Mulvenon, I am told you're an expert in China's Internet censorship. This has been an issue of great importance to me, and on the Finance Committee in particular. And we have looked at the way the Chinese government uses Internet censorship to silence its critics. Internet censorship, whether at the hands of the Chinese government or nominally private companies not only undermines free speech and human rights, but has an economic impact on companies who can't or won't be able to participate in markets under

those terms. For example, a recent U.S. International Trade Commission report described how censorship is creating barriers to the entry of U.S. tech firms in China and protects Chinese companies from competition.

The question would be, given China's expanding economic influence, how do we stop the PRC cyber and censorship policies and its views—very odd and ominous views—on Internet sovereignty from spreading outside of China?

Dr. MULVENON. I agree with you, Senator. I've been looking at this issue for a long time. We're entering a new era where the Chinese model, if you will, of the so-called panopticon surveillance state is now being globalized. We used to talk about the Chinese Internet censorship issue largely in a China context in terms of inbound and outbound information from China itself. But the export of the Chinese surveillance industry, whether it's via SmartCities in Africa and other belt and road countries, up to and including China's proposals to the international standards bodies, which propose, frankly, a re-architecting of the Internet and Internet 2.0 that is extremely surveillance friendly and very national sovereignty friendly, vice our traditional model of focusing on a global notion of Internet freedom.

Senator WYDEN. One more question if I might ask. There have been a number of reports of the PRC using its economic power, in particular its status as a market for American entertainment, to influence the movies and the television that Americans consume. Doctor, what do you see is the future of this kind of censorship and how widespread it might be?

Dr. MULVENON. Frankly, I've been deeply troubled by the trends over the last 10 or 15 years where major studios, because of China's rapidly growing theater market, are reluctant to depict any negative depictions of China in movies up to and including, as I'm sure you're aware, the CGI re-rendering of the remake of "Red Dawn" where all of the Chinese in the movie were remade through CGI into North Koreans so that studio did not anger the Beijing regime. And I don't see how we reverse that given the economic pull of the theaters, except to acknowledge that it is in fact happening and it is fundamentally not compatible with our values.

Senator WYDEN. Mr. Chairman, can I get one last question in? Thank you, Mr. Chairman.

This influence, obviously, of the PRC could be indirect. For example, Twitter's owner has heavily invested in China. Tesla cars are manufactured in China, rely on the Chinese market, depend on Chinese lithium for batteries. Do any of the three of you have concerns that the PRC might try to leverage Tesla's dependence on China to limit anti-PRC content on Twitter?

Ms. NIKAKHTAR. Can you repeat the last part? I had a hard time hearing.

Senator WYDEN. Do you have concerns that the PRC might try to leverage Tesla's dependence on China to limit anti-PRC content on Twitter?

Ms. NIKAKHTAR. Absolutely, absolutely.

By having more of any company's operations and supply chains in China, we're giving them full ability to basically be the puppet master and dictate how these companies operate companywide,

owner-wide. Once you hold them hostage, you can essentially compel them to do anything. And people forget that in China you don't have the ability to make decisions yourself.

Senator WYDEN. I'm way over my time. If either one of you want to make a quick comment, please do. But I get the sense that maybe the previous answer to my question is in line with the other witnesses today. Is that true? Okay. Thank you.

Chairman WARNER. I'm going to momentarily bigfoot for one second, since I've got a TV headline upstairs. And this will be a lightning round. We touched a little bit on this earlier around, and I agree that the alliance of democracies. Should that be—brief, brief answers because I've got one more question quickly after this and then I want to get Senator Sasse to close out.

But should it be a formal alliance or not? I had pushed the Administration to maybe think about this in a more formalized way. There are good arguments both ways. There might be different alliances on different issues. Although I'd point out the fact that by not having some formal alliance approach on semiconductors, for example, Germany is moving even quicker than us, even though we had the idea to start with. Maybe done it in alliance?

But I think you got the gist of the question. Right down the line: formal alliance, not formal alliance in recognizing it? Maybe different countries. If you had a core group, you could expand or contract based upon the technology.

Dr. MURDICK. Yes, I think if you're dealing with the right parties who actually have the play in the question, I think a formal alliance makes a lot of sense. I think most of these questions, for them to be effective, require multi-party engagement because a single actor trying to stop a multi-party system just gives an opportunity for people to run around that single actor saying no.

Ms. NIKAKHTAR. Some formal, some informal. Sometimes our allies don't want to be out there because the fear of repercussions from China. On a case-by-case basis, sometimes formal, sometimes informal, to give our allies top cover.

Dr. MULVENON. In my 2021 word bingo was plurilateral. In other words, by specific industries or specific technology, so that you only have the right countries in the room. Semiconductors, for instance. We know the Netherlands has to be in the room because of ASML and their EEV technology. But if you keep it small like that, then you can set standards and you can have industrial planning within those small groups and have coherence, whereas you can't have that at a multilateral level like the Wassenaar Arrangement, which is just too big, too diffuse.

Chairman WARNER. My concern with that—I'll go to the last question—and I'd like to get the response. Then I'm going to turn over to Senator Sasse. And I apologize for jumping back in like this—is that when you're thinking about technology development, it's hard to decide who the right countries are at the right end. Maybe we're doing some of this in a NATO level. We're doing some of this at a QUAD level. I don't know. It's a fair question that most of you are not completely unformal, but I'd like to continue that.

The second half of this, which we've talked a lot about, the need for us to make investments. I do think, particularly Dr. Murdick, some of your ideas about how we might structure this in the gov-

ernment makes sense. One of the things I'm concerned with is our first time out of the chute here has been semiconductors. I would posit if you didn't have a huge high-employment industry that was losing share, and we didn't have the moment of COVID where suddenly that supply chain loss drove beyond even the industry, I'm not sure we would making this kind of $52 billion investment.

How would we ever—? Maybe I'll just leave this for the record and you can come back to me on it. If it's a new technology, where China's about to sweep the field, and there's not a mature industry to invest in that's got the lobbying power here or we're not seeing the immediate repercussions of that until potentially years down the line, how do we make a decisionmaking process that at least elevates this to say you, Congress, ought to be thinking about making a major investment?

And I would love to get your answers on that but recognizing that I've abused my jumping in front of my friend. Senator Sasse, you get to close out this. And thank you, thank you, thank you. We've had a large number of my colleagues on both sides of the aisle who have come up and said, very good hearing.

Senator Sasse.

Senator SASSE [presiding].

Senator SASSE. Chairman, thank you for scheduling this in public. It's a very important topic. I wish I could hold you all hostage for half an hour, but the reason I'm the only one left here is that the vote closes soon, so I'll also ask you to speak quickly.

But pursuing more of what the Chairman just said, I want to get back to something like a D10 or a D12 technology standard-setting and free trade agreement.

But first, explain to us what is Chairman Xi doing in his own tech crackdown right now? What's motivating him?

Dr. MULVENON. Well, I think that there is an inherent suspicion in the Chinese central government about private entrepreneurship. You see this. There's a number of indications and warning of this. One is the re-imposition of the requirement for party committees within private enterprises as the only reliable mechanism of political control that they're familiar with.

Secondly, it is fair to say that Alibaba and Tencent were reeled back in because they had been so fabulously successful at creating a new mobile digital payment market that it was having a negative revenue effect on the Chinese state-owned banking system. And so in some sense what you see is the revenge of the regulators because of course the state banks and the state bank regulators are the same people just rotating jobs every couple of years. There was a sense that as they were developing eCNY and their own digital currency that they could imagine—this is my prediction, that there will be a future in which the Chinese state digital currency will subsume what had previously been the private enterprise mobile payment system, and that would allow them to have that kind of central understanding of what's going on, on their central blockchain, which helps them with their capital flight concerns, helps them with their anti-corruption investigations.

There's a lot of things merging together, I think, that explain why they didn't want so-called rogue elements. It's also true, by the way, that these entrepreneurs that they're reining in are not mem-

bers of the tribe, in a sense. They're not red princelings. They're not red family members. They have not asked under common prosperity for any high-ranking party kid to give millions of dollars to charity. There really is this sense from Xi Jinping that there is a red tradition and that there are groups of people that he trusts. And these by-the-bootstrap entrepreneur guys were not in that circle of trust. That's just my personal view.

Senator SASSE. Very helpful. And what's the state of the internal debate with Xi and his closest cronies about a digital decoupling that they rather than we initiate?

Dr. MULVENON. Well, I actually agree with the idea that it's a false dichotomy to say that the U.S., viewing this hyper-globalized economy, seeing these early problems with the pandemic, has now been the one that is decoupling. It is important to remember from a regulatory perspective that the Chinese state has never allowed us to invest in areas like telecommunications services and other areas. So to get upset about removal of Huawei equipment from the U.S. telecoms market, the natural question is, what is the current Ministry of Industry and Informatization allowing companies to do in their market?

I would argue that their protectionist system was a form of decoupling even before we began thinking about re-shoring. I think the causation era was backward in terms of blaming the U.S. now for severing connections with China.

Ms. NIKAKHTAR. And may I just quickly add to that? To the extent that U.S. businesses don't care, I try to remind them all the time that as China's digital currency flourishes, this is a mechanism to displace U.S. and Western competitors to manufacturers out of the market because they're just not going to accept dollars.

Senator SASSE. Helpful.

Sir?

Dr. MURDICK. Just to add in one more point on the last question. Obviously, I'm not privy to the internal discussions that are happening within China. However, there's a very interesting, I referenced it earlier, this Peking University piece from The Institute of International Strategic Studies. At the very end of this document they lay out, basically, the dynamics of technical decoupling has evolved from a one-way to a two-way process. China and the U.S. have different starting points, but they are moving toward a common goal, which objectively facilitates a two-way decoupling trend. Whether the technology level or industry level. Both China and the U.S. are facing losses brought about this decoupling and China's losses might be greater at this point.

There is a clear thinking about this as a two-way process. And I think it's really important to understand that they recognize there are losses involved in this space. But this seems to be an ongoing discussion, and they're monitoring whether they can convert from a loss position, which is what it seems that they're assessing, to a position where they can have a little less loss.

Senator SASSE. Very helpful. The vote is technically closed, so I need to sprint to it. But on behalf of the whole Committee, thank you for all three of your work and your time with us today. I'm going to followup with you with some more questions related to an

ideal version of a D10 or a D12 or a TPP with technology standards and teeth.

But thank you for your work. This hearing is adjourned.

[Whereupon at 4:45 p.m., the hearing was adjourned.]

○