HEARING ON CURRENT AND EMERGING TECHNOLOGIES IN U.S.-CHINA ECONOMIC AND NATIONAL SECURITY COMPETITION

HEARING

BEFORE THE

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

ONE HUNDRED EIGHTEENTH CONGRESS
SECOND SESSION

THURSDAY, FEBRUARY 1, 2024

Printed for use of the
U.S.-China Economic and Security Review Commission
Available online at: www.USCC.gov

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

WASHINGTON: 2024

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

ROBIN CLEVELAND, *ACTING CHAIRMAN*
REVA PRICE, *VICE CHAIR*

Commissioners:
AARON FRIEDBERG
KIMBERLY T. GLAS
JACOB HELBERG
HON. RANDALL SCHRIVER
MICHAEL R. WESSEL

The Commission was created on October 30, 2000 by the Floyd D. Spence National Defense Authorization Act of 2001, Pub. L. No. 106–398 (codified at 22 U.S.C. § 7002), as amended by: The Treasury and General Government Appropriations Act, 2002, Pub. L. No. 107–67 (Nov. 12, 2001) (regarding employment status of staff and changing annual report due date from March to June); The Consolidated Appropriations Resolution, 2003, Pub. L. No. 108–7 (Feb. 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of the Commission); The Science, State, Justice, Commerce, and Related Agencies Appropriations Act, 2006, Pub. L. No. 109–108 (Nov. 22, 2005) (regarding responsibilities of the Commission and applicability of FACA); The Consolidated Appropriations Act, 2008, Pub. L. No. 110–161 (Dec. 26, 2007) (regarding submission of accounting reports; printing and binding; compensation for the executive director; changing annual report due date from June to December; and travel by members of the Commission and its staff); The Carl Levin and Howard P. ''Buck'' McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113–291 (Dec. 19, 2014) (regarding responsibilities of the Commission).

The Commission's full charter and statutory mandate are available online at: https://www.uscc.gov/charter.

CONTENTS

THURSDAY, FEBRUARY 1, 2024

HEARING ON CURRENT AND EMERGING TECHNOLOGIES IN U.S.-CHINA ECONOMIC AND NATIONAL SECURITY COMPETITION

Panel I: Risks of Chinese Information Technology Products in the United States

Panel II: China's Race to Transform its Military Through AI and Quantum

Panel III: China's Progress in Commercial Applications of Selected Emerging Technologies

STATEMEMT FOR THE RECORD

QUESTIONS FOR THE RECORD

HEARING ON CURRENT AND EMERGING TECHNOLOGIES IN THE U.S.-CHINA ECONOMIC AND NATIONAL SECURITY COMPETITION

THURSDAY, FEBRUARY 1, 2024

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Washington, DC

The Commission met in Room 215 of Dirksen Senate Office Building, Washington, DC and via videoconference at 9:30 a.m., Commissioner Jacob Helberg and Commissioner Michael R. Wessel (Hearing Co-Chairs) presiding.

OPENING STATEMENT OF COMMISSIONER JACOB HELBERG HEARING CO-CHAIR

COMMISSIONER HELBERG: Good morning and welcome to the first hearing of the U.S. China Economic and Security Review Commission's 2024 Report Cycle. I would like to thank everyone for joining us and thank our witnesses for the time and effort that they've put into their testimonies.

Thank you to the staff for the time they took to help prepare today's hearing. And thank you to Commissioner Wessel. It's an honor to co-chair this hearing with you today.

While this commission deals with a variety of issues in the U.S.- China relationship, today's hearing focuses on a topic that has rightfully emerged at the forefront of the policy debate in both chambers of Congress in recent months. That topic is technology.

While much remains unconcern about the 2020s and the 2030s, recent events have made it unmistakably clear that technology will be the indispensable precondition for American propensity, security, and national sovereignty in the years ahead.

President Eisenhower once observed, "There is only one thing I can tell you about war, and almost one only, and it is this; no war ever shows the characteristics that were expected. It is always different."

It has now been 79 years since the world last experienced a war between great powers. That's the same amount of time that elapsed between the American Civil War and War World II. Just think of how different the world of the American Civil War was compared to the world on the eve of World War II.

Similarly, the world today bears little resemblance to the world of 79 years ago. If a great power war broke out tomorrow, we can't know exactly what shape it would take, but we do know, as President Eisenhower wisely suggested, that it would bear little in common with the last great power war of the 1940s.

It is, therefore, essential for the future of American security and deterrence to fully understand the implications of recent breakthroughs and commercial and military technologies. America cannot remain capable of winning great power wars beyond any reasonable doubt if it does not remain superior technologically, and conversely America cannot deter great power wars from happening if the world doubts America's capacity to win them.

Since the days of David and Goliath, or the Trojan Horse of Troy, the books of history are full of stories of smarter adversaries out maneuvering larger foes. The greatest risk to America is that we underestimate the importance that intelligence will play in reconfiguring military power in the decade ahead.

We can think of AI as a factory for intelligence, a system that can solve any puzzle, find a cyber exploit, predict the next chess move, locate tanks in a satellite image, anticipate an adversaries' response options, and so forth.

I look forward to discussing at greater length the critical role of AI in the future of the U.S.-China rivalry, and diving deeper into China's adoption of AI into its global military strategy.

Second, technology will be the sine qua non for the U.S. to remain the world's preeminent economic power. In the U.S.-China rivalry, the nation with the most advanced technology will also be the nation with the larger economy.

Look no further than the difference between Israel and Nigeria today. Nigeria has more than 21 times the population of Israel and has 37 billion barrels in oil reserves. Yet, Israel has the larger economy and the stronger military. The reason is technology.

Contrary to popular belief, America can, in fact, stay ahead of China economically but to do so it must also stay ahead technologically. With four times our population, if China simply manages to converge with us technologically and to get to parity on productivity, it could have four times our GDP, and maybe four times our military making it the dominant power.

So parity means the West is losing. Parity cannot be the by-product of American technology policy. Technology dominance should be our north star and that will be my focus today.

Third, technology is challenging our traditional conceptions of national sovereignty. As China's cyber influence increases, the single free internet of the sort American officials once envisioned is giving way to ideologically opposed de facto techno blocs.

The global internet is already divided into between the decentralized democratic internet familiar to Americans, and the centrally controlled internet, authoritarian internet built by China.

The latter is spreading rapidly in the developing world where countries from South East Asia to Latin America have opted to rely on Chinese technology for 5G networks and other critical digital infrastructure.

The influence of the authoritarian internet is also expanding into advanced democracies as companies susceptible to CCP influence become more central to our online lives.

If China's efforts to export these systems abroad are left unchecked, the CCP may soon enjoy the capacity to envelope dozens of countries behind its great firewall and reconstitute 20th century style spheres of influence through 21st century technologies.

Popular Chinese platforms like TikTok make a mockery out of free speech and are internationalizing Chinese surveillance everywhere including in the United States.

TikTok is a scourge attacking our children and our social fabric, a threat to our national security, and likely the most extensive intelligence operation a foreign power has ever conducted against the United States.

Senators Blackburn and Blumenthal are right; TikTok misled Congress. It should be held to account. Americans deserve to know if the CEO of this country's largest news source committed perjury on its relationship with a foreign adversary.

More importantly, American security should be protected and that means the app should be fully divested from its Chinese parent company, or be banned entirely.

But TikTok is far from an isolated case. America is due for a comprehensive rethink of its technology trading relationship with China. I look forward to discussing actionable ways that Congress can mitigate the urgent security risk posed by Chinese hardware and software technologies in the United States.

I also look forward to hearing from our expert witnesses and I will now turn the floor to my co-chair Commissioner Wessel for his opening remarks.

PREPARED STATEMENT OF COMMISSIONER JACOB HELBERG
HEARING CO-CHAIR

Hearing: Current and Emerging Technologies in U.S.-China Economic and National Security Competition
February 1, 2024
Opening Statement of Jacob Helberg

Good morning and welcome to the first hearing of the U.S.-China Economic and Security Review Commission's 2024 report cycle.

I would like to thank everyone for joining us and thank our witnesses for the time and effort they have put into their testimonies. Thank you to the staff for the time they took to help prepare for today's hearing. And thank you to Commissioner Wessel, it's an honor to Co-Chair this hearing with you today.

While this Commission deals with a variety of issues in the U.S.-China relationship, today's hearing focuses on a topic that has rightfully emerged at the forefront of the policy debate in both chambers of Congress in recent months. That topic is technology.

While much remains uncertain about the 2020s and 2030s, recent events have made it unmistakably clear that technology will be the indispensable precondition for American security, prosperity, and national sovereignty in the years ahead.

President Eisenhower once observed, "There is only one thing I can tell you about war, and almost one only, and it is this: no war ever shows the characteristics that were expected; it is always different."

It has now been 79 years since the world last experienced a war between great powers. That is the same amount of time that elapsed between the American Civil War and World War II. Just think of how different the world of the American Civil War was compared to the world on the eve of World War II.

Similarly, the world today bears little resemblance to the world of 79 years ago. If a great power war broke out tomorrow, we cannot know exactly what shape it would take, but we do know, as President Eisenhower wisely suggested, that it would bear little in common with the last great power war of the 1940s.

It is therefore essential for the future of American security and deterrence to fully understand the implications of recent breakthroughs in commercial and military technologies.
America cannot remain capable of winning great power wars beyond any reasonable doubt if it does not remain superior technologically; and conversely, America cannot deter great power wars from happening if the world doubts America's capacity to win them.

Since the days of David and Goliath or the Trojan Horse in Troy, the books of history are full of stories of smarter adversaries outmaneuvering larger foes. The greatest risk to America is that we underestimate the importance that Intelligence will play in reconfiguring military power in the decade ahead.

We can think of AI as a factory for intelligence: a system that can solve any puzzle: find a cyber-exploit, predict the next chess move, locate tanks in a satellite image, anticipate an adversary's response options, and so forth.

I look forward to discussing at greater length the critical role of artificial intelligence in the future of the US-China rivalry and diving deeper into China's adoption of AI into its global military strategy.

Second, technology will also be the sine qua non for the US to remain the world's preeminent economic power. In the US-China rivalry, the nation with the most advanced technology will also be the nation with the larger economy.
Look no further than the difference between Israel and Nigeria today. Nigeria has more than 21 times the population of Israel and has 37 billion barrels in oil reserves, yet Israel has the larger economy and the stronger military. The reason is technology.

Contrary to popular belief, America can in fact stay ahead of China economically, but to do so it must also stay ahead technologically. With four times our population, if China simply manages to converge with us technologically and get to parity on productivity, it could have four times our GDP and maybe four times our military, making it the dominant power. And so *parity* means the West is losing. Parity cannot be the byproduct of American technology policy. Technology dominance should be our north star and that will be my focus today.

Third, technology is also challenging our traditional conceptions of national sovereignty. As China's cyber influence increases, the single, free Internet of the sort American officials once envisioned is giving way to ideologically opposed de facto techno-blocs.

The global Internet is already divided in two—between the decentralized, democratic Internet familiar to Americans and the centrally controlled, authoritarian Internet built by China.
The latter is spreading rapidly in the developing world, where countries from Southeast Asia to Latin America have opted to rely on Chinese technology for 5G networks and other critical digital infrastructure.

The influence of the authoritarian Internet is also expanding into advanced democratic societies, as companies susceptible to CCP influence become more central to our online lives.

If China's efforts to export these systems abroad are left unchecked, the CCP may soon enjoy the capacity to envelop dozens of countries behind its Great Firewall and reconstitute a 20th–style global sphere of influence through 21st-century technologies.

Popular Chinese platforms like TikTok make a mockery out of free speech and are internationalizing Chinese surveillance everywhere, including in the United States.

TikTok is a scourge attacking our children and our social fabric, a threat to our national security, and likely the most extensive intelligence operation a foreign power has ever conducted against the United States.

Senators Blackburn and Blumenthal are right: TikTok misled Congress. It should be held to account. Americans deserve to know if the CEO of this country's largest news source committed perjury on its relationship with a foreign adversary.
More importantly, American security should be protected and that means the app should be fully divested from its Chinese parent company or be banned entirely.

But TikTok is far from an isolated case. America is due for a comprehensive rethink of its technology trading relationship with China. I look forward to discussing actionable ways that Congress can mitigate the urgent security risks posed by Chinese hardware and software technologies in the United States.

I look forward to hearing from our expert witnesses. I will now turn the floor to my co-chair, Commissioner Wessel, for his opening remarks.

OPENING STATEMENT OF COMMISSIONER MICHAEL R. WESSEL
HEARING CO-CHAIR

COMMISSIONER WESSEL: Thank you, Commissioner Helberg. Thank you for the engagement and process we've gone through in preparing for this hearing.

Commissioner Helberg has deep knowledge and insights on technology issues which he has brought to the Commission which we all appreciate.

I would also like to thank everyone for joining us and thank our witnesses for the time and effort they have put into their testimonies and preparation.

Today's hearing will assess the Chinese government's ambitions and progress toward global leadership in several key emerging technology sectors. The commercial applications of these technologies are profound. Their adoption and diffusion throughout the economy over the coming years holds the potential both to disrupt industries and to create new wealth and opportunity.

At the same time, the wide-spread adoption of these technologies and China's competitive position and approaches could undermine U.S. economic and national security by creating new dependencies or vectors of attack that China may seek to exploit as it has already shown it is willing to do so in certain areas.

These disruptive technologies are already shaping our economies and our security interests. China's efforts to gain a decisive edge in emerging technologies are clear, systemic, and underpinned by a raft of government policies and investments.

These efforts present a significant challenge to U.S. interest across various industries. Chinese manufactured equipment embedded in information technology networks poses a threat to our critical infrastructure.

China's strides in biotechnology have solidified the role of Chinese drug manufacturers and global supply chains for lifesaving medications and could make China less dependent on U.S. agriculture production in the long run with the U.S. potentially becoming dependent on China for certain agricultural inputs such as amino acids, vitamins, and other products used in animal feed.

China's rapid progress in battery technology and manufacturing has also helped it dominate critical nodes in the supply chain for new energy systems and potentially is creating unacceptable security risks.

We have identified both capital and technology as key facilitating areas where Western support often unwittingly has advanced the goals of the Chinese Communist Party (CCP). This has been a long-term effort of this Commission and we are very proud of the work we have done.

The focus on technology is intense but, in my view, we still are only scratching the surface. I hope today's hearing and our efforts in this report cycle will advance the analysis and provide potential recommendations for consideration by Congress.

The challenge is immense. Export controls and investment restrictions have already hindered some of Beijing's efforts to acquire cutting-edge technology but it continues to capitalize on gaps in these regimes and the relative openness of U.S. academia.

An important problem remains in defining what constitutes emerging and foundational technologies in linking that definition to export control and investment screening actions.

As a critical issue, we need to understand how AI is altering and advancing China's military capabilities. In the past we assessed China's asymmetrical warfare approach with its focus on space and the electronic domain as avenues to challenge U.S. military capabilities. We

now need to better understand how China is using AI to challenge our capabilities and alter the balance and power.

My co-chair identified many questions that must be addressed regarding the competition that exist between our two great nations. Technology has the ability to address some of our greatest problems in areas ranging from medicine to the environment to agriculture to education and many others.

In assessing China's approaches and their efforts to control and dominate so many of these technologies, we must carefully evaluate and respond to the threats. But we must also seek to find ways to ensure that technology itself does not become a battlefield that limits the ability to address critical human needs.

So far the CCP's approach undermines that possibility.

Before we introduce our first panel, I would like to remind our audience that witness testimonies and the hearing transcript is available on our website, USCC.gov. Our next hearing, Examining China's Exports and Product Safety in Chinese Manufacturing Consumer Goods, will take place on March 1st.

Now I turn the gavel over, the microphone over, to my co-chair.

PREPARED STATEMENT OF COMMISSIONER MICHAEL R. WESSEL
HEARING CO-CHAIR

Hearing: Current and Emerging Technologies in U.S.-China Economic and National Security Competition

February 1, 2024

Opening Statement of Michael Wessel

Thank you, Commissioner Helberg. I would like to thank everyone for joining us and thank our witnesses for the time and effort they have put into their testimonies.

Today's hearing will assess the Chinese government's ambitions and progress toward global leadership in several key emerging technology sectors. The commercial applications of these technologies are profound; their adoption and diffusion throughout the economy over the coming years holds the potential both to disrupt industries and to create new wealth and opportunity. At the same time, the widespread adoption of these technologies and China's competitive position and approaches could undermine U.S. economic and national security by creating new dependencies or vectors of attack that China may seek to exploit as it has already shown its willingness to do in certain areas.

These disruptive technologies are already shaping our economies and our security interests. China's efforts to gain a decisive edge in emerging technologies are clear, systematic, and underpinned by a raft of government policies and investments. These efforts present a significant challenge to U.S. interests across various industries. Chinese-manufactured equipment embedded in information technology networks poses a threat to our critical infrastructure. China's strides in biotechnology have solidified the role of Chinese drug manufacturers in global supply chains for lifesaving medications, and could make China less dependent on U.S. agricultural production in the long-run — with the U.S. potentially becoming dependent on China for certain agricultural inputs such as amino acids, vitamins and other products used in animal feed. China's rapid progress in battery technology and manufacturing has also helped it dominate critical nodes in the supply chain for new energy systems and potentially is creating unacceptable security risks.

We have identified both capital and technology as key facilitating areas where Western support — often unwittingly — has advanced the goals of the Chinese Communist Party.

The focus on technology is intense but, in my view, we still are only scratching the surface. I hope today's hearing and our efforts in this report cycle will advance the analysis and provide potential recommendations for consideration by Congress.

The challenge is immense. Export controls and investment restrictions have already hindered some of Beijing's efforts to acquire cutting-edge technology, but it continues to capitalize on gaps in these regimes and the relative openness of U.S. academia. An important problem remains in defining what constitutes "emerging and foundational technologies," and linking that definition to export control and investment screening actions.

As a critical issue, we need to understand how AI is altering and advancing China's military capabilities. In the past we assessed China's asymmetric warfare approach with its focus on space and the electronic domain as avenues to challenge U.S. military capabilities. We now need to better understand how China is using AI to challenge our capabilities and alter the balance of power.

My co-chair identified many questions that must be addressed regarding the competition that exists between our two great nations. Technology has the ability to address some of our greatest problems in areas ranging from medicine to the environment to agriculture to education and many others. In assessing China's approaches, and their efforts to control and dominate so many of these technologies, we must carefully evaluate and respond to the threats. But we must also seek to find ways to ensure that technology itself does not become a battlefield that limits the ability to address critical human needs. So far, the CCP's approach undermines that possibility.

Before we introduce our first panel, I would like to remind our audience that witness testimonies and the hearing transcript is available on our website, uscc.gov. Our next hearing, examining China's exports and product safety in Chinese-manufactured consumer goods, will take place on March 1st.

PANEL I INTRODUCTION BY COMMISSIONER JACOB HELBERG

COMMISSIONER HELBERG: Thank you, Commissioner Wessel.

Our first panel will assess the national security risks created by Chinese manufactured information technology hardware and software sold in the United States, as well as the legal tools available to mitigate these risks.

We'll start by welcoming back the Honorable Nazak Nikakhtar, a partner at Wiley Rein law firm who co chairs their national security CFIUS (Committee on Foreign Investment in the United States) practice.

Ms. Nikakhtar previously served as the Department of Commerce's assistant secretary for Industry & Analysis at the International Trade administration, and also as the Under Secretary for Industry and Security at Commerce's Bureau of Industry and Security in the Trump Administration. Her testimony will address the risks of Chinese IT equipment used in commercial and government networks.

Next, we'll hear from Mr. Ivan Tsarynny, CEO of Feroot Security, a data protection intelligence software company. Mr. Tsarynny's company has reported extensively on the tools used to track user activity online. He will discuss Chinese software products and the risk they pose to users, data, and privacy.

This is his first time testifying before the Commission.

Third we'll hear from Mr. Jack Corrigan, a Senior Research Analyst at Georgetown's Center for Security and Emerging Technology, known as CSET. Prior to joining CSET, Mr. Corrigan worked as a journalist covering federal technology and cybersecurity policy. He will discuss the existing policy framework for regulating Chinese IT products sold in the United States. Mr. Corrigan is a new voice for the Commission.

Thank you all very much for your testimony. The Commission is looking forward to your remarks. I ask that all of our witnesses please keep their remarks to seven minutes.

Ms. Nikakhtar, we'll begin with you.

OPENING STATEMENT OF NAZAK NIKAKHTAR, PARTNER, WILEY REIN LLP

MS. NIKAKHTAR: Okay. Thank you very much Co-Chair Commissioner Wessel, Co-Chair Commissioner Helberg, and all esteemed commissioners and staff. Thank you for holding this hearing, first and foremost. It's a very important topic. And thank you for inviting me to testify.

I'm an attorney and economist and I've been working on the frontlines of the U.S.-China technological goods battle for over 20 years. I do need to state that the views and opinions expressed in this testimony are mine only and do not represent the views of Wiley Rein, or any of the firm's clients.

Let's step back for a second. Just over 20 years ago when China joined the World Trade Organization, the entire world was excited about taking advantage of China's low-cost non-market economy structure and we moved production capacity there. We moved production capacity, and then we moved technology.

Folks didn't really think about it much at first because they thought, well, it's just the commodity sector. Commodity sector funds, right? It creates the revenue streams for the next gen technologies.

The world didn't say very much and, all of a sudden, China starts working up the value chain. Now we find ourselves just 20 years later having some of the most critical high-tech goods dependent on the Chinese supply chain, dependent on Chinese technology.

When you look at all of the items that are critical to U.S. national security, from raw materials to semi-finished goods, etc., there is a list of 700-plus items. Much of those items are vital to technology and manufacturing. Much of those items are concentrated exclusively, or a majority of the production, in China.

One of the things that -- one of the reasons why -- I mentioned some of the reasons why this happened. One of the other reasons is that America has just become consumed with this notion of software. We've become coders. We've become app developers and we've forgotten how to make the nuts and bolts goods, and that gives China an enormous technological advantage.

When we look at telecommunications hardware, we don't have those discussions. We talk about open RAM. We talk about software developments in terms of innovations across the more semi-conductor designs, etc., but we've transferred the hardware to China.

That gives China an enormous advantage because it couples its hardware with the software to gain the advantages over us. If we don't produce the hardware, we have a huge vulnerability and that's what I'm going to concentrate my testimony on.

I don't need to tell you everywhere there is Chinese hardware embedded in our system and through the hardware capability creates vulnerability through software infiltration. In our defense system it's prevalent. Some may say, well, wait a second. We have the DOD trusted micro-electronics program. That is a fraction of the DOD systems that use electronic components from China.

Drones, right? We should talk about this because drones are emblematic of not only the problem, but the fact that we refuse to do anything about the problem. We've got -- okay, so we've got Chinese drones, DGI Autel, flying around the country.

We've got the American Drone Security Act. For just a limited three-year period of time, three years, 2025 to 2028, it's prohibiting the use of federal dollars to buy drones from foreign countries of concern for U.S. use.

A number of federal agencies have been exempt from this requirement, and waivers are eligible. Even if we take care of the government side, on the commercial side we have these drones roaming around the country collecting massive surveillance across the United States.

We have ample legal authorities to address it. We have for DGI, for example, the U.S. government put DGI on the entity list because by the government's own findings, DGI was involved in forced labor. Yet, through the Uyghur Forced Labor Prevention Act we refused to band the importation of DGI drones into the United States.

The Uyghur Forced Labor Prevention Act, and the Uyghur Human Rights Policy Act of 2020 allowed for sanctions. We're not sanctioning DGI, right? It's so emblematic of the fact that we're really good at talking about the problem but terrified of exercising the laws that we have, utilizing the laws that we have to address the problem.

By virtue of doing that, we are stifling innovation on the country. There are a number of American drone developers, drone producers, who want to get into this market but they can't because of the Chinese low-cost structure, and we're doing nothing to help them by perpetuating this.

We've got issues with the telecommunication infrastructure, Chinese components in the telecommunication towers. Even when we think about the China Commission that the House Select Committee on the CCP has flagged some of these modules, these modems, in the telecommunications towers that are not just across the United States.

Because China is the only producer of these components, it's across the entire world, right? This is China's dominance. Yet, we are terrified of ripping and replacing. We are struggling with the money to fund the rip and replace.

Even if we ripped and replaced, that's part of the solution but not comprehensibly because if we have TikTok on our phones, and if we have other apps, that software still infiltrates the telecommunications towers and spreads the cancer, spreads the malign software into other devices.

I'm going to rattle off some legal solutions. We have the Treasury Department's investment ban through the Chinese Military Industrial Complex legal authority. We have the Entity List. We have the 1260(h) of the NDAA.

We have the Export Controls Military End User List, Military Intelligence End Users, Section 889, Section 5949. Yet, all of those -- virtually all of those products and the companies that are listed and these authorities, we do nothing to prevent their hardware from getting into our system and creating enormous vulnerabilities.

Finally, I just wanted to spend a few seconds on the solution. The reason it merits a few seconds is because the solutions aren't complicated. You have companies telling you over and over again I don't know what's in my supply chain, my third, fourth, or fifth supply chain. So, you know, you're going to pass these laws but I can't comply, and everybody knows that's wrong.

I used to be a former auditor for the U.S. government for a number of years. Every single company if they are mandated by the U.S. government can audit the supply chains.

You start with a bill of materials and you only focus on the items that can be tampered with, so not the wires, not the chemicals, not the plastic, but the true hardware that can be

tampered with, and through several layers of audit traces you can find -- a company can find what is in their systems so they can replace it.

The legal authority exist, the capability exist, but across the board from industry to government the will does not exist. Thank you.

COMMISSIONER HELBERG: Thank you very much.

We will now move to our next witness, Mr. Tsarynny.

PREPARED STATEMENT OF NAZAK NIKAKHTAR, PARTNER, WILEY REIN LLP

February 1, 2024

Statement of Hon. Nazak Nikakhtar*

Partner, International Trade, 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 United States-China Economic and Security Review Commission*

Current and Emerging Technologies in U.S.-China Economic and National Security Competition

I. INTRODUCTION

Co-Chair Commissioner Michael Wessel and Co-Chair Commissioner Jacob Helberg, and all Commissioners, thank you for the opportunity to speak about the threats posed by the People's Republic of China and the Chinese Communist Party ("CCP"), specifically the presence of Chinese-manufactured hardware and software in the information technology networks of sensitive Government and commercial systems in the United States. My focus today is on potential hardware vulnerabilities in Chinese information technology products.

My name is Nazak Nikakhtar, and it is an honor to appear before you today. I am an international trade and national security attorney, and I chair 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 I recently completed my second tour in the U.S. Government. Twenty years ago, I began my career as an analyst at the U.S. 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 United States' steady erosion of its domestic industrial base. Beginning in the early 2000s, America rapidly transferred production capacity and technology to China, and we now find ourselves relying on Chinese components to power our most sensitive electronic devices – from commercial items to defense articles. And because China is an adversary, it is leveraging our supply chain dependence against us. The Chinese hardware we use contain backdoors that allow critical systems to be infiltrated by malicious software. And China has a bigger hacking program than every other country in the world combined. The system failure vulnerabilities at America currently faces nationwide are beyond alarming, they are likely catastrophic.

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

In 2004, I helped institute Commerce's China/Non-Market Economy Office where we warned the broader U.S. Government about such supply risks. Then, for several years thereafter, I audited numerous foreign (including Chinese) companies and their affiliates for the Commerce Department and witnessed firsthand China's efforts to decimate our most critical production capabilities to gain the upper hand. 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 Under Secretary for the Bureau of Industry and Security. My time at Commerce, from 2018 through 2021, marked the first time in modern U.S. history that the Executive Branch tackled critical supply chain vulnerabilities. Many of those efforts were spearheaded by my offices from 2018 to 2020. We rolled out the United States' whole-of-government semiconductor strategy in 2018, and, in 2019, we tackled head-on the risks arising from technology transfer to China. We were the first advocates for a meaningful American industrial base strategy to reshore critical capabilities and grow the American workforce. And, in 2019 and 2020, we rolled out innovative legal strategies to prevent malicious Chinese hardware and software from infiltrating America's infrastructure and undermining our national security.

Today, my work to protect national security continues in the private sector. Altogether, I have been working to strengthen the U.S. commercial and defense industrial base for the past 20+ years. It is from all of these vantage points that I offer my testimony and observations today.

II. CHINESE LAWS CREATE THE THREAT TO U.S. NATIONAL AND ECONOMIC SECURITY

First and foremost, context is important. China and other foreign adversaries pose significant national security threats to the United States. China, in particular, is undermining the peace and stability of the world order by threatening to harm the United States and its allies, and it is weaponizing its supply chains, intellectual property ("IP"), and technologies against the rest of the world. And I want to be clear that this is a fact, not conjecture - it is a matter of Chinese law. The CCP compels Chinese companies, including American firms in China forced to form joint ventures, to serve the country's national security interests through a variety of legal measures. The country's Civil-Military Fusion strategy imposes the CCP's ultimate control over all Chinese corporations through a range of national security laws. These laws demand that Chinese entities cooperate with the People's Liberation Army ("PLA") to advance the military strength and ambitions of the CCP 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 CCP's routine installation of CCP officials inside private firms – including American businesses in China – ensures compliance with the party's mandates. The Chinese nationwide credit rating system for all corporations operating with in China further requires that companies follow CCP laws or risk losing business opportunities. CCP laws further require that sensitive data (including personal data and intelligence data) and proprietary technical information, including IP, be transferred to the CCP whenever requested. The laws also prohibit all companies in China from complying with the laws of other jurisdictions, including U.S. national security sanctions and export control laws. The

objective of the CCP's laws is to coerce the sizeable Chinese commercial sector to align with the CCP's interests and to transfer technological innovations and information to the PLA to augment its military power.

The reality is that Chinese entities operate in a highly-controlled government- and military-driven ecosystem that is designed to advance the country's military capabilities, intelligence and surveillance operations, and national security apparatus. The legal framework through which the CCP forces entities to contribute to the modernization and expansion of the CCP's capabilities continues to expand rapidly through the promulgation of far-reaching laws and policies. The CCP's legal mandates direct corporate practices in China such that our hardware supply chain dependence poses a significant threat to the national security and economy of the United States. A summary of some of the most relevant CCP laws is provided in **Appendix 1**.

III. AMERICA'S SUPPLY CHAIN VULNERABILITIES ARE SIGNIFICANT

Today there are over 700 items – raw materials, semifinished goods, and finished goods – that are essential to U.S. national security, and the majority of these supply chains are concentrated or maintained exclusively in China. Much of these supply chains include critical hardware (as well as the raw materials necessary to manufacture the hardware) – such as semiconductors, microprocessors, and electronic computing systems – with backdoor capabilities permitting software enabled security risks. Their use in commercial electronic devices, such as personal computers and handsets, pose significant surveillance risks to users. And these devices' connections to critical U.S. infrastructure poses substantial dangers through the transfer of software from, e.g., personal computing devices, to modems or hardware modules in telecommunications towers, for example.

While it is impossible to list all the places where Chinese hardware exist and the resulting threats to the U.S. infrastructure, the illustrations in this paper are intended to provide examples of current vulnerabilities. To emphasize, however, the extent of Chinese hardware penetration in U.S. systems is far greater. As FBI Director Wray testified to Congress:

> China's hackers are positioning on American infrastructure in preparation to wreak havoc and cause real-world harm to American citizens and communities. If or when China decides the time has come to strike, they're not focused solely on political or military targets. We can see from where they position themselves, across civilian infrastructure, that low blows aren't just a possibility in the event of a conflict. Low blows against civilians are part of China's plan.[1]

Obviously, the United States needs to develop and implement viable national strategy to protect its essential security interests. It does not have one yet, and time is running out.

[1] FBI, News, Director Wray's Remarks to the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (Jan. 31, 2024).

A. Telecommunications Infrastructure and Personal Devices

It is well documented that Chinese hardware has infiltrated telecommunications networks across the country and poses a direct threat to U.S. national security and American privacy. Yet is counterintuitive that the U.S. Government has, to date, done nothing meaningful about it.

Congress and the Executive Branch are well aware of and have been working to address hardware vulnerabilities in the telecommunications sector for several years. Senators Markey and Wyden wrote to the Federal Communications Commission ("FCC") in 2021 regarding potential national security risks posed by foreign companies that manage and service U.S. wireless phone networks.[2] It is very common for the U.S. wireless industry to outsource the installation and administration of networking technology to managed service providers, some of which are foreign service providers subject to the jurisdiction of foreign countries of concern.[3] For example, the U.S. Federal Bureau of Investigation found in 2022 that Chinese company Huawei Technologies Co., Ltd.'s equipment was widespread in cell towers in close proximity to sensitive military bases.[4] The FBI recognized that Huawei equipment has the ability to intercept commercial cell traffic, access restricted U.S. military airwaves, and disrupt U.S. strategic command communications, potentially providing a window into the U.S. nuclear arsenal.[5] Given this risk, the FCC designated Huawei to its "Covered Equipment or Services" List in 2021 and it issued a rule in 2022 banning American carriers from using federal subsidies to procure equipment from Huawei and other entities on the Covered List.[6] Subsequently, in February 2023, the FCC prohibited Covered Equipment from obtaining *new* equipment authorizations. The new prohibition did not apply to any equipment with *prior* authorization, moreover, meaning that much of Huawei equipment still remains in telecommunications networks including infrastructure close to sensitive military installations.[7]

In 2019, following the U.S. Department of Commerce's decision to place Huawei on the Entity List,[8] Congress allocated $1.9 billion through the Secure and Trusted Communications Network Act to reimburse small cellular and broadband providers to "rip and replace" Huawei and ZTE

---

[2] Letter from Off. of Ron Wyden, U.S. Senator, to Jessica Rosenworcel, Acting Chairwoman, Federal Communications Commission (Oct. 20, 2021), *available at* https://docs.fcc.gov/public/attachments/DOC-392396A1.pdf.

[3] *Id.*

[4] Katie Bo Lillis, *CNN Exclusive: FBI investigation determined Chinese-made Huawei equipment could disrupt US nuclear arsenal communications*, CNN (July 25, 2022), *available at* https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html.

[5] *Id.*

[6] Brian Fung, *US regulators rule that China's Huawei and ZTE threaten national security*, CNN Business (Nov. 22, 2019), *available at* https://www.cnn.com/2019/11/22/tech/fcc-huawei-zte/index.html.

[7] Federal Communications Commission, Prohibition on Authorization of "Covered" Equipment (last updated Feb. 6, 2023), *available at* https://www.fcc.gov/laboratory-division/equipment-authorization-approval-guide/equipment-authorization-system.

[8] *Addition of Entities to the Entity List*, 84 Fed. Reg. 22,961 (Dep't Commerce May 21, 2019).

equipment on their networks.[9] To date, the FCC has been confronting repeated problems with the delay-ridden rip and replace program,[10] including the fact that the cost of this rip and replace effort is more than double the estimated $1.9 billion.[11] Absent additional appropriations, the FCC is only able to reimburse companies for a fraction of their rip and replace costs.[12] As of May 2023, 15% of projects approved for rip and replace have not commenced at all, continuing to put sensitive U.S. telecommunications in peril of interception by the CCP.[13]

The U.S. Department of Commerce is additionally probing whether, and the extent to which, Huawei gear is able to intercept communications from nearby missile silos.[14] Huawei hardware placed near U.S. military installations across the United States may already be obtaining sensitive information about the sites, not only about the number of people on duty in buildings and when equipment is online and offline, but also through the interception of actual missile communications from the silos. The risk also exists that Huawei hardware can facilitate access to the computer and telecommunications networks that are operating the silos.[15]

Recently, the House Select Committee on the Chinese Communist Party identified additional risks arising from hardware modules in internet of things ("IoT") devices manufactured by Chinese entities Quectel and Fibocom. These companies own a significant market share of IoT modules globally,[16] and are in part owned by the CCP:[17]

> Quectel is an IoT service provider, and it is the world's largest supplier of IoT modules. The company supplies cellular modules, WiFi/GNSS modules, and IoT antennas. Products are mainly used in the fields of wireless payment, vehicle transportation, smart energy, smart city, intelligent security, wireless gateway, industrial applications, medical health, and agricultural environment. The company, which was founded in Shanghai in 2010, was listed on the Shanghai Stock Exchange in 2019. Over 60% of Quectel's shares are public free float. At least 3.6% up to 6.2% of Quectel is owned by the CCP.[18]

---

9 U.S. Senate Committee on Commerce, Science, and Transportation, *Press Release: President Signs Rip and Replace Bill Into Law* (Mar. 12, 2020), *available at* https://www.commerce.senate.gov/2020/3/president-signs-rip-and-replace-bill-into-law.

10 *See* Jared Foretek, *FCC's 'Rip And Replace' Delays Upset Rural Providers*, Law360 (Nov. 16, 2023), *available at* https://www.law360.com/articles/1767711/fcc-s-rip-and-replace-delays-upset-rural-providers.

11 *See* Katie Bo Lillis, *supra* note 3.

12 *Id.*

13 Makena Kelly, *Congress called Huawei a national security risk — it's still in US networks*, The Verge (May 15, 2023), *available at* https://www.theverge.com/23721573/huawei-zte-rip-and-replace-china-telecom-carriers-fcc.

14 *See* Katie Bo Lillis, *supra* note 3.

15 Alexandra Alper, *Exclusive: U.S. probes China's Huawei over equipment near missile silos*, Reuters (July 21, 2022), *available at* https://www.reuters.com/world/us/exclusive-us-probes-chinas-huawei-over-equipment-near-missile-silos-2022-07-21/.

16 Alexi Drew, *Chinese technology in the 'Internet of Things' poses a new threat to the west*, Financial Times (Aug. 10, 2022), *available at* https://www.ft.com/content/cd81e231-a8d3-4bc0-820a-13f525a76117.

17 WireScreen, The Leading China Business Intelligence Platform, *available at* https://www.wirescreen.ai/.

18 *Id.*

> Fibocom is a leading global provider of IoT wireless solutions and wireless communication modules. In 2017, Fibocom become the first listed wireless module provider in China. Fibocom provides modules to Huawei, Hikvision, and SZ DJI Technology Co., Ltd. or Shenzhen DJI Sciences and Technologies Ltd. ("DJI"), all three of which have come under scrutiny from the U.S. government. At least 5.4% up to 9.9% of Fibocom is owned by the Chinese government. [19]

In September 2023, FCC Chairwoman Rosenworcel asked U.S. Government agencies to consider declaring that Quectel and Fibocom pose unacceptable national security risks.[20] Their modules are used throughout the United States by U.S. and foreign companies, and Quectel has nearly exclusive market share in the United States, as there are millions of Quectel modules in the telecommunications infrastructure and in smart devices across the country.[21] The letter to the FCC also details that Quectel and Fibocom contribute to China's defense industrial base by supplying Huawei and numerous firms designated by the U.S. Department of Defense ("DOD") as PLA affiliates and firms listed on the FCC's Covered List.[22]

TikTok is another important example of a major threat. It is well established that the Chinese government has been spying on Americans through the TikTok personal device application ("app"), controlled by Chinese parent company ByteDance. Beyond surveillance capabilities, the TikTok app has the ability to transfer malicious software to the hardware contained in devices in close proximity to it (e.g., from personal handsets to U.S. Government computers) and to the hardware installed in telecommunications infrastructure (e.g., modems and modules). In January 2023, the U.S. military banned TikTok from government devices after the DOD labeled it a security risk.[23] Approximately 34 states have already banned employees from using the app on government devices,[24] and in February 2023, the Biden Administration prohibited federal agencies from installing the app on their Government devices. There is also growing international consensus about the risks arising from the TikTok app. Looking abroad, India took the lead in banning the platform in 2020. Other countries and government bodies — including the United Kingdom, Australia, Canada, the executive arm of the European Union, France, and New Zealand's parliament — have similarly decided to ban the app from government devices as well.[25] Yet

---

19 *Id.*

20 David Shepardson, *US FCC chair says China's Quectel, Fibocom may pose national security risks*, Reuters (Sept. 6, 2023), *available at* https://www.reuters.com/technology/us-fcc-chair-asks-agencies-consider-restrictions-quectel-fibocom-2023-09-06/.

21 *Id.*

22 *Id.*

23 Brandi Vincent, *Pentagon issues rule to ban TikTok on all DOD-connected devices, including for contractors*, DefenseScoop (June 2, 2023), *available at* https://defensescoop.com/2023/06/02/pentagon-proposes-rule-to-ban-tiktok-on-all-dod-connected-devices-including-for-contractors/.

24 Brian Fung and Christopher Hickey, *TikTok access from government devices now restricted in more than half of US states*, CNN Business (Jan. 16, 2023), *available at* https://www.cnn.com/2023/01/16/tech/tiktok-state-restrictions/index.html.

25 Sapna Maheshwari and Amanda Holpuch, *Why Countries Are Trying to Ban TikTok*, New York Times (Dec. 12, 2023), *available at* https://www.nytimes.com/article/tiktok-ban.html.

despite the widespread acknowledgement of the risks posed by TikTok, the U.S. federal government has done little more to protect Americans from this risk.

Finally, the RISC-V open source chip design architecture is creating significant vulnerabilities in devices in which they are installed. The architecture is heavily leveraged by Chinese (and Russian) companies to undermine U.S. technological advantages in telecommunications related systems such as artificial intelligence ("AI"), autonomous systems, high-performance computers, and semiconductors. This is because the open-source nature of RISC-V's designs provide adversaries with the architectural designs and information to access and embed cybersecurity vulnerabilities at the chip design phase creating significant openings for exploitation. Chinese companies have become major contributors to RISC-V, and the CCP's national champions Huawei Technologies, ZTE Corp, and Alibaba Group Holding Ltd. are all members of RISC-V International, the global non-profit standards home of the open standard RISC-V Instruction Set Architecture. In 2022, 10 billion RISC-V chips were produced globally, of which half were made in China. Current U.S. regulations do not capture this technology, once again giving rise to major national security risks.

B. Military Materiel and Defense Networks

The degree to which U.S. military platforms depend on Chinese hardware is alarming. It is estimated that approximately 41% of DOD weapon systems and infrastructure supply chains rely on Chinese semiconductors.[26] U.S. Navy vessels, in particular, are utilizing thousands of Chinese semiconductors in critical naval ships with the U.S.'s carrier fleet, the workhorse of the U.S. Navy[27] and the heart of USINDOPACOM's strategic capabilities,[28] utilizing over 5,000 Chinese semiconductors per carrier.[29] Additionally, the U.S. Navy uses Chinese hardware in a variety of other essential naval military platforms, including the F/A 18 aircraft, the F/A 18 Growler, and the Navy's air-launched armament, including JASSM, JDAM, LRASM, and Tomahawk cruise missiles.[30]

The DOD's information technology ("IT") ecosystem is severely vulnerable according to a 2019 DOD Inspector General report, which found that at least $32.8 million of commercial off-the-shelf IT items procured by DOD officials had known cybersecurity vulnerabilities in FY 2018 alone.[31] This was a limited-scope study focused on Army and Air Force Government Purchase Card holders. The result was the purchases of high-risk electronic items, such as Lenovo computers,

---

[26] Jeffrey Nadaner and Tara Dougherty, *Numbers Matter: Defense Acquisition, U.S. Production Capacity, and Deterring China*, Govini, *available at* https://govini.com/research/numbers-matter-2024/ ("Govini Report").

[27] U.S. Navy, Aircraft Carriers – CVN (Nov. 12, 2021), *available at* https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2169795/aircraft-carriers-cvn/.

[28] U.S. Navy, Commander, U.S. 7th Fleet, The United States Seventh Fleet, *available at* https://www.c7f.navy.mil/About-Us/Facts-Sheet/.

[29] Govini Report.

[30] Govini Report.

[31] U.S. Dep't of Defense, Inspector General, *(U) Audit of the DoD's Management of the Cybersecurity Risks for Government Purchase Card Purchases of Commercial Off-the-Shelf Items* at i, *available at* https://www.oversight.gov/report/DoD/Audit-DoD%E2%80%99s-Management-Cybersecurity-Risks-Government-Purchase-Card-Purchases-Commercial.

which the DOD believes can severely compromise electronic defense platforms and classified information systems.

Chinese companies identified by the DOD as being high-risk companies have not been excluded from the domestic supply chain. In 1999, the National Defense Authorization Act ("NDAA") mandated that the DOD identify Communist Chinese military companies ("CCMC") operating directly or indirectly in the United States or in any of its territories or possessions pursuant to section 1237.[32] The Department issued its first CCMC list 20 years later in 2020, and designated dozens of Chinese companies to the list over the course of several subsequent months. Immediately thereafter, section 1260H of the 2021 NDAA became law and expanded the definition of Chinese military companies in order to enhance the DOD's ability to keep pace with the CCP's and the PLA's expanding control over the Chinese commercial sector.[33] The DOD then sunsetted the 1237 list and, despite having a new legal authority to designate a greater number of PLA companies to its list, the Pentagon opted to designate a smaller subset of companies to its new 1260H list.[34] The reason for this is unclear.

The 1260H designation has very limited legal implications, namely for U.S. Government contractors and other companies participating in the U.S. Government's supply chain. The Federal Acquisition Regulations ("FAR") prohibit U.S. Government agencies from "procuring or obtaining" "any equipment, system, or service" that utilizes "covered telecommunications equipment or services" for certain critical technology or a "substantial or essential component of any system."[35] While Congress in 2019 identified five Chinese companies as being subject to the FAR prohibitions, the statute and implementing regulations can apply to any other company "that the Secretary of Defense . . . reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a foreign country.[36] Further, the DOD's supplement to the FAR (the Defense Federal Acquisition Regulation Supplement, "DFARS") prohibits the acquisition of items covered by the United States Munitions List from a 1260H company.[37] Moreover, Section 514 of the Consolidated Appropriations Act for 2018 specifies that for "high-impact or moderate-impact" information systems, agencies must review the "supply chain risk,"

---

[32] *Strom Thurmond National Defense Authorization Act for Fiscal Year 1999*, Public Law 105-261 (as amended by section 1233 of Public Law 106-398 and section 1222 of Public Law 108-375), U.S. Congress (Oct. 17, 1998), *available at* https://www.govinfo.gov/link/plaw/105/public/261.

[33] Terri Moon Cronk, *China Poses Largest Long-Term Threat to U.S., DOD Policy Chief Says*, Dep't of Defense (Sept. 23, 2019), *available at* https://www.defense.gov/Explore/News/Article/Article/1968704/china-poses-largest-long-term-threat-to-us-dod-policy-chief-says/.

[34] Dep't of Defense, *DOD Releases List of People's Republic of China (PRC) Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021* (Oct. 5, 2022), *available at* https://www.defense.gov/News/Releases/Release/Article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/.

[35] *Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment*, 85 Fed. Reg. 42,665 (Dep't Defense July 14, 2020).

[36] Section 4.2101(4) of *Federal Acquisition Regulation: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment*, General Services Administration, *available at* https://www.acquisition.gov/far/subpart-4.21.

[37] Subpart 225.770 of *Defense Federal Acquisition Regulation Supplement*, Off. of the Sec'y of Defense (last revised Oct. 30, 2023), *available at* https://www.acq.osd.mil/dpap/dars/dfars/html/current/225_7.htm.

including the risk related to cyber-espionage or sabotage by entities identified by the U.S. Government "including but not limited to, those that may be owned, directed, or subsidized by the People's Republic of China."[38]

These regulations are seldom used to secure defense supply chains, let along commercial ones. At present are a number of Chinese military companies on the 1260H list, including Huawei, Inspur Group, and Semiconductor Manufacturing International Corporation ("SMIC") that enjoy significant commercial presence in the U.S. market. The exact extent to which their hardware remains in military systems remains is unknown given the purported inability of defense contractors, or "primes," to audit their full supply chains. The presence of Chinese hardware in military systems, including legacy military systems, is believed to be significant.

There are additional legal authorities that identify Chinese military companies under U.S. law, but they similarly fail to prohibit the use of these companies' hardware in U.S. systems. For instance, in 2021, President Biden issued E.O. 14032 entitled "Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China" which identified just over sixty "Chinese Military Industrial Complex" companies and Chinese companies involved with the development or use of surveillance technologies to facilitate repression or serious human rights abuses.[39] The E.O. prohibited certain U.S. public investments in the designated companies, but did not prohibit the use of hardware from these companies in U.S. commercial and defense systems.[40]

Additional legal authorities impose other types of prohibitions on activities with high-risk Chinese companies, including the Entity List (requiring U.S. Government licenses for exports of goods, software and technology), Section 889 of the 2019 National Defense Authorization Act (federal procurement prohibition), and Section 5949 of the 2023 National Defense Authorization Act (federal procurement prohibition).[41] Despite the fact that the hundreds of Chinese military and surveillance companies identified on these lists (although far from comprehensive) have each been deemed a U.S. national security risk, their presence and participation in the U.S. commercial and military sectors remains largely unregulated. For example, Chinese chip maker Hulan and its subsidiary Initio are on the U.S. Department of Commerce's Entity List, yet are still permitted to

---

[38] *Consolidated Appropriations Act, 2018*, Public Law 115-141, U.S. Congress (2018), *available at* https://www.congress.gov/bill/115th-congress/house-bill/1625/text.

[39] White House, *Executive Order on Addressing the Threat from Securities Investments that Finance Certain Companies of the People's Republic of China* (June 3, 2021), *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/03/executive-order-on-addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples-republic-of-china/.

[40] *Id.*

[41] Bureau of Industry and Security, U.S. Dep't of Commerce, *Entity List*, *available at* https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list; Off. of Foreign Assets Control, U.S. Dep't of the Treasury, *Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists*, *available at* https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists; Section 889 of the *National Defense Authorization Act for Fiscal Year 2019*, U.S. Congress (2019), *available at* https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf; Section 1260H of the *National Defense Authorization Act for Fiscal Year 2021*, U.S. Congress (2021), *available at* https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf; Section 5949 of the *James M. Inhofe National Defense Authorization Act for Fiscal Year 2023*, U.S. Congress (2023), *available at* https://www.govinfo.gov/content/pkg/PLAW-117publ263/pdf/PLAW-117publ263.pdf.

supply encrypted hard drives to the U.S. Navy and numerous other North Atlantic Treaty Organization fighting forces. Hulan and Initio maintain concerning connections to the PLA, and their hard drives have multiple security vulnerabilities, potentially deliberately placed, identified by third party analysts.[42] For its part, semiconductors produced by SMIC, a Chinese company specifically designated under Section 5949 for federal government procurement bans, is likely prevalent in U.S. military systems but the U.S. Government is unable to identify where those chips are located. The lack of adequate domestic capacity to replace Chinese product is another factor frustrating the defense sector's ability to wean itself off Chinese chips.[43]

In addition to IT equipment, the DOD continues to use Chinese drones manufactured by DJI, a Chinese company designated to the Entity List, the 1260H list, and CMIC list.[44] The U.S. Government has long known that DJI's drones conduct surveillance activities in the United States and that the data obtained are shared with the Chinese government. In 2020, the U.S. Government also found that DJI was involved in forced labor in China.[45] Subsequently, the Uyghur Forced Labor Prevention Act ("UFLPA") became law in 2021 and banned the U.S. importation of products involved in forced labor. [46] Despite the UFLPA's import restrictions, imports of DJI drones continue to flow into the United States. And even though the UFLPA amended the Uyghur Human Rights Policy Act of 2020[47] to permit U.S. Government sanctions on companies involved in forced labor, the U.S. Government has declined to sanction DJI. Finally, despite the fact that certain U.S. investments in DJI are banned under the CMIC E.O., DJI's drones are permitted to roam freely and spy on communities across the United States.

Today, DJI accounts for well over 70% of the commercial drone use in the United States.[48] The remaining market share is held by another, lesser-known Chinese company named Autel Robotics, Inc., which similarly supplies both the commercial market as well as federal and state government bodies.[49] In an effort to address the pervasive presence of Chinese drones in the United States, the U.S. Government passed the American Security Drone Act ("ASDA") as part of the National

---

[42] Andy Greenberg, *How a Shady Chinese Firm's Encryption Chips Got Inside the US Navy, NATO, and NASA*, Wired (June 15, 2023), *available at* https://www.wired.com/story/hualan-encryption-chips-entity-list-china/.

[43] Alan Patterson, *Experts: U.S. Military Chip Supply Is Dangerously Low*, EE Times (Jan. 6, 2023), *available at* https://www.eetimes.com/experts-u-s-military-chip-supply-is-dangerously-low/.

[44] Chris Rodrigo and Maggie Miller, P*entagon report clears use of drones made by top Chinese manufacturer*, The Hill (June 1, 2021), *available at* https://thehill.com/policy/defense/556370-pentagon-report-clears-use-of-drones-made-by-top-chinese-manufacturer/.

[45] *Addition of Entities to the Entity List, Revision of Entry on the Entity List, and Removal of Entities From the Entity List*, 85 Fed. Reg. 83,416 (Dep't Commerce Dec. 22, 2020)**Error! Hyperlink reference not valid.**.

[46] Uyghur Forced Labor Prevention Act in 2021, U.S. Congress (2021), *available at* https://www.govinfo.gov/content/pkg/PLAW-117publ78/pdf/PLAW-117publ78.pdf.

[47] Uyghur Human Rights Policy Act of 2020, U.S. Congress (2020), *available at* https://www.congress.gov/116/plaws/publ145/PLAW-116publ145.pdf.

[48] Nessa Anwar, *World largest done maker is unfazed – even if it's blacklisted by the U.S.*, CNBC (Feb. 7, 2023), *available at* https://www.cnbc.com/2023/02/08/worlds-largest-drone-maker-dji-is-unfazed-by-challenges-like-us-blacklist.html.

[49] Eric Sayers and Klon Kitchen, *DJI isn't the only Chinese drone threat to US security. Meet Autel.*, DefenseNews (Sept. 15, 2023), *available at* https://www.defensenews.com/opinion/2023/09/15/dji-isnt-the-only-chinese-drone-threat-to-us-security-meet-autel/.

Defense Authorization Act for Fiscal Year 2024.[50] Although the ASDA bans federal agencies from using federal funds to purchase or using drones made in or made with components from foreign countries of concern, including China, Iran, Russia, and North Korea,[51] the prohibitions on procurement and use do not kick in until December 2025 and last only through December 2028.[52] Further, many U.S. federal agencies have been exempt from complying with the ban and all agencies are able to apply for waivers in order to continue procuring and using covered drones. Finally, DJI and Autel have not been excluded from the U.S. commercial market through any legal measures, meaning that Chinese surveillance continues across the United States and the resulting threats to national security remain unaddressed.

Next, the DOD's modern vision for U.S. military doctrine, particularly its efforts to multiply U.S. airpower capabilities through increased used of unmanned autonomous aerial vehicle systems, similarly raises concern about America's reliance on Chinese hardware in these systems. DOD's recently announced Replicator Initiative, which is an initiative to field thousands of autonomous systems across a broad range of warfighting domains to counter China's rapid armed forces buildup, relies on the production and procurement of low-cost drones.[53] The DOD plans to have these drones online quickly within 18-24 months of the program's August 2023 announcement.[54] But, in light of China's existing dominance in aerial drone production and related hardware components, combined with the short timeline that the DOD has given for onboarding these aerial systems, there is reason for concern that many of the systems deployed in the Replicator Initiative will rely on Chinese hardware.[55]

The risks associated with relying on Chinese hardware and designs in U.S. military systems is self-evident and immense. Cyber-vulnerabilities enabled through Chinese hardware could render DOD platforms inoperable and unavailable to respond to potentially hostile Chinese action.[56] In a sophisticated operation, outside actors may even be capable of gaining access to U.S. systems and directing them to harm military and civilian targets.[57]

---

[50] National Defense Authorization Act for Fiscal Year 2024, U.S. Congress (2024), *available at* https://www.govinfo.gov/content/pkg/BILLS-118hr2670rh/pdf/BILLS-118hr2670rh.pdf.

[51] Zacc Dukowitz, *A Federal DJI Ban Is Coming–Here's Why It Matters*, UAV Coach (Dec. 20, 2023), *available at* https://uavcoach.com/asda-law/.

[52] Eric Holdeman, *Federal Government Will Require Purchase of 'Made in America' Drones*, Government Technology (Jan. 8, 2024), *available at* https://www.govtech.com/em/emergency-blogs/disaster-zone/federal-government-will-require-purchase-of-made-in-america-drones.

[53] Chris Gordon and John Tirpak, *Pentagon Wants to Buy 1,000s of Small, Cheap, Autonomous Drones in Next Two Years*, Air & Space Forces Magazine (Aug. 28, 2023), *available at* https://www.airandspaceforces.com/pentagon-replicator-small-cheap-autonomous-drones/.

[54] *Id.*

[55] Eva Dou and Gerrit De Vynck, *Pentagon plans a drone army to counter China's market dominance*, The Washington Post (Dec. 1, 2023), *available at* https://www.washingtonpost.com/technology/2023/12/01/pentagon-drones-replicator-ukraine/.

[56] Lukas Olejnik, *The Dire Possibility of Cyberattacks on Weapons Systems*, Wired (Mar. 10, 2021), *available at* https://www.wired.com/story/dire-possibility-cyberattacks-weapons-systems/.

[57] *Id.*

As already noted, at the heart of the DOD's struggle with Chinese hardware is its continued failure to develop a robust and economically secure domestic manufacturing base. The DOD continues to prioritize low-costs items, and the Pentagon as an institution incentivizes a military-industrial base that cannot respond to potential needs for mass production. A select few large companies fulfill procurement for low-volume and highly-tailored equipment, and the remaining items are generally outsourced.[58] Even when larger DOD suppliers are involved, they rely on secondary and tertiary suppliers for hardware components, which are increasingly difficult to find in the United States as orders and margins are too small and too inconsistent to sustain domestic production capacities.[59] With the concentration of hardware supply chains in China, DOD suppliers often have no choice but to resort to Chinese hardware for their systems. This, of course, renders defense systems vulnerable to potential cyberattacks and system failures.[60]

C. Water Facilities and Energy Utilities

Utilities are increasingly relying on outsourced computing and automation hardware, and consequently becoming susceptible to foreign exploitation of their internal systems.

a. Water Treatment Facilities

Water treatment plants increasingly utilize automated systems to perform treatment processes that deliver safe and potable water.[61] If commandeered by hostile actors, automated systems can cause significant disruption to municipal water supplies including limiting access to water or producing toxic, contaminated water.[62] In February 2021, an employee at the Bruce T. Haddock Water Treatment Plant in Oldsmar, Florida reported unauthorized access to the plant's control and an attempt to raise the amount of lye in the plant's treated water to toxic levels.[63] Although an investigation never publicly identified a culprit for the alleged incident, experts on critical infrastructure systems concede that cyberattacks are a threat.[64] The degree to which American water treatment facilities utilize Chinese hardware and related software is difficult to determine, but trends in the water treatment industry point to an increased reliance on Chinese components for plant operations.

---

58 Govini Report.

59 *Id.*

60 *Id.*

61 Idrica, *Water Trends in automation for 2023: Improving operability and management* (Mar. 7, 2023), *available at* https://www.idrica.com/blog/water-trends-in-automation-for-2023-improving-operability-and-management/#:~:text=In%202023%2C%20and%20in%20the,different%20DWTP%20processes%20in%20isolation.

62 Cybersecurity & Infrastructure Security Agency, *Water and Wastewater Systems*, *available at* https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/water-and-wastewater-sector.

63 Cybersecurity & Infrastructure Security Agency, *Cybersecurity Advisory: Compromise of U.S. Water Treatment Facility* (Feb. 12, 2021), *available at* https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a.

64 Christian Vasquez, *Did someone really hack into the Oldsmar, Florida, water treatment plant? New details suggest maybe not*, CyberScoop (Apr. 10, 2023), *available at* https://cyberscoop.com/water-oldsmar-incident-cyberattack/.

Water treatment facilities across the United States are increasingly adopting autonomous and networked systems, such as supervisory control and data systems ("SCADA") and IoT devices, such as smart readers, to operate water treatment systems independent of human input.[65] The CCP, for its part, has prioritized industrial automation as an essential sector and, so, has dedicated significant funding to advancing its domestic SCADA manufacturing capabilities. In fact, the CCP highlighted industrial automation in its last two Five-year Plans and identified automation as one of the ten key industries in its Made in China 2025 ("MIC 2025") initiative.[66] CCP-funded government guidance funds tied to the MIC 2025 have registered a capital target of $1.5 trillion and had raised $627 billion of that target as of 2020.[67] Beyond direct funding, the CCP assists MIC 2025 entities through tax, trade, and investment measures, forced joint ventures and partnerships, technology licensing and equipment, and talent recruitment and training assistance. [68] These programs are organized to mature Chinese industries more quickly than competitors. [69] They are also designed to provide low-cost alternatives to markets globally, including SCADA. Beyond economic gains, the CCP's motivation is to export systems that enable backdoor access to other countries' critical infrastructure, which could then be leveraged at any time to gain an upper hand in a conflict. Chinese hardware in automated systems is a significant concern for the U.S. Cybersecurity and Infrastructure Security Agency ("CISA"), among other cybersecurity organizations, which identifies SCADA and other industrial control systems in critical infrastructure as particularly vulnerable to cybersecurity risks.[70]

It is likely that American water treatment facilities, where cybersecurity oversight at the state and federal level is limited, are already using Chinese SCADA systems and components in their automated facilities, rendering the systems vulnerable to dangerous cybersecurity attacks.[71] Water treatment facilities that serve smaller and more rural communities are even more likely to utilize

---

[65] Inductive Automation, *SCADA: Supervisory Control and Data Acquisition: What is SCADA, Who Uses it and How SCADA Has Evolved* (Sept. 12, 2018), *available at* https://inductiveautomation.com/resources/article/what-is-scada.

[66] *See* Stanford University, *Translation: 14th Five-Year Plan for National Informatization – Dec. 2021*, *available at* https://digichina.stanford.edu/wp-content/uploads/2022/01/DigiChina-14th-Five-Year-Plan-for-National-Informatization.pdf; Nat'l Dev. and Reform Comm'n., *The 13th Five-Year Plan for Economic and Social Development of the People's Republic of China*, *available at* https://en.ndrc.gov.cn/policies/202105/P020210527785800103339.pdf; Center for Security and Emerging Technology, Georgetown University, *Translated: Made in China 2025*, *available at* https://cset.georgetown.edu/wp-content/uploads/t0432_made_in_china_2025_EN.pdf; *see also* Outlier Automation, *How China Became an Industrial Automation Powerhouse* (Feb. 1, 2022), *available at* https://www.outlierautomation.com/blog/how-china-became-an-industrial-automation-powerhouse.

[67] Congressional Research Service, *"Made in China 2025" Industrial Policies: Issues for Congress* (last updated Mar. 10, 2023) at 2, *available at* https://sgp.fas.org/crs/row/IF10964.pdf.

[68] *Id.*

[69] Shaoshan Liu, *China's Pursuit of Autonomous Machine Computing Self-Sufficiency*, The Diplomat (Nov. 17, 2023), *available at* https://thediplomat.com/2023/11/chinas-pursuit-of-autonomous-machine-computing-self-sufficiency/.

[70] Cyber Security & Infrastructure Security Agency, Industrial Control Systems, *available at* https://www.cisa.gov/topics/industrial-control-systems.

[71] Robert F. Powelson, *Without federal action, hackers will continue to endanger US water systems*, The Hill (Dec. 24, 2023), *available at* https://thehill.com/opinion/cybersecurity/4373600-without-federal-action-hackers-will-continue-to-endanger-us-water-systems/.

Chinese hardware given their lower costs and weaker cybersecurity software controls.[72] The foregoing risks to the water infrastructure have not been adequately addressed by federal and state governments. Cybersecurity requirements are at best extremely lax or, in large part, nonexistent.

b. U.S. Energy Providers and the Electricity Grid

For several years, Members of Congress, executive agencies, and third-party organizations have been sounding the alarm on the potential risks caused by Chinese components and hardware embedded into U.S. energy grid. In testimony before the Senate Energy and Natural Resources Committee, Director of CESAR (the Department of Energy's ("DOE") Office of Cybersecurity, Energy Security, and Emergency Response) Puesh Kumar, pointed to reports from the Director of National Intelligence ("DNI") and emphasized that cyber actors are targeting U.S. energy infrastructure, and they are posing serious threats to national security.[73] Further, the 2023 Annual Threat assessment from DNI identified China as representing "the broadest, most active, and persistent cyber espionage threat to U.S. Government and private-sector networks [and that] China's cyber pursuits and its industry's export of related technologies increase the threats of aggressive cyber operations against the U.S. homeland."[74]

Today, outsider actors are capable of exploiting hardware vulnerabilities in U.S. systems to destroy physical components of the U.S. electric grid.[75] The attacks could originate from hardware within the grid itself, or the transmission of malicious code to the grid from external hardware devices, such as electric vehicles ("EV") charging stations, large data and power storage devices, or telecommunication equipment scattered nationwide. Large attacks on the U.S. electric grid, should they occur, will have devastating impact on the United States population – leaving masses without access to electricity and heat and will cause critical service systems such as hospitals, emergency services, utility providers (water/sewer, gas), and military installations incapable of performing essential tasks.[76] Attacks on military utility installations have been a particular area of concern as hostile nations could utilize preemptive blackouts to limit U.S. defensive and responsive capabilities.

---

[72] *See* Robert F. Powelson, *Without federal action, hackers will continue to endanger US water systems*, The Hill (Dec. 24, 2023), *available at* https://thehill.com/opinion/cybersecurity/4373600-without-federal-action-hackers-will-continue-to-endanger-us-water-systems/; Connor Griffin, *Billions for Water Infrastructure, but Small Communities Risk Being Left Out to Dry*, Governing (June 23, 2023), *available at* https://www.governing.com/infrastructure/billions-for-water-infrastructure-but-small-communities-risk-being-left-out-to-dry.

[73] *Cybersecurity Vulnerabilities to the United States' Energy Infrastructure*, Hearing Before the Senate Energy and Natural Resources Committee, 118th Cong. (Mar. 23, 2023) (testimony of Puesh Kumar, Director, Off. of Cybersecurity, Energy Security, and Emergency Response, Dep't of Energy), *available at* https://www.energy.senate.gov/services/files/7C2EC274-467C-4444-BD14-D4F11E474492.

[74] Off. of the Director of National Intelligence, *Annual Threat Assessment of the U.S. Intelligence Community* (Feb. 6, 2023), *available at* https://www.dni.gov/files/ODNI/documents/assessments/ATA-2023-Unclassified-Report.pdf.

[75] Andy Greenberg, *How 30 Lines of Code Blew Up a 27-Ton Generator*, Wired (Oct. 23, 2020), *available at* https://www.wired.com/story/how-30-lines-of-code-blew-up-27-ton-generator/.

[76] Senate Republican Policy Committee, *Infrastructure Cybersecurity: The U.S. Electric Grid* (July 16, 2021), *available at* https://www.rpc.senate.gov/policy-papers/infrastructure-cybersecurity-the-us-electric-grid.

Moreover, power plants and petrochemical refineries and facilities may similarly be rendered inoperable due to cyber intrusions.[77] And nuclear generation facilities, in particular, pose a risk for catastrophic destruction should outside interference induce a radiological release.[78] These are merely a few examples of the range of risks that exist today. These risks become all the more dangerous when coordinated cyberattacks simultaneously cripple multiple power sources across broad geographic regions.

In the DOE's 2021 Prohibition Order Securing Critical Defense Facilities, the DOE correctly observed that attacks may be leveraged preemptively to handicap the U.S. defense posture: *"Such attacks are most likely during crises abroad where Chinese military planning envisions early cyberattacks against the electric power grids around CDFs in the U.S. to prevent the deployment of military forces and to incur domestic turmoil.*" [79] Consequently, the DOE is attempting to identify vulnerabilities in energy systems at the subcomponent level, by identifying which components are manufactured in China by testing equipment "down to the chips level" with the support of DOE-partnered laboratories.[80]

It is likely that the DOE will find a large number of Chinese hardware in its systems, but then what will it propose to do? To date, the DOE has not made any concerted effort to remove Chinese components from the domestic energy infrastructure. Previously in 2020, President Trump issued an E.O. prohibiting the acquisition, importation, transfer, or installation of specified bulk-power system electric equipment from China (and other adversaries) that directly serve Critical Defense Facilities ("CDF"s).[81] The Biden Administration subsequently revoked the E.O. and has not yet addressed the threat to CDFs.[82] The power supply for military installations will continue to be vulnerable as long as Chinese hardware remains in use, so inaction is not an option.

It has been reported that some non-defense utility companies in the United States have already, to varying degrees, recognized the threats posed by the use of Chinese hardware and have begun to look for alternatives.[83] To the extent this is true, and even if Chinese hardware is fully removed

---

77 Katie Benner and Kate Conger, *U.S. Accuses 4 Russians of Hacking Infrastructure, Including Nuclear Plant*, New York Times (Mar. 24, 2022), *available at* https://www.nytimes.com/2022/03/24/us/politics/russians-cyberattacks-infrastructure-nuclear-plant.html#:~:text=WASHINGTON%20%E2%80%94%20The%20Justice%20Department%20unsealed,petrochemical%20facility%20in%20Saudi%20Arabia.

78 Susan Pickering and Peter Davies, *Cyber Security of Nuclear Power Plants: US and Global Perspectives*, Georgetown Journal of International Affairs (Jan. 22, 2021), *available at* https://gjia.georgetown.edu/2021/01/22/cyber-security-of-nuclear-power-plants-us-and-global-perspectives/.

79 *Prohibition Order Securing Critical Defense Facilities*, 86 Fed. Reg. 533 (Dep't Energy Jan. 6, 2021).

80 Robert Walton, *DOE cyber chief gets bipartisan grilling as senators question US reliance on China for grid equipment*, Utility Dive (Mar. 24, 2023), *available at* https://www.utilitydive.com/news/doe-cyber-chief-bipartisan-grilling-senators-china-power-grid-transformers/645914/.

81 *Exec. Order 13920*, 85 Fed. Reg. 26,595 (Exec. Off. May 1, 2020); *Prohibition Order Securing Critical Defense Facilities*, 86 Fed. Reg. 533 (Dep't Energy Jan. 6, 2021).

82 *Revocation of Prohibition Order Securing Critical Defense Facilities*, 86 Fed. Reg. 21,308 (Dep't Energy Apr. 22, 2021).

83 Michael Novinson, *US Officials Urged to Examine Chinese Risk to Electric Grid*, Bank Info Security (Mar. 23, 2023), *available at* https://www.bankinfosecurity.com/us-officials-urged-to-examine-chinese-risk-to-electric-grid-a-21508.

from the energy grid, the fact remains that external devices containing Chinese hardware (e.g., EV charging station) can connect to the grid and transfer malicious software to the grid. This remote-access issue is another dimension of the problem that remains to be addressed.

It should also be noted that renewable energy is also an area where Chinese hardware can pose a potential vulnerability. As solar energy's role in domestic energy production continues to grow to meet America's climate goals, so does the share of the U.S. solar market controlled by Chinese panel makers.[84] Inverters required for solar energy production are particularly vulnerable to cyber exploitation.[85] China is the top producer of inverters in the U.S. market, and Huawei, already known for its cooperation with the CCP, is the world's largest producer of inverters.[86] In Australia, where the domestic solar market is even more dependent on Chinese solar companies than the United States,[87] the national government has received increasing calls to assess the cybersecurity vulnerabilities of relying on Chinese hardware for solar production.[88] China's domination of the global wind tower market poses similar threats.

Finally, large energy material producers, including petrochemical facilities, face similar vulnerabilities to water treatment facilities due to their increasing reliance on industrial automation including SCADA technologies.[89] As China continues to expand its role as a supplier of industrial automation systems, production facilities will increasingly adopt Chinese hardware in their internal systems, raising the risk that cyberattacks will render these systems inoperable.

D. Public Transportation

In 2020, Congress passed the Transit Infrastructure Vehicle Security Act into law, which barred transit agencies from using federal funds to purchase Chinese rolling stock or buses manufactured

---

84 Phred Dvorak, *China's Dominance Over U.S. Solar Market Grows Despite Efforts to Stem It*, Wall Street Journal (Apr. 26, 2023), *available at* https://www.wsj.com/articles/china-dominates-u-s-solar-market-as-lawmakers-tussle-over-tariffs-7c2d749d.

85 Raymond Watts and Brian Kline, *Potential Electric Grid Vulnerability from Cyber Enabled Foreign Actors*, Ridge Global (Oct. 29, 2018), *available at* https://protectourpower.org/resources/ridge-global-report-2018.pdf; *see also* Andrew Smith, *Former US Homeland chief warns Chinese solar inverters pose cyber threat*, S&P Global (Nov. 6, 2018), *available at* https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/former-us-homeland-chief-warns-chinese-solar-inverters-pose-cyber-threat-47589890 ("S&P Report").

86 S&P Report.

87 Jayant Chakravarti, *Australia Focuses on Threat of Chinese Attack on Solar Power*, Bank Info Security (Oct. 25, 2023), *available at* https://www.bankinfosecurity.com/australia-focuses-on-threat-chinese-attack-on-solar-power-a-23395#:~:text=China%20dominates%20the%20Australian%20solar,to%20renewable%20sources%20by%202028.

88 Cindy Li, *Australian Government Urged to Assess Chinese Solar Panels Over Cybersecurity Concerns*, The Epoch Times (Aug. 10, 2023), *available at* https://www.theepochtimes.com/world/australian-government-urged-to-assess-chinese-solar-panels-over-cybersecurity-concerns-5456025.

89 *See* Gregory Miller, *Automation: a positive force in the power sector*, Power Electronic News (July 26, 2019), *available at* https://www.powerelectronicsnews.com/automation-a-positive-force-in-the-power-sector/; *see also* INDUSTLABS, *The Importance of Automation in the Oil & Gas Industry* (Jan. 12, 2023), *available at* https://industlabs.com/news/oil-and-gas-automation#:~:text=SCADA%20Systems,make%20trips%20to%20the%20sites.

by state-owned, controlled, or subsidized companies.[90] However, several of America's largest transit systems use Chinese rolling stock or will be supplied with Chinese rolling stock as part of contracts signed before the 2020 ban.[91] Four of America's largest cities, Boston, Chicago, Philadelphia, and Los Angeles, utilize rolling stock produced by the China Railway Rolling Stock Corp., China's largest producer.[92] Beyond rolling stock, a 2022 Center for Security and Emerging Technology report also flagged that a number of U.S. transit agencies have procured information and communications technology and services hardware from covered entities such as Huawei and ZTE.[93]

U.S. transit systems' utilization of Chinese hardware presents yet another major cyber vulnerability. Transit rail is highly networked and often coordinated at a system-wide level.[94] A hostile actor with access to a specific network vulnerability could exploit it to disrupt or damage major U.S. transit systems or cause rolling stock to deliberately derail or collide.[95] In addition, transit agencies maintain a sizable amount of riders' personal information, including their names, addresses, emails, and payment information. Chinese actors certainly have the ability and motivation to exploit network vulnerabilities to access such user information for surveillance purposes, financial gains, or other reasons. U.S. laws are ultimately inadequate to protect America from these risks as well.[96]

---

[90] *Transit Infrastructure Vehicle Security Act*, U.S. Congress, *available at* https://www.congress.gov/bill/116th-congress/senate-bill/846?q=%7B%22search%22%3A%22H.R.+3%22%7D&s=1&r=76; *see also* Off. of Congressman Eric Swalwell, Swalwell, Garamendi Introduce Legislation to Secure FAA Transit Vehicles from Chinese Ownership (Apr. 26, 2023), *available at* https://swalwell.house.gov/media-center/press-releases/swalwell-garamendi-introduce-legislation-secure-faa-transit-vehicles#:~:text=The%20Transit%20Infrastructure%20Vehicle%20Security,%2C%20controlled%2C%20or%20subsidized%20companies.

[91] Zhong Nan, *Chinese maker delivers 1st of 400 subway cars for Chicago*, China Daily (last updated July 9, 2022), *available at* https://www.chinadaily.com.cn/a/202206/09/WS62a12d1ba310fd2b29e61855.html#:~:text=CRRC%2C%20China's%20largest%20rolling%20stock,Chicago%2C%20Philadelphia%20and%20Los%20Angeles.

[92] *Id.*

[93] Jack Corrigan, Sergio Fontanez, and Michael Kratsios, *Banned in D.C.: Examining Government Approaches to Foreign Technology Threats*, Center for Security and Emerging Technology (Oct. 2022), *available at* https://cset.georgetown.edu/wp-content/uploads/CSET-Banned-in-D.C.-1.pdf.

[94] *See* Washington Professional Systems, *Washington Metro Area Transit Authority – Rail Operations Control Center (ROCC)*, *available at* https://wpsproav.com/integration-case-studies/washington-metro-area-transit-authority/.

[95] Paulina Okunyte, *Infrastructure at risk: can trains be hacked*, Cybernews (Nov. 15, 2023), *available at* https://cybernews.com/editorial/train-hacking-explained/.

[96] Nassim Benchaabane, *Hackers steal data and demand ransom from Metro Transit in St. Louis*, St. Louis Post-Dispatch (Oct. 12, 2023), *available at* https://www.stltoday.com/news/local/crime-courts/hackers-steal-data-and-demand-ransom-from-metro-transit-in-st-louis/article_97f4ed36-67bb-11ee-9e48-4fcfe5eaa7ac.html.

E. Passenger Vehicles

Over the past two decades, automotive manufacturers have installed an ever-larger number of computer hardware components in the U.S. passenger vehicle fleet.[97] While the additional hardware has allowed the addition of numerous quality-of-life and safety improvements, the connection of many modern vehicles to the Internet enables outside actors to exploit their internal processes.[98] These hostile actors are able to exploit passenger vehicle vulnerabilities to leave vehicles inoperable,[99] cause vehicles to crash,[100] or cause EV batteries explode.[101] As vehicles become more interconnected, moreover, vulnerabilities can be exploited in order to launch a coordinated attack that renders fleets of vehicles simultaneously inoperable crippling U.S. defense capabilities and leaving populations hostage in the event of a kinetic attack.[102]

Moreover, as original equipment manufacturers ("OEM") include additional microelectronic features to augment their vehicles' electronic capabilities, users become more vulnerable to unknown entities accessing their personal information stored on vehicle computer systems without their authorization.[103] Even when OEMs claim to have full access to the vehicle's data, the foreign-origin components in automotive parts are likely to have embedded backdoors that allow infiltration by malign actors.

The degree to which U.S. automakers utilize Chinese hardware in the U.S. passenger vehicles is difficult to determine and may be part of the Commerce Department's recently announced semiconductor industrial base assessment.[104] Whatever the outcome of the agency's assessment, it is abundantly clear at the moment that China's semiconductor industry is well-positioned to dominate the auto chip sector. As the majority of semiconductors used in passenger vehicles are

---

97 *See* Wired, *Cars Are Just Software Now* (Oct. 20, 2022), *available at* https://www.wired.com/story/gadget-lab-podcast-571/#:~:text=This%20week%2C%20we%20discuss%20how,drive%2C%20and%20maintain%20our%20vehicles.&text=Modern%20cars%20are%20giant%20computers,%2C%20safer%2C%20and%20more%20comfortable.

98 U.S. Dep't of Transportation, *Connected Vehicles and Cybersecurity*, *available at* https://www.its.dot.gov/factsheets/pdf/cv_%20cybersecurity.pdf.

99 Kevin Poulsen, *Hacker Disables More Than 100 Cars Remotely*, Wired (Mar. 17, 2018), *available at* https://www.wired.com/2010/03/hacker-bricks-cars/.

100 Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, Wired (July 21, 2015), *available at* https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

101 Bart Ziegler, *Could Electric Vehicles Be Hacked?*, The Wall Street Journal (Feb. 14, 2023), *available at* https://www.wsj.com/articles/could-electric-vehicles-be-hacked-71a543e3.

102 Georgia Institute of Technology, News Release, *Hackers could use connected cars to gridlock whole cities* (July 28, 2019), *available at* https://www.eurekalert.org/news-releases/697837.

103 Patrick George, *Car Hackers Are Out for Blood,* The Atlantic (Sept. 11, 2023), *available at* https://www.theatlantic.com/technology/archive/2023/09/electric-car-hacking-digital-features-cyberattacks/675284/.

104 Press Release, U.S. Dep't of Commerce, Office of Public Affairs, Commerce Department Announces Industrial Base Survey of American Semiconductor Supply Chain (Dec. 21, 2023), *available at* https://www.commerce.gov/news/press-releases/2023/12/commerce-department-announces-industrial-base-survey-american.

legacy chips,[105]China has been rapidly expanding its production of these chips so that by 2027, it is estimated to control at least 33% of all legacy chip production worldwide.[106] China's focus on automotive semiconductor production stems, in part, from its need to support its growing OEM sector.[107] China's 2027 plans to engage in overcapacity, however, are nefarious and intended to distort global markets. To be clear, China has been a significant producer of legacy semiconductors and other electronic auto components for many years, and its products have been prevalent in most American and European vehicles since at least 2012-2015.[108] But, to date, very little has been done to mitigate the associated risks.

F. Election Infrastructure

Hardware and software vulnerabilities in the American voting system are likewise a very serious threat that should be addressed before the elections this year.[109] Voting systems are concentrated targets for attack,[110] and there are numerous hardware and software points of access to voting systems, including the individual voting machines, election-management systems (which are small networks of computers operated by state or county governments or outside vendors), and memory cards or USB sticks for the voting machines.[111] More than 30 states allow voters to cast electronic ballots, but many do not have basic security measures like encryption.[112] There are many additional gaps in election security, particularly in polling place equipment, that render large parts of the U.S. voting apparatus vulnerable to foreign interference.[113] More needs to be done to protect the integrity of Americans' ballots.

Congress and industry experts have already found that voting machines typically contain foreign-made chips and are particularly vulnerable to interference. The Senate Intelligence Committee

---

105 Sujai Shivakuma, Charles Wessner, and Thomas Howell, *The Strategic Importance of Legacy Chips*, Center for Strategic and International Studies (Mar. 3, 2023), *available at* https://www.csis.org/analysis/strategic-importance-legacy-chips.

106 *Id.*; Joanne Chiao and Eden Chung, *China's Share in Mature Process Capacity Predicted to Hit 29% in 2023, Climbing to 33% by 2027*, TrendForce (Oct. 18, 2023), *available at* https://www.trendforce.com/presscenter/news/20231018-11889.html.

107 Jeff Pao, *Will US target China's auto chip supply next?,* Asia Times (Oct. 29, 2022), *available at* https://asiatimes.com/2022/10/will-us-target-chinas-auto-chip-supply-next/; Sarah Wu, Jane Lee, and Kevin Krolicki, *Insight: How China became ground zero for the auto chip shortage*, Reuters (July 19, 2022), *available at* https://www.reuters.com/business/autos-transportation/how-china-became-ground-zero-auto-chip-shortage-2022-07-18/#:~:text=The%20scramble%20for%20workarounds%20has,maker%20and%20an%20auto%20supplier.

108 CBS News, *Ford Motor loses $3.1 billion due to chip shortage and Rivian* (Apr. 27, 2022), *available at* https://www.cbsnews.com/news/ford-motor-losses-chip-shortage-rivian/.

109 *See* Christina Cassidy, *Voting experts warn of 'serious threats' for 2024 from election equipment software breaches*, Associated Press (Dec. 5, 2023), *available at* https://www.pbs.org/newshour/politics/voting-experts-warn-of-serious-threats-for-2024-from-election-equipment-software-breaches.

110 *Id.*

111 *See id.*

112 Jerod Macdonald-Evoy, *In the absence of national regulations, how vulnerable is our voting infrastructure?*, Arizona Mirror (Sept. 24, 2020), *available at* https://www.azmirror.com/2020/09/24/in-the-absence-of-national-regulations-how-vulnerable-is-our-voting-infrastructure/.

113 *See, e.g.*, Jen Schwartz, *The Vulnerabilities of our Voting Machines*, Scientific American (Nov. 1, 2018), *available at* https://www.scientificamerican.com/article/the-vulnerabilities-of-our-voting-machines/

found significant supply chain vulnerabilities in voting machines in 2018.[114] A separate study found that some had security features turned off when they were shipped and used unencrypted hard drives.[115] A another study by a supply chain monitoring company found that a voting machine widely used in the United States from an unnamed vendor contained parts made by companies with ties to Russia and China. Despite pushback from the prominent American voting-machine suppliers, including Election Systems & Software, Dominion Voting Systems, and Hart InterCivic,[116] the report drew attention from the Hill and news outlets.

In January 2020, the CEOs of all three top voting-machine vendors testified before the Committee on House Administration of the U.S. House of Representatives.[117] Tom Burt, the CEO of Election Systems & Software, acknowledged that programmable logic devices for DS200 polling place ballot scanner are produced at a factory in China.[118] Additionally, John Poulos, CEO of Dominion Voting Systems, testified that his company sources "chip component level" inputs from China. He further indicated that there is currently no option for manufacturing some of these components in the United States. Julie Mathis, CEO of Hart InterCivic, concurred with Poulos on the supply chain issues and necessity of sourcing chips and other hardware components from China. All three CEOs conceded during the hearing that they would welcome guidance, comprehensive regulations, and reporting requirements from the federal government to protect the integrity of the U.S. voting system. There are currently no national guidelines for the procurement of voting machine components, for enhanced cybersecurity measures, or for local election officials to conduct audits or tests on electronic voting devices.[119]

The stream of coverage of these vulnerabilities since the 2016 election also has the effect of decreasing voter confidence in our election process.[120] The UCISA found that voting machines from Dominion Voting Systems used in at least 16 states had cybersecurity vulnerabilities that left them susceptible to hacking.[121] Particularly in the cybersecurity space, there is a low bar for supply

---

114 Alexa Corse, *Voting – Machine Parts Made by Foreign Suppliers Stir Security Concerns*, Wall Street Journal (Dec. 17, 2019), *available at* https://www.wsj.com/articles/voting-machine-parts-made-by-foreign-suppliers-stir-security-concerns-11576494003.

115 *See* Arizona Mirror, *supra* note 110.

116 Michaela Ross, *Chinese Technology in Voting Machines Seen as Emerging Threat*, Bloomberg Law (Jan. 9, 2020), *available at* https://www.bloomberglaw.com/bloomberglawnews/privacy-and-data-security/XADVSQES000000?bna_news_filter=privacy-and-data-security#jcite.

117 *See 2020 Election Security – Perspectives from Voting System Vendors and Experts*, 116th Cong. (Jan. 9, 2020), *available at* https://www.govinfo.gov/content/pkg/CHRG-116hhrg41318/html/CHRG-116hhrg41318.htm.

118 *See id.*; *see* Ben Popken, Cynthia McFadden, and Kevin Monahan, *Chinese parts, hidden ownership, growing scrutiny: Inside America's biggest maker of voting machines*, NBC News (Dec. 19, 2019), *available at* https://www.nbcnews.com/news/all/chinese-parts-hidden-ownership-growing-scrutiny-inside-america-s-biggest-n1104516.

119 *See* Arizona Mirror, *supra* note 110.

120 *See* Scientific American, *supra* note 111.

121 Kate Brumback, *Voting software in some states is vulnerable to hacking, U.S. cyber agency says*, Fortune (May 31, 2022), *available at* https://fortune.com/2022/05/31/voting-software-vulnerable-hacking/.

chain attacks.[122] The advent of AI creates an additional need to address threats and implement best practices for hardware and software. With vulnerabilities rampant and foreign meddlers already exaggerating the effects of attacks to spread misinformation, immediate action is necessary.[123]

In the 2020 hearing before the House, the CEO of Hart InterCivic asserted that a "sea change" would be necessary in global technology supply chains for the U.S. to produce the parts needed for voting machines. The time for that "sea change" has come.

G. Emergency Services and Medical Equipment

In addition to the long list of risks that result from significant U.S. dependence on Chinese hardware, the American Hospital Association's Center for Health Innovation recently pointed out that cyber threats to hospitals are grave and are directly influenced by the geopolitical climate.[124] Existing vulnerabilities from Chinese hardware in computer systems and medical equipment may be readily exploited to cripple healthcare systems. Ransomware attacks, which have affected hospitals and healthcare companies, provide an example of the potential impact of such vulnerabilities.[125] Experts predict that medical equipment and devices will increasingly become targets for malicious attacks, as health record management systems improve their ability to resist efforts to steal patient records.[126] For instance, malign actors can attack pacemakers to deliver lethal electric shocks to patients, and they can manipulate drug infusion and insulin pumps to deliver lethal doses.[127]

The House of Representatives China Select committee has already noted that China has the ability to access and remotely control U.S. medical equipment if the equipment contains Chinese-made cellular modules.[128] In recognition of such risks, the U.S. Food and Drug Administration ("FDA") is now requiring manufacturers to submit plans to address cybersecurity vulnerabilities for any

---

[122] Ashlee Benge, *Software Supply Chain Risks Loom Over Elections Systems*, SpiceWorks (Nov. 14, 2023), *available at* https://www.spiceworks.com/it-security/cyber-risk-management/guest-article/software-supply-chain-risks-loom-over-elections-systems/.

[123] Frank Bajak, *EXPLAINER: Threats to US election security grow more complex*, Associated Press (Nov. 2, 2022), *available at* https://apnews.com/article/2022-midterm-elections-technology-d6bf92f594343d7a489d40394e56e2a1.

[124] John Riggi, *Ransomware Attacks on Hospitals Have Changed*, AHA Center for Health Innovation (June 12, 2020), *available at* https://www.aha.org/center/cybersecurity-and-risk-advisory-services/ransomware-attacks-hospitals-have-changed.

[125] *See* Ryan Levi, *Ransomware attacks against hospitals put patients' lives at risk, researchers say*, NPR (Oct. 20, 2023), *available at* https://www.npr.org/2023/10/20/1207367397/ransomware-attacks-against-hospitals-put-patients-lives-at-risk-researchers-say.

[126] Tina Reed, *"A real Achilles' heel": Medical devices could be hacked next, officials fear*, Axios (Jan. 4, 2024), *available at* https://www.axios.com/2024/01/04/hackers-health-care-cybersecurity-medical-devices.

[127] Peter Jaret, *Exposing vulnerabilities: How hackers could target your medical devices*, AAMC News (Nov. 12, 2018), *available at* https://www.aamc.org/news/exposing-vulnerabilities-how-hackers-could-target-your-medical-devices.

[128] David Shepardson, *Two US lawmakers raise security concerns about Chinese cellular modules*, Reuters (Aug. 8, 2023), *available at* https://www.reuters.com/world/us/lawmakers-want-us-address-security-concerns-about-chinese-cellular-modules-2023-08-08/.

new medical devices.[129] The security requirements, passed as part of the December 2022 omnibus spending bill, require that all new medical device applicants to report how they intend to "monitor, identify, and address" cybersecurity issues and to provide the FDA with a "software bill of materials."[130] However, these FDA requirements do not apply to devices already on the market, nor do they adequately address the supply chain for hardware components.[131] There are also requirements to strengthen cybersecurity measures to prevent attacks. The American medical equipment system has substantial vulnerabilities that to date remain ignored and significantly unaddressed.

IV. POLICY RECOMMENDATIONS

What the forgoing discussion demonstrates is that the current capabilities of the United States' adversaries in the hardware-enabled cybersecurity domain is far greater than the United States'. China in particular is far better positioned to infiltrate our systems than we are to infiltrate theirs. Indeed, China controls the global supply chains for critical hardware components, and Chinese companies have their government's support to continue dominating the global markets in critical high-tech sectors. And whereas the CCP gives its national champions significant competitive advantages through heavy industrial subsidies and protections through aggressive market access barriers for foreign competitors, the United States welcomes cheap Chinese imports into its borders and does little to protect American industries that are injured by China's predatory economic practices.

As a result, America has ceded too much manufacturing capacity and technology to China over the past 20 years, and it needs to reverse this trend before it is too late. The U.S. Government needs a new policy mindset to strengthen its industrial base, and contrary to widespread belief, the solution is neither difficult nor impossible.

There exist today a broad range of effective legal authorities that can be – and ought to be – leveraged to restrict the U.S. importation and use of components sourced from China and other foreign adversaries. In particular, the E.O. entitled "Securing the Information and Communications Technology and Services Supply Chain"[132] is structured to prevent the use of high-risk Chinese hardware in U.S. telecommunications systems. The E.O. was issued in 2019 pursuant to the International Emergency Economic Powers Act ("IEEPA"), a federal law authorizing the president to regulate international commerce during peacetime after declaring a national emergency in response to any unusual and extraordinary threat to the United States. The E.O. was groundbreaking in that it represented the first time IEEPA was used to prohibit transactions involving information and communications technology or services ("ICTS") provided by foreign adversaries. More specifically, the E.O. authorizes the Commerce Department to prohibit transactions that involve ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary whenever the

---

129 *Id.*

130 Jennifer Korn, *FDA requires medical devices be secured against cyberattacks*, CNN (Mar. 29, 2023), *available at* https://www.cnn.com/2023/03/29/tech/fda-medical-devices-secured-cyberattacks/index.html.

131 *See id.*

132 White House, *Executive Order on Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019), *available at* https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-information-communications-technology-services-supply-chain/.

Government determines that such a transaction, or a class of transactions poses a serious risk to U.S. national security. At this time, the E.O. has been in existence for nearly four years. Although the threats posed by ICTS transactions with Chinese entities increase exponentially day by day, the E.O. has not yet been leveraged to prohibit *any* high-risk transactions.

Apart from forming the legal basis of the ICTS E.O., IEEPA is, by itself, a powerful and flexible legal authority. IEEPA grants to the President broad authority to regulate commerce for national security reasons. With respect to risks to critical domestic capabilities, including commercial items as well as infrastructure and defense systems, IEEPA can be used to prevent transactions with Chinese and other foreign malign entities. Even though IEEPA is valid law today, it has not yet been used to protect critical national security systems from Chinese infiltration.

To the extent the U.S. Government is reluctant to use these legal authorities to prohibit transactions with Chinese entities due to concerns about the absence of domestic production to meet supply chain needs, several points are in order. First, whenever national security risks are at issue, inaction is not an option; solutions must be found and implemented before catastrophic events take place. Second, the United States enjoyed strong and resilient supply chains merely 20 years ago before manufacturing capacity gradually offshored to China. In fact, 20 years is not too far off in history, which means that America has the ability replicate resilient supply chains onshore once again. Through incentive programs like the CHIPS Act, the Inflation Reduction Act, the Bipartisan Infrastructure and Jobs Act, and other federal award programs, the U.S. Government should focus on the manufacturing capabilities necessary to strengthen and sustain the *defense* industrial base. From the national security standpoint, priority sectors should include hardware necessary to support defense systems (e.g., integrated circuits for weapons systems) as well as leap ahead technologies that enable the United States to gain technological leadership over global competitors (e.g., leading edge chips).

Furthermore, given that Government resources are limited, federal awards may not be available to support manufacturing capacity for purely *commercial* hardware. Nevertheless, domestic production may be incentivized using laws that level the domestic playing field vis-à-vis foreign competition. Such laws restrict the importation of predatorily priced goods that threaten to displace domestic industry, and thereby give American industries the opportunity to grow and regain market share by operating in a fair economic environment. The trade laws include antidumping and countervailing duty laws; measures taken pursuant to Section 301 of the Trade Act of 1974, as amended; measures under Section 201 of the Trade Act of 1974, as amended; and restrictions under Section 232 of the Trade Expansion Act of 1962, as amended. Legal action taken under these authorities have been consistently upheld by U.S. Courts and the WTO, have been in use for decades, and are supported by substantial empirical data demonstrating their effectiveness.

Admittedly, lead time is always an important factor as domestic industrial growth does not happen overnight. As onshored production capacity gradually begins to come online (and/or as supply chains shift away from adversaries to trusted third-country partners), prohibitions on the use of high-risk hardware should be calibrated so as to not impede procurement for critical applications. Accordingly, the measures described above, including IEEPA and the trade laws, need not always be implemented in a sweeping manner. Whenever necessary, each prohibition on the use of foreign hardware may be phased in gradually to correspond with production capacity growth in both the domestic and allied markets. Beyond protecting U.S. systems from risks, these legal prohibitions

are also important in that they give investors confidence to support domestic projects with the knowledge that the project will be protected from economic predation in the future.

Finally, enforcement will be key. To the extent the U.S. Government prohibits the use of high-risk Chinese hardware in supply chains, it will need to ensure compliance. Today, most companies claim to lack adequate supply chain visibility at the third, fourth, fifth tier levels to comply with such restrictions. While this lack of visibility may be true, it is also deliberate. To be clear, companies have the ability to peer into their supply chains to eliminate prohibited hardware to ensure that they are compliant with any U.S. Government restrictions. The process involves a multi-level supply chain audit that begins with the product's bill of materials, and the audit only needs to be conducted for hardware items with potential for backdoor vulnerabilities. It does not need to reach every individual component in the finished item. Tamper-resistant products such as wires, chemicals, and plastics, are exempt from the audit trace, and by eliminating unnecessary traces, the audit process becomes focused, expeditious, and manageable for companies. The document contained in **Appendix Two** attached hereto represent a study I produced in cooperation with China Tech Threat that detail this audit approach. The document illustrates that compliance with prohibitions on the use of high-risk hardware is possible and not onerous. Inaction should no longer be an option.

In light of the ability to act immediately, the U.S. Government has no excuse for failing to act. The national security of the United States and the security and safety of United States persons depends on action now.

Appendix I

MEMORANDUM

DATE: October 20, 2023

RE: National Security Laws of the People's Republic of China and Their Capability to Undermine Compliance with U.S. or International Law

---

I. Introduction

The People's Republic of China (PRC) has spent over a decade shoring up a "legal Great Wall" to bolster national security protections and combat the ability of foreign regimes to undermine the government of China's (GOC), i.e., the Chinese Communist Party's (CCP), progress.[1] Several of the most prominent laws that have extraterritorial reach impacting Chinese, U.S., and foreign businesses, whether or not operating in China, are described below. Fundamentally, these Chinese laws conflict with U.S. laws and laws of other nations, and therefore render it impossible for businesses to simultaneously comply with both Chinese laws and the laws of the other jurisdictions in which they operate.

II. Biosecurity Law of 2020

The 2020 Biosecurity Law gives the National Security Commission of the CCP responsibility to coordinate biosecurity work.[2] The most prominent biosecurity area implemented to date is human genetic resources, reflected in Chapter VI of the law. The law's section on biotechnology states that the GOC must strengthen security management for research, development, and application activities and implement traceable management of "important equipment and special biological factors."[3] Biotechnology R&D efforts are categorized into high-, low-, and medium-risk activities under the law. Article 38 blocks foreign entities from conducting high- or medium-risk biotechnology R&D activities in China, requiring these entities to be "lawfully established and organized" as legal entities in the PRC and draft risk prevention and control plans.[4] Finally, the law imposes high penalties for violations. Under Article 75, the PRC can order a halt to R&D efforts while imposing a fine of up to 2 million RMB. Under Article 74, conduct found to be illegal

[1] China Daily, China builds legal Great Wall to safeguard national security: Official (Apr. 25, 2022), *available at* https://global.chinadaily.com.cn/a/202204/25/WS62663de4a310fd2b29e5926d.html.

[2] Zhonghua Renmin Gongheguo Shengwu Anquan Fa (中华人民共和国生物安全法) [Biosafety Law of the People's Republic of China] (promulgated at the 22nd Meeting of the Standing Comm. of the 13th Nat'l People's Cong., Oct. 17, 2020, effective Apr. 15, 2021), *translated in* China Law Translate, *Biosecurity Law of the P.R.C.*, https://www.chinalawtranslate.com/en/biosecurity-law/, Art. 4. ("Biosecurity Law").

[3] Biosecurity Law Art. 34, 39.

[4] Biosecurity Law Art. 38.

under the R&C provisions of the Biosecurity Law can result in sanctions on a company's managers and responsible personnel and management and fines between 1 and 10 million RMB where the value of unlawful gains is below 1 million RMB. When the value of unlawful gains is above 1 million RMB, fines can be between 10 and 20 million RMB and can be concurrently imposed with prohibition on conducting R&D efforts from 10 years to life.

While largely prompted to finalization by the COVID-19 outbreak, this law brings biosecurity into the umbrella of the national security apparatus, deeming it an "important aspect of national security."[5] Any individual or organization handling biological materials in China is potentially subject to the criminal provisions and penalties provided by the law. International biotechnology companies in a wide range of industries, including cosmetics, food and agriculture, healthcare, biotech, and pharmaceuticals, are affected by this law and its implementation. **The law has the effect of forcing companies working on R&D deemed as high- or medium-risk to incorporate as a PRC business entity and become subject to reporting requirements, potentially resulting in compulsory technology transfer in violation of U.S. laws.**

III. Negative Lists Updated in 2021 and 2022

The GOC restricts foreign investment through three negative lists. The Negative List for Market Access (Negative List) consists of sectors where investment from both Chinese and foreign companies is prohibited without special regulatory approval. Chinese and foreign investors are treated the same with respect to investment restrictions and approval requirements for sectors on the Negative List. The second, Special Administrative Measures for Foreign Investment Access (FDI Negative List), applies only to foreign investors. Similarly, the Special Administrative Measures for Foreign Investment Access in Free Trade Pilot Zones (FTZ Negative List) applies only to foreign investors with respect to their investment activities in free trade zones. The negative lists are updated regularly. The 2022 update to the Negative List added the news media sector to a list of 117 total items.[6] The current version of the FDI Negative List contains 31 industries, including mining of rare earths and tungsten, shipping and postal enterprises, legal businesses, research in the humanities and social sciences, and medical facilities.[7] The current version of the FTZ Negative List contains 27 of the industries listed on the FDI Negative list.[8] The four industries appearing on the FDI Negative List but not the FTZ Negative List are fishing of aquatic products, social research, printing of publications, and manufacture of Chinese proprietary medical products.

The GOC considers industries on the FDI Negative List to be critical to national security. For companies in FDI Negative List industries, Chinese government pre-approval is required for overseas initial public offerings. Overseas investors purchasing shares in overseas IPOs may not participate in the operation or management of these companies. The Administrative

[5] Biosecurity Law Art. 3.

[6] China Briefing, China's 2022 Negative List for Market Access (Apr. 12, 2022), *available at* https://www.china-briefing.com/news/chinas-2022-negative-list-for-market-access-restrictions-cut-financial-sector-opening/.

[7] C.I. Process, China foreign investment law and 2023 regulatory update (Aug. 8, 2023), *available at* https://www.ciprocess.com/china-foreign-investment-law-and-regulation.htm.

[8] Ziyou Maoyi Shiyan Qu Waishang Touzi Zhunru Tebie Guanli Cuoshi (Fumian Qingdan) (2021 Nian Ban) (自由贸易试验区外商投资准入特别管理措施（负面清单）（2021年版)) [Special Administrative Measures for Foreign Investment Access in Pilot Free Trade Zones (Negative List) (2021 Edition)] (promulgated by the 18th Executive Committee of the National Development and Reform Commission, Sept. 18, 2021, promulgated by Order No. 48 of the National Development and Reform Commission and the Ministry of Commerce, Dec. 27, 2021, effective, Jan. 1, 2021), *translated in* Garrigues, *Special Administrative Measures for Access of Foreign Investments in Pilot Free Trade Zones (Negative List) (2021 Edition)*, https://www.garrigues.com/sites/default/files/documents/2021_pftz_list.pdf.

Measures on Domestic Securities Investment by Qualified Foreign Institution Investors of 2012 provides that foreign investors may not participate in the operation or management of these companies and caps their holdings at 30% of shares. To avoid this equity cap, foreign investors that wish to participate in the market must enter partnerships, which often requires the transfer of technology, in addition to fraud, trade with sanctioned entities, and other types of activities that would be illegal under U.S. or international laws but entirely consistent with GOC laws.[9]

The PRC contends that the system of negative lists is comparable to review of investments in the United States by the Committee on Foreign Investment in the United State (CFIUS). These measures go beyond the scope of CFIUS review in the United States, however, by covering a broader range of transactions, including greenfield investments, and the review process is opaque. These negative lists generally foreclose certain investments entirely if foreign entities are unwilling to enter joint venture partnerships or incorporate as PRC entities.

IV. Hong Kong National Security Law of 2020

Article 3 of the law asserts that the GOC has "an overarching responsibility for national security affairs relating to the Hong Kong Specia Administrative region."[10] Article 54 specifies that the government will take "necessary measures to strengthen the management of" organs of foreign countries, international organizations, non-governmental organizations, and news agencies of foreign countries. This exposes U.S. citizens and companies to penalties and criminal fines for violations deemed a threat to Chinese national security, including calling for sanctions or authoring anti-GOC opinion articles. Under Article 55, courts in mainland China can exercise jurisdiction over national security cases that are "complex due to the involvement of a foreign country or external elements," in situations where the government in Hong Kong is unable to enforce the law, or if a "major and imminent threat to national security" has occurred.

V. Anti-Foreign Sanctions Law (AFSL) of 2021

The 2021 Anti-Foreign Sanctions Law (AFSL) provides legal basis for the GOC to implement retaliatory countermeasures against foreign laws and it prohibits compliance with foreign laws that undermine the GOC's or CCP's national objectives. In addition to creating a new PRC Countermeasure List, it codifies the administrative measures that created China's Provisions on the List of Unreliable Entities (PRC Entity List) and Measures for Blocking Importer Extraterritorial Application of Foreign Laws and Measures (Blocking Measures) – the GOC's mechanisms to sanction foreign persons or entities. Further, the AFSL creates a private right of action for Chinese citizens and organization to seek injunctive relief and damages against designated persons/entities.[11] The AFSL's first publicized use was in July 2021 when, in response to U.S. sanctions on PRC officials in Hong Kong, sanctions were imposed by China on seven U.S.

[9] U.S. Dep't of State, 2023 Investment Climate Statements: China, *available at* https://www.state.gov/reports/2023-investment-climate-statements/china/.

[10] Zhonghua Renmin Gongheguo Xianggang Tebie Xingzhengqu Weihu Guojia Anquan Fa (中华人民共和国香港特别行政区维护国家安全法) [Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region] (promulgated and effective at the 20th Meeting of the Standing Committee of the 13th National People's Cong., June 30, 2020, *translated in* Hong Kong Free Press, *In full: Official English translation of the Hong Kong national security law* (July 7, 202), https://hongkongfp.com/2020/07/01/in-full-english-translation-of-the-hong-kong-national-security-law/.

[11] Zhonghua Renmin Gongheguo Fan Waiguo Zhicai Fa (中华人民共和国反外国制裁法) [Anti-Foreign Sanctions Law of the People's Republic of China] (promulgated and enforced at the 29th Meeting of the Standing Comm. of the 13th Nat'l People's Cong., June 10, 2021), *translated in* China Law Translate, *Law of the PRC on Countering Foreign Sanctions*, https://www.chinalawtranslate.com/en/counteringforeignsanctions/#:~:text=Article%201%3A%20This%20Law%20is,our%20nation's%20citizens%20and%20organizations, Art. 12 ("AFSL").

persons, including former Commerce Secretary Wilbur Ross, the China director of Human Rights Watch, and directors and managers of the Congressional-Executive Commission on China and International Republican Institute.[12]

The GOC can designate persons and organizations to the PRC Countermeasure List that "directly or indirectly participate in the drafting, decision-making, or implementation"[13] of foreign sanctions. Relatives of designated persons, senior managers or actual controllers of listed organizations, organizations in which designated persons serve as senior management, and organizations in which designated persons are "actual controllers or participate in establishment and operations" may also be placed on the PRC Countermeasures List at the discretion of the GOC.[14] Entities on the PRC Countermeasures List can be subjected to visa restrictions, seizure and freezing of all types of property in the PRC, and prohibitions on any transactions or cooperation with organizations and persons in the PRC.[15] The law also includes an "{o}ther necessary measures" catch-all provision, which appears to give the GOC additional punitive authority.[16]

The ASFL is directly targeted towards U.S. sanctions, including primary sanctions imposed on Specifically Designated Nationals (SDNs) designated under the Uyghur Human Rights Policy Act of 2020 and the Hong Kong Autonomy Act of 2020 and secondary sanctions imposed on financial institutions transacting with SDNs. Because of its broad scope, the AFSL will cause challenges for MNCs operating in China because compliance with U.S. and other government sanctions will violate the AFSL and vice versa. The AFSL further expands the risk for both PRC and non-PRC companies and individuals who do business in China. Specifically, foreign investors or supply chain providers for Chinese technology companies will be impacted. The U.S. is not likely to accept compliance with the AFSL as a defense to alleged violations of U.S. sanctions. Potentially impacted companies can pursue mitigation measures including negotiating agreements to make litigation and arbitration subject to U.S. or international jurisdiction as the exclusive remedy from all disputes. Companies should also seek to include a provision in contracts that U.S. law governs, including in the event of a conflict of law, and avoid agreeing to contractual provisions permitting non-performance by parties based on the inclusion of a U.S. company or association with a person on the PRC Countermeasure List. Penalties should be included in contracts for breach even where failure to fulfill contract obligations is caused by the AFSL.

VI. Counter-Espionage Law of 2023

Updates to China's Counter-Espionage Law went into effect in July 2023. The PRC Ministry of State Security has emphasized the necessity of a system that makes it "normal" for the masses to participate in counter-espionage.[17] The law codifies this policy by obliging all PRC citizens and organizations to support and assist counter-espionage efforts.[18] However, the amendments to the law went beyond efforts to involve the populace: they expanded the scope of activities that can be considered espionage and codified the GOC's enforcement powers. Article 4(6) of the law

[12] Politico, Maeve Sheehey, China sanctions Wilbur Ross, others in response to U.S. warnings on Hong Kong (July 23, 2021), *available at* https://www.politico.com/news/2021/07/23/china-wilbur-ross-biden-us-warning-500686.

[13] AFSL Art. 4.

[14] AFSL Art. 5.

[15] AFSL Art. 6.

[16] AFSL Art. 6.

[17] Reuters, China wants to mobilise entire nation in counter-espionage (Aug. 1, 2023), *available at* https://www.reuters.com/world/china/china-wants-mobilise-entire-nation-counter-espionage-2023-08-01/.

[18] Zhonghua Renmin Gongheguo Fan Jiandie Fa (中华人民共和国反间谍法) [Counterespionage Law of the People's Republic of China] (promulgated at the 11th Meeting of the Standing Comm. of the 12th Nat'l People's Cong., Nov. 1, 2014, revised at the 2nd Meeting of the Standing Comm. of the 14th Nat'l People's Cong., Apr. 26, 2023), *translated in* China Aerospace Studies Institute, *In Their Own Words: Translation from Chinese source documents: Anti-espionage Law of the People's Republic of China*, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2023-05-15%20ITOW%20PRC%20Anti-Espionage%20Law.pdf, Art. 7-8 ("Counter-Espionage Law").

provides a new "other espionage activities" catch-all provision.[19] Further, where the prior law covered "state secrets and intelligence," Article 4(3) of the law expands the definition of espionage to cover "other documents, data, materials, or items related to national security" and information "incited, enticed, coerced, or bought" from state employees.[20] Article 4 also directly targets hacking and cyber-attacks, notably including disruption of "critical information infrastructure" in its list of acts of espionage and "agencies, organs, individuals, or other collaborators domestically or outside the PRC borders" within its espionage definition.[21]

The Counter-Espionage Law prompted the U.S. National Counterintelligence and Security Center, part of the Office of the Director of National Intelligence, to issue a public warning on heightened foreign business risk in China.[22] It has the potential to create legal risks and uncertainty for companies doing business in China because any documents, data, materials, or items could be considered relevant to PRC national security due to ambiguities in the law. The broad provisions of the law might apply to regular business activities. This law is of particular concern to companies doing business with the U.S. government, working on technology collaborations with Chinese enterprises, using data centers and cloud services in China, or conducting marketing research and business intelligence activities.[23] Such companies could be deemed to be conducting intelligence activities.

VII. Data Security Law of 2020

The Data Security Law broadly defines "Data Activities" in Article 2 to include activated undertaken by organizations and individuals outside of the PRC.[24] It imposes obligations in Article 28 to "promote economic and social development" in line with the CCP's "social morals and ethics."[25] Article 24 subjects companies processing "important data" to periodic security reviews.[26] Regardless of its origin, companies must obtain approval from the GOC under Article 36 to release data stored in China to any foreign judicial or law enforcement agencies.[27] The law authorizes CCP authorities to conduct compliance interviews.[28] Under Article 45, companies found in violation of regulations concerning "core data" can be penalized through forced shutdown of their businesses, fines of up to 10 million RMB, and criminal charges.[29] Under Article 48, companies found in violation of regulations concerning "important data" face penalties of up to 5 million RMB.[30] Article 26 authorizes the GOC to take reciprocal measures against "countries or regions" the CCP determines to be discriminatory with respect to data-related trade, investments, or technologies.[31]

[19] Counter-Espionage Law Art. 4(6).
[20] Counter-Espionage Law Art. 4(3).
[21] Counter-Espionage Law Art. 4(4).
[22] United States National Counterintelligence and Security Center, Safeguarding our Future: U.S. Business Risk: People's Republic of China (PRC) Laws Expand Beijing's Oversight of Foreign and Domestic Companies (June 20, 2023), *available at* https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/FINAL_NCSC_SOF_Bulletin_PRC_Laws.pdf.
[23] Forbes, Jill Goldenziel, China's Anti-Espionage Law Raises Foreign Business Risk (July 3, 2023), *available at* https://www.forbes.com/sites/jillgoldenziel/2023/07/03/chinas-anti-espionage-law-raises-foreign-business-risk/?sh=73989abc769e.
[24] Zhonghua Renmin Gongheguo Shuju Anquan Fa (中华人民共和国数据安全法) [Data Security Law of the People's Republic of China] (promulgated at the 29th Meeting of the Standing Committee of the 13th National People's Cong., June 10, 2021, effective, Sept. 1, 2021.), *translated in* DIGICHINA, *Translation: Data Security Law of the People's Republic of China (Effective Sept. 1, 2021)*, https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/ Art. 2 (Data Security Law).
[25] Data Security Law Art. 28.
[26] Data Security Law Art. 24
[27] Data Security Law Art. 36.
[28] *Id.*
[29] Data Security Law Art. 45.
[30] Data Security Law Art. Art. 48.
[31] Data Security Law Art. 26.

The U.S. Department of Homeland Security indicates that this law represents a shift in the CCP's attitude away from protecting Chinese data systems as a defensive mechanism and towards collecting data as an offensive act.[32] Given the Data Security Law's expansive compliance obligations, companies doing business in China must seek advice before exporting data from the PRC. The broad language in Article 2 extending liability beyond the territory of the PRC is a political tool in the U.S.-China technology relationship. Further, Article 24 gives the CCP the power to respond if CFIUS were to alt an acquisition over data access, or if any government enacts restrictions based on data issues related to China. It targets the expansion of CFIUS jurisdiction in 2018 to review transactions involving sensitive U.S. data, responding to U.S. government efforts to restrict companies like TikTok from storing data abroad.

VIII. Network Product Security Vulnerability Reporting Law of 2021

The Network Product Security Vulnerability Reporting Law imposes strict reporting requirements and controls on publicization of network security information. Article 4 direct organizations and individuals not to "illegally collect, sell, or publish" information on network product security vulnerabilities.[33] Article 7(2) mandates reporting to the PRC Ministry of Information and Technology on network security vulnerabilities within 2 days of discovery.[34] Organizations and individuals engaged in network product security work are directed by Article 9(3) not to "carry out malicious sensationalization" of vulnerabilities.[35] Article 9(6) specifies that during periods when the GOC holds "major activities," these organizations and individuals are prohibited from publishing information on network product security vulnerabilities without the consent of the Ministry of Public Security.[36] Further, Article 9(7) provides that information on vulnerabilities that is not public "must not be provided to overseas organizations or individuals other than the network product provider."[37] Penalties are provided for in accordance with the PRC's Cybersecurity Law.

The law tightens controls on the flow of information to the public, particularly before vulnerabilities have been resolved or addressed by the Ministry of Information and Technology and Ministry of Public Security. The law and its ambiguity in its references to covered entities, including individuals who discover product vulnerabilities, complicates the business environment for companies and vendors of network devices.

IX. Personal Information Protection Law of 2021

Like the Data Security Law and AFSL, the Personal Information Protection Law (PIPL) imposes extraterritorial jurisdiction. Article 3 of the law specifies that it applies that it is applicable not only

[32] U.S. Dep't of Homeland Security, Off. of Trade and Economic Security, Data Security Business Advisory: Risks and Considerations for Businesses Using Data Services and Equipment from Firms Linked to the People's Republic of China at 7 (Dec. 22, 2020), *available at* https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

[33] Gongye he xinxihua bu Guojia hulianwang xinxi bangongshi Gong'anbu guanyu yinfa wangluo chanpin anquan loudong guanli guiding de tongzhi (工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知) [Notice from the Ministry of Industry and Information Technology, the State Internet Information Office, and the Ministry of Public Security on the issuance of regulations for the management of network product security vulnerabilities] (promulgated by Order No. 66 of the Ministry of Industry and Information Technology, National Internet Information Office, Ministry of Public Security, July 12, 2021, effective, Sept. 1, 2021), *translated in* China Law Translate, *Provisions on the Management of Network Product Security Vulnerabilities* (July 14, 2021), https://www.chinalawtranslate.com/en/product-security-vulnerabilites/#:~:text=Provisions%20on%20the%20Management%20of%20Network%20Product%20Security%20Vulnerabilities,-By%20China%20Law&text=Article%201%3A%20These%20Provisions%20are,to%20defend%20against%20security%20risks Art. 4 (Network Product Security Vulnerability Reporting Law).

[34] Network Product Security Vulnerability Reporting Law Art. 7(2).

[35] Network Product Security Vulnerability Reporting Law Art. Art. 9(3).

[36] Network Product Security Vulnerability Reporting Law Art. Art. 9(7).

[37] Network Product Security Vulnerability Reporting Law Art. 9(7).

to organizations and individuals who process personally identifiable information (PII) in China, but also and organizations and individuals who process data of Chinese citizens' PII outside of China.[38] Article 3 also includes a catchall provision applying the law to "other circumstances provided in laws or administrative regulations."[39] Article 36 expands the restrictions imposed by the Data Security Law by requiring companies operating in the PRC to locally store all personal information collected and produced.[40] Non-PRC companies that need to provide PII to entities outside the PRC are required to agree to a GOC-formulated contract.[41] Article 38 mandates a security assessment by GOC authorities for cross-border transfers of personal information.[42] However, Article 38 references Article 40, specifying that if laws, administrative regulations, GOC information department provisions prevail if they prohibit such a security assessment.[43] "Personal Information" is broadly defined in Article 4 as "all kinds of information, recorded by electronic or other means, related to identified or identifiable natural persons," including video, voice, or image data.[44] Article 66 provides penalties for violating the law including fines of up to 50 million RMB or 5% of a company's annual revenue for the previous year, suspension of related business activities, revocation of operating permits for recertification, and negative social credit scores.[45] Directly responsible persons can be prohibited from holding supervisory positions or serving as personal information protection officers for an unspecified period of time and fined up to 1 million RMB.[46]

Like the Data Security Law, the PIPL would create conflicts of law that delay or impede discovery requests from U.S. and international courts. It focuses on protecting individuals, society, and national security in the CCP's political system, mirroring the broad political aims of the GOC.

X. Foreign Relations Law of 2023

This law, which provided a comprehensive framework for PRC foreign relations for the first time, is the latest in a sequence of statutes targeting U.S. and other countries' export control and sanctions regimes. The broadly scoped Foreign Relations Law asserts in Article 8 that "any organizations or individuals" that violate it and any other relevant laws will be held liable.[47] Article 32 asserts the PRC's right to employ countermeasures or restrictive measures that threaten its "sovereignty, security, and developmental interests."[48] This provision echoes language in the AFSL, reaffirming the GOC's ability to provide responses to foreign sanctions and emphasizing its authority to take action. Article 32 of the Foreign Relations Law likewise states that the PRC

[38] Zhonghua Renmin Gongheguo Geren Xinxi Baohu Fa (中华人民共和国个人信息保护法) [Personal Information Protection Law of the People's Republic of China] (promulgated by the Standing Committee of the 13th National People's Cong., Aug. 20, 2021, effective, Nov. 1, 2021), *translated in* DIGICHINA, *Translation: Personal Information Protection Law of the People's Republic of China – Effective Nov. 1, 2021*, https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/ Art. 3 (PIPL).

[39] *Id.*

[40] PIPL Art. 6.

[41] *Id.*

[42] PIPL Art. 38.

[43] PIPL Art. 38, 40.

[44] PIPL Art. 4.

[45] PIPL Art. 66.

[46] *Id.*

[47] Zhonghua Renmin Gongheguo Duiwai Guanxi Fa (中华人民共和国对外关系法) [The Law on Foreign Relations of the People's Republic of China] (promulgated by the Third Meeting of the Standing Comm. of the 14th Nat'l People's Cong., June 28, 2023, effective July 1, 2023), t*ranslated in* China Law Translate, *Foreign Relations Law (2023)* (June 28, 2023), https://www.chinalawtranslate.com/en/foreign-relations-law/, Art. 8 ("Foreign Relations Law").

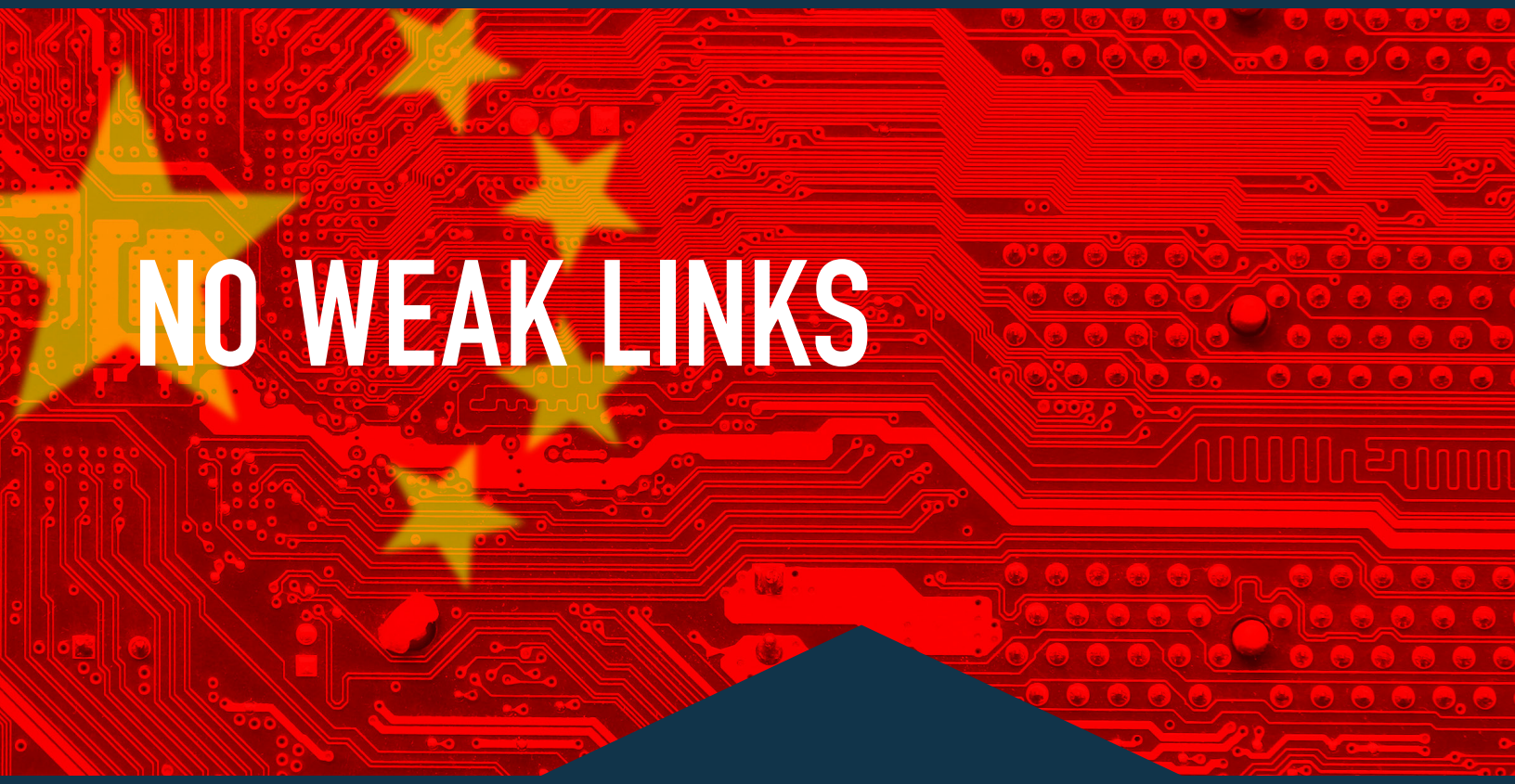
[48] Foreign Relations Law Art. 32.

will act to strengthen the implementation and application of laws and regulations in "foreign-related fields," suggesting wider extraterritorial application of the laws discussed above.[49]

Coupled with others, including the ASFL and the Data Security Law, the Foreign Relations Law demonstrates the PRC's continued efforts to assert its authority over companies and individuals doing business in China and abroad. It further codifies the PRC's intent to apply its national security laws extraterritorially in conflict with other countries' national security laws. Companies caught between conflicting laws will be forced to weigh their options and take risk-based approaches to their activities.

[49] Foreign Relations Law Art. 32.

Appendix II



NO WEAK LINKS

A STRATEGY FOR KEEPING U.S. DEFENSE SUPPLY CHAINS CLEAN OF DANGEROUS CHINESE TECHNOLOGIES

JUNE 1, 2023

IN CONSULTATION WITH NAZAK NIKAKHTAR, CHINA TECH THREAT SPECIAL ADVISOR[1]

China TECH THREAT

TABLE OF CONTENTS

PREFACE: WHY THE U.S. GOVERNMENT NEEDS TO ENSURE "CLEAN" SUPPLY CHAINS FOR DOD AND OTHER AGENCIES

The United States Government controls troves of sensitive information. Agencies responsible for American defense, intelligence, and diplomatic efforts, as well as numerous other federal agencies, rely on billions of dollars' worth of technologies to protect that information. Keeping that information secure is always a challenge, as the recent case of alleged leaker Jack Teixeira, a Massachusetts Air National Guardsman, indicates. Foreign adversaries' attempts to penetrate U.S. systems can have equally or even more damaging consequences.

Unfortunately, major government contractors may unwittingly be compromising sensitive information in their reliance on on electronic technology and/or software manufactured by companies owned or controlled by foreign adversaries, especially China. Today many items used by the federal government – e.g. smartphones, batteries, vehicles, and weapons systems – contain components with backdoor surveillance capabilities that retrieve sensitive U.S. Government information, "kill switches" that enable a foreign adversary to disable equipment while in use or tamper with the device remotely, causing systems disruptions or intentional malfunction. The additional reality is that a substantial quantity of these foreign-sourced components come from the People's Republic of China (PRC).

FBI Director Christopher Wray says that there is "no country that presents a broader threat" than the People's Republic of China.[2] At the same time, China is both a major technology manufacturer and home to a 2017 intelligence law which compels Chinese companies and citizens to turn over to the Chinese government any information it deems necessary for national security purposes. While Chinese business leaders have said they would refuse government directives, independent analysts insist they would be forced to comply.

> "They have no position to say no to the Chinese government."[3]
>
> *- Dr. Miles Yu, former State Department China Policy Advisor, commenting on the obligations of Chinese companies under Chinese law*

So why would contractors rely on suspect technology and how could our adversaries use backdoors? In recent years, Chinese President Xi Jinping has directed tens of billions of dollars in investments into semiconductor national champions YMTC, SMIC, and CXMT, growing their market share by 30 percent.[4] These sizable investments, coupled with China's non-market economy structure where prices of goods, land, electricity, and labor are intentionally distorted by the central government, enable Chinese products to be priced lower than competitors by approximately 40%-60% in many instances. But these price discrepancies are artificial (not driven by market forces), and are always subject to manipulation by the Chinese government. Nevertheless, major American contractors working with the U.S. Government have opted over the past 15 years to rely on Chinese electronics equipment and software, largely because Chinese products are less expensive.

It is technologically conceivable that the Chinese government could tamper with certain products in ways that would put U.S. national security interests in serious peril.[5] One prominent weapons system used on Ukrainian battlefields is BAE Systems' AGM88 harm air-to-surface missile.[6] This weapon relies on an array of highly sophisticated semiconductors. What if it was built with semiconductors from PRC-controlled companies and the PRC manipulated the microchips to disable the weapons?

While there are a handful of U.S. Government procurement regulations that prohibit the acquisition of Chinese equipment, the regulations are not fully enforced. Government contractors also lack adequate visibility into their upstream supply chains to ensure their own compliance. The U.S. Government has itself acknowledged many times that it lacks full visibility into its own supply chain dependence on Chinese entities. This creates a serious vulnerability in both the security of its electronics communications systems and its military systems.

The U.S. government does not know the extent to which Chinese technologies have penetrated the defense supply chain. This lack of visibility can and should be cured, and the process of doing so is not prohibitively complex. The solution depends on (1) knowing which critical government systems may rely on insecure technology and (2) replacing the technology with items sourced from trusted suppliers.

PROBLEM STATEMENT: CONTRACTORS' OPAQUE SUPPLY CHAINS INVITE INFILTRATION

Present high-technology supply chains are extremely layered. Federal government vendors, contractors, and "primes" (original equipment manufacturers) often lack adequate visibility into the supply chains of their second tier, third tier, etc. suppliers of goods or software. This lack of visibility encourages supply chain infiltration by foreign adversaries. Such risk to U.S. Government systems is unacceptable: infiltration into the Government's information and communications technology and services ("ICTS") systems and defense systems can introduce surveillance and/or hardware malfunction capabilities that could compromise America's communications, intelligence, and weapons capabilities and put the Defense Department's warfighters in serious peril. These vulnerabilities could impact allies as well, to the extent they procure U.S. equipment and software, and vice versa.

The core problem with existing supply chain rules is that they require self-policing without any enforcement mechanism.

At present, some, albeit limited, U.S. Government authorities exist that discourage or outrightly prohibit reliance on materials sourced from certain Chinese entities. These include the Federal Acquisition Regulations, the Defense Federal Acquisition Regulations Supplement, the Consolidated Appropriations Act of 2018, Section 889 of the 2019 National Defense Authorization Act ("NDAA") and Section 5949 of the 2023 NDAA. The core problem with these rules is that they require contractors to self-police, which most (if not all) simply lack the will (but not the resources) to do.[7] Nor does the U.S. Government have a mechanism to enforce these prohibitions, which means that vendors routinely ignore these requirements. The risks associated with ignoring supply chain vulnerabilities are too great and the Government's mitigation strategy needs to evolve

SOLUTION: INFORMATION GATHERING AND U.S. GOVERNMENT REPORTING THROUGH DEFENSE PRODUCTION ACT SURVEYS

Despite U.S. Government inaction to date, the Government does have authority to compel vendors to review their supply chain vulnerabilities and report them to the Government. For example, the Pentagon can mandate its primes to audit their supply chains for risks. Pursuant to authorities under section 705 of the Defense Production Act of 1950 as amended ("DPA") (50 U.S.C. app. 2155) and § 104 of Executive Order 13603 of March 16, 2012 (National Defense Resources Preparedness, 77 FR 16651, 3 CFR, 2012 Comp., p. 225), the U.S. Government conducts studies to determine whether the U.S. industrial base's capabilities appropriately support the U.S. Government, defense sector, or the broader domestic commercial supply chain.

To produce these studies, the Government (through the Department of Commerce) may issue Defense Production Act Surveys to collect detailed information related to the health and competitiveness of the U.S. industrial base from Government sources and private individuals or organizations. Such surveys are mandatory (they operate analogous to subpoenas) and are routinely issued to assess specific weak links in supply chains. Unfortunately, to date, the Surveys have not been used to comprehensively probe the supply chains of vendors that provide critical ICTS and defense capabilities to the U.S. Government. This is a significant shortcoming. The U.S. government has the capabilities to identify the source of the technological components in its supply chains. It should use them.

SURVEY METHODOLOGY AND OUTPUT: The following describes how the U.S. Government, including the Pentagon, could compel contractors and defense primes to audit their supply chains. The end goal would be for these contractors/primes to (1) certify that the chains are clean from components/software sourced from entities associated with foreign countries of concern or (2) report to the Government the presence of problematic components/software in their supply chains. Entities associated with foreign countries of concern would be entities located in or affiliated with (through ultimate beneficial owners, "UBOs") foreign countries of concern (including but not limited to China and Russia) – hereinafter collectively referred to as Foreign Entities of Concern, i.e., "FEOCs." The audit steps are straightforward and could materially affect the U.S. Government's supply chains for the better.

The Commerce Department, which would administer the Surveys, would start with a pilot project that could then be replicated for the broader industrial base, as follows:

1. COMMERCE DEPARTMENT ISSUES SURVEYS TO CONTRACTORS

Commerce would develop and issue on behalf of federal agencies surveys to all U.S. Government contractors/primes within a specific sector, for example unmanned aerial systems. (UAS). The

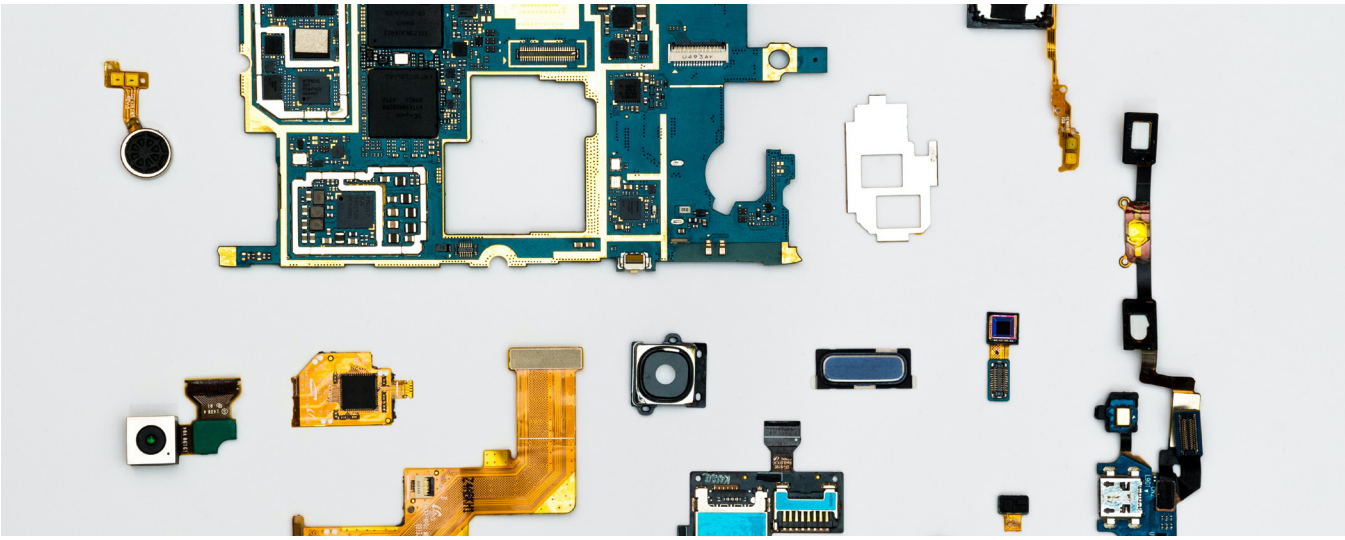
surveys would request information from the contractors/primes as to their material and software supply chains, and then require the contractors/primes to identify any potential critical components/software sourced from FEOCs. The following information would specifically be required:

a. All bills of materials ("BOMs") required to produce the final product (e.g., UAS) and imbedded critical components (e.g., lithium-ion batteries).

b. All software bills of materials ("SBOMs") required to produce the imbedded software.[8]

c. Description of all critical components/software included in the BOMs/SBOMs sourced from FEOCs. Critical components/software are all parts of the final product that could be used by a foreign adversary to (1) damage the operations of the final product, (2) create safety risks, (3) collect and transmit surveillance-type data from or through the final product or any related component/software, and (4) cause any other harm to U.S. national security.

d. Certification from the contractor/prime that it has conducted a complete audit of its supply chains up to the critical components/software, and that it confirms the absence of critical components/software from FEOCs, or if such supply chain vulnerabilities exist such that a certification cannot be provided, the contractor/prime would be required to report the supply chain vulnerability to the U.S. Government.



2. SURVEY RECIPIENTS CONDUCT DUE DILIGENCE

Upon receipt of the surveys, contractors/primes would need to take the following steps to comply with requirements 1.a-d:

a. Obtain the requested BOMs and SBOMs from in-house engineers and additional BOMs/SBOMs from all parts/software suppliers.

b. Identify all critical components from the BOMs/SBOMs identified in 2.a.

c. Steps 2.a and 2.b would continue until the contractor/prime has obtained BOMs/SBOMs identifying every upstream input used to manufacture the critical components that make up its final product (e.g., UAS). An upstream input would be defined as a product derived from

raw materials which are commodities and do not require specialized engineering processes to manufacture or which are tamper-resistant in their final form. So, for a lithium-ion battery, the inputs of interest would include the anode, cathode, electrolyte, and all building blocks of any embedded software code.

d. The contractor/prime would then identify all critical components that could be used to maliciously interfere with the operation of the final product, its parts, or otherwise collect surveillance data as described in 1.c above.

3. CONTRACTORS DIRECT SUPPLY CHAIN AUDITS

Based on the steps listed in 2.a-d above, the contractor/prime would then be required to conduct audits of its supply chains up to its critical component/software suppliers. This is a straightforward process and requires standard audit-type checks that identify all critical component/software suppliers to ensure that they are trusted. This is accomplished through a process of:

a. inventory record checks and production schedules,

b. examinations of supplier contracts,

c. purchase order reviews,

d. sales invoice reviews, and

e. corroboration against relevant accounting legers.

With respect to the UBO of each critical component/software supplier, there are databases, such as Dun & Bradstreet, that provide ownership information. To the extent a contractor/prime is unable to find the UBO of any supplier, this gap should be reported to the U.S. Government.

PROCESS EXAMPLE: THE LITHIUM-ION BATTERY

To illustrate the simplicity of this process, we provide the example of a lithium-ion battery included in a UAS, where the lithium-ion battery is produced by a battery pack manufacturer (tier two), who sources lithium-ion cells from cell suppliers (tier three), who then source the raw material anodes, cathodes, and electrolytes from other suppliers (tier four). Because the anodes, cathodes, and electrolytes are tamper-resistant, the supply chain audit would stop after the identities of the cell manufacturers are known (i.e., tier three being the highest point in the supply chain where tampering could occur).

In this example, the UAS contractor/prime could audit its own production records as well as the production records of its lithium-ion battery pack manufacturer (or it could contract with a third-party auditor to do this). To begin, the UAS manufacturer would examine its BOMs to determine the specific type of lithium-ion batteries that it incorporated into the UASs sold to the U.S. Departments of Interior and Defense. Using the BOMs, the UAS manufacturer would then identify the unique, product-specific serial numbers associated with the batteries to identify the battery pack manufacturers. The next steps involve supply chain audits of the battery pack manufacturers. Using the same serial numbers plus relevant production/sales records, the battery pack manufacturers will be able to identify their cell providers for each battery pack produced and sold to the contractor/prime. Relevant production/sales records include those listed in 3.a-e above. Again, the lithium-ion battery supply chain trace would end at the lithium-ion cell producer because the cell producer's raw materials are tamper-resistant, meaning that the highest level in the supply chain where malicious vulnerabilities could be introduced is at the cell level. If the cell and battery pack manufacturers are non-FEOCs, then the battery supply chain check is complete and the audit is successful.

The battery's SBOM, as it is itself a nested inventory (i.e., a self-contained list of ingredients that make up software components), could itself be checked by the UAS manufacturer. Alternatively, there are firms that can review software codes to detect backdoors and potentially malicious code, and could be hired by contractor/primes to review software that is being used.

CONCLUSION: A SUCCESSFUL PILOT PROGRAM PAVES THE WAY FOR BROADER IMPLEMENTATION

The foregoing audit checks may take several weeks up to several months to complete (depending on the complexity of the supply chain). However, even for larger contractors/primes, such as aircraft manufacturers, the traces can be accomplished within a year.[9]

Again, audit results and certifications should be provided to the U.S. Government through Survey responses, and records should be kept for at least five years. Certifications should confirm the absence of any components/software provided by FEOCs. Should contractors/primes find that certain components/software were provided by FEOCs, disclosures should be provided to the U.S. Government through Survey responses, and the Government should take immediate remedial action.

This pilot project, when proven to be successful, could be extended to all U.S. government contractors/primes using the same methodology described here.

ENDNOTES

1 China Tech Threat staff drafted this paper after consulting with CTT Advisor Nazak Nikakhtar. From 2018 to 2021, Nikakhtar served as the Department of Commerce's Assistant Secretary for Industry & Analysis at the International Trade Administration (ITA). Nikakhtar also fulfilled the duties of the Under Secretary for Industry and Security at Commerce's Bureau of Industry and Security (BIS). Additionally, Nikakhtar spearheaded the United States' first-ever whole-of-government initiative to evaluate and strengthen supply chains across all strategic sectors of the economy.

2 https://www.fbi.gov/news/stories/director-wray-addresses-threats-posed-to-the-us-by-china-020122

3 https://www.youtube.com/watch?v=jk3u2sfPQAg

4 https://www.nytimes.com/2022/08/29/technology/china-semiconductors-technology.html

5 https://semiengineering.com/chip-backdoors-assessing-the-threat/

6 https://www.reuters.com/graphics/UKRAINE-CRISIS/ARMS/lgvdkoygnpo/

7 This would be much like the current self-policing prohibitions on the importation and use of items derived from forced labor or conflict minerals.

8 SBOM is "a list of all the open source and third-party components present in a codebase. An SBOM also lists the licenses that govern those components, the versions of the components used in the codebase, and their patch status, which allows security teams to quickly identify any associated security or license risks." https://www.synopsys.com/blogs/software-security/software-bill-of-materials-bom/

9 Audits may be conducted every few years depending on the nature of the contractor's/prime's operations. If, however, the contractor/prime is required by the U.S. Government to keep FEOC components/software out of its supply chains and establish a robust system to ensure ongoing compliance, then audits will not need to be conducted as frequently.

NO WEAK LINKS

A STRATEGY FOR KEEPING U.S. SUPPLY CHAINS CLEAN OF DANGEROUS CHINESE TECHNOLOGIES

IN CONSULTATION WITH NAZAK NIKAKHTAR,
CHINA TECH THREAT SPECIAL ADVISOR

www.chinatechthreat.com

OPENING STATEMENT OF IVAN TSARYNNY, CHIEF EXECUTIVE OFFICER, FEROOT SECURITY

MR. TSARYNNY: Thank you very much, Co-Chairs Commissioner Wessel and Commissioner Helberg, for inviting me to the hearing today. I am the CEO of Feroot Security. Our company helps organizations eliminate threats posed by software that secretly tracks people online.

My testimony will focus on China's IT software products and the risks that they pose to American's user data and privacy. Feroot's research has given us an unprecedented look into the techniques our adversaries use to steal sensitive information. Therefore, I'm going to cover these three important areas:

Number one: what our research has revealed on web tracking pixels that collect sensitive information of U.S. persons and make it accessible to entities under Chinese jurisdiction including the Communist Party, the Chinese Intelligence, and other Chinese authorities.

Number two: how software connected hardware has a potential to conduct, and has been conducting, equally damaging surveillance.

Number three: policy recommendations along the lines that the Commission might make to Congress.

I will now start with the first part. We analyzed 3,500 websites of major companies and government agencies to really establish the baseline of data collection by tracking pixels.

What is a tracking pixel? It is a piece of code used by websites to track digital marketing campaigns, ad campaigns, and usually remain on websites after ad campaigns end. We found that ByteDance's TikTok collects a huge amount of U.S. based user data, even data belonging to people who never signed up or ever used TikTok in their life.

In fact, we worked with the Wall Street Journal to inform government agencies that their sites were indeed activating TikTok web tracking pixels without their knowledge.

So in March of 2023, less than a year ago, TikTok was collecting user data on approximately 7.5% of all of the U.S. business and government websites that we looked at. By December of '23, the presence of TikTok tracking pixels increased by 75% on financial services and banking sites rising from 5% to 8.5% of all sites; and increased by 178% on healthcare service provider websites, rising from 2% to 5% in just nine months.

So while tracking pixels collect data for legitimate purposes, that collected data can also be used for illegitimate and nefarious purposes including spying, interference in elections, spreading campaigns, and illegal surveillance.

For instance, TikTok tracking pixels are silently loaded on webpages where users enter their logins, passwords, schedule a doctor's appointment, or renew a license, or buy an airline ticket, amongst any other things. And TikTok sees everything that users enter into those online forms.

And unlike tracking pixels from other similar companies such as Meta, what we saw – and what we found is instances when TikTok also collects information that is shown to users on the pages themselves. So it's not just ad information.

Given this, it can capture very personal information such as search keywords that you enter, search results that you see on a page, purchases, transactions, and any other information you exchanged on or were shown on a page.

The below real-life examples in a screenshot in the testimony shows that happening on an appointment booking page for a healthcare provider.

So overall collection of data isn't new overall for social media companies or data brokers. But, because TikTok is governed by China's Cybersecurity Law, which requires all Chinese companies to share the data with China's authority, which are under the CCP's control. It creates a large risk.

For example, in '23 TikTok admitted to using the application's data to spy on journalists. Specifically, employees of TikTok's Chinese parent company ByteDance, accessed users' personal data including location data to track reporters' physical movements.

Additionally, just on January 30th, a couple of days ago, the Wall Street Journal reported that TikTok's workers are sometimes instructed to share data with ByteDance's employees without going through official channels.

Number two. Another channel for China's surveillance are the back doors in smart devices and appliances that can be used to allow someone to turn on the cameras, microphones, and silently modify software without anyone's permission to do whatever the vendor wants to do.

For instance, smart TVs have been found to have backdoors that enabled Chinese operators to silently modify software, take screenshots of what is on the page, upload those screenshots to servers in mainland China.

Last week, Radio Freedom published findings that various CCTV cameras manufactured by Hikvision and Dahua still uploaded videos to their servers even after users disable that feature. And also, these cameras have been found and have been reported to have been used by Russia in its January 2nd bombing of Ukraine that killed 39 civilians.

Today many TVs, refrigerators, music speakers, cameras, tablets—think of everything you might have at home, or in the office—even light switches, are always on, connected to the internet, and are controlled by software that is, can be, and was manipulated by Chinese companies, which makes them particularly useful for silent surveillance.

So what can be done about it? The CCP) has created powerful channels to collect data of U.S. based users. They are doing this by embedding their software into the building blocks of smart devices.

Our existing regulations do not adequately protect data against surveillance by China while creating a nightmare in terms of compliance and cost for honest businesses that follow the law.

I have four recommendations. Number one: establish clear rules for everyone that are compatible with other major regulations such as the European GDPR and other global rules.

Number two: prohibiting granting access to and transfer of U.S. based users' data to entities who are under Chinese control.

Number three: companies should be required to secure their technology supply chain to protect the data of U.S. based users at every stage, from the point of data creation and collection to the point of data destruction.

Number four: accountability - companies, along with their executives, that collect data from U.S. users should be held accountable, in a manner similar to how companies and their executives are personally accountable for compliance with regulations such as the Sarbanes Oxley Act.

Thank you.

COMMISSIONER HELBERG: Thank you, Mr. Tsarynny.

Mr. Corrigan.

PREPARED STATEMENT OF IVAN TSARYNNY, CHIEF EXECUTIVE OFFICER, FEROOT SECURITY

“Testimony before the U.S.-China Economic and Security Review Commission”

Current and Emerging Technologies in U.S.-China Economic and National Security Competition.

February 1, 2024
Ivan Tsarynny
CEO, Feroot Security.

Thank you very much, Co-Chairs Wessel and Helberg, for inviting me to the hearing today.

I am the CEO and Co-founder of Feroot Security, a company that helps organizations eliminate threats posed by software that secretly tracks people online.

My testimony will focus on China’s IT software products and the risks they pose to American users’ data and privacy.

Feroot’s research has given us an unprecedented look into the techniques our adversaries use to steal sensitive information. Therefore, I'm going to cover these three important areas:

Number one - what our research has revealed on web tracking pixels collecting sensitive information of U.S. persons and making it accessible to entities under China’s jurisdiction including the Communist Party, Chinese Intelligence, PLA and other Chinese authorities.

Number two - how software connected hardware has the potential to conduct—and has been conducting—equally damaging surveillance.

Number three - policy recommendations along these lines that the Commission might make to Congress.

Why Data Collection by Tracking Pixels is a National Security Risk?

The first portion of my testimony will focus on the collection of U.S. user data on websites.

Feroot analyzed more than 3,500 websites of major companies, healthcare providers and governments to establish the baseline of collection of user data by tracking pixels. A tracking pixel is a piece of code used by websites to track digital ad campaigns, and usually remain on websites after ad campaigns end.

We found that ByteDance's TikTok collects a huge amount of U.S.-based user data, even data belonging to people who have never signed up or used the TikTok app.

In fact, we worked with the *Wall Street Journal* to inform government agencies that their sites were indeed activating TikTok web tracking pixels without their knowledge, contrary to the executive orders that prohibited the use of TikTok and other technologies products from China.

By March of 2023, TikTok web tracking pixels were collecting user data on 7.5% of U.S. business and government websites.

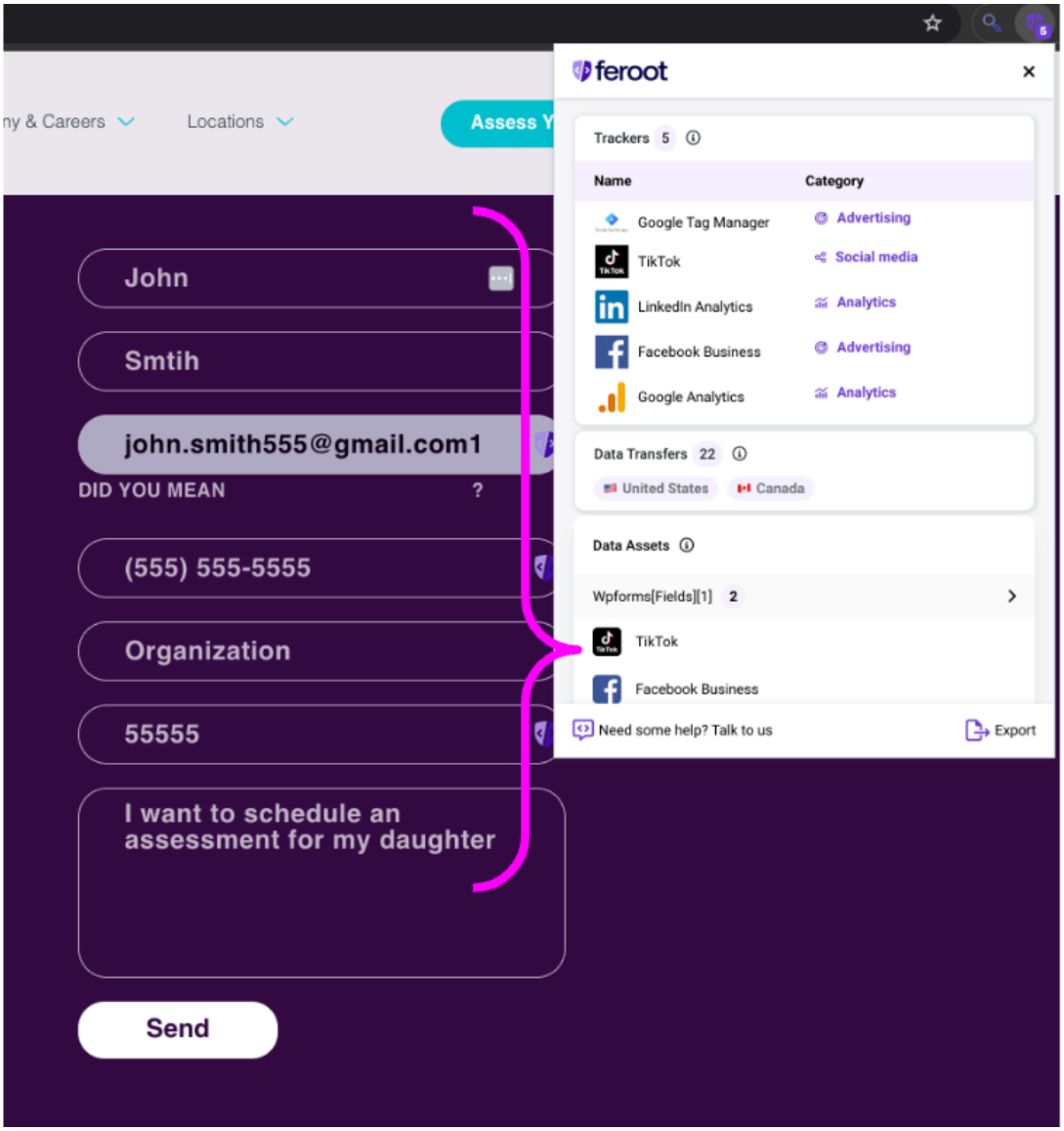
What's even more startling is that by December of 2023, we found that the presence of TikTok tracking pixels increased by 75% on financial services and banking websites—rising from 5% to 8.5%; and increased by 178% on healthcare service provider websites—rising from 2% to 5% of healthcare websites.

While tracking pixels collect data for legitimate purposes such as to advertise, enhance user experience, personalize content, or improve services, the collected data can also be used for illegitimate or nefarious purposes including spying, interference in elections, and illegal surveillance.

For instance, TikTok tracking pixels are silently loaded on webpages where users enter their login and password, schedule an appointment, renew a license or buy an airline ticket. TikTok sees everything users enter into online forms—and unlike tracking pixels from other similar companies such as Meta, we found instances when TikTok tracking pixel also collects information that is *shown to* users on web pages.

Given this, the data collection can capture very personal information: search keywords, search results, purchases, transactions, and any other information you exchanged or were shown online—which can reveal medical test results, pregnancy status, or pre-existing health conditions.

The below real life example demonstrates this:



In short, TikTok tracking pixels can know what websites you visit, what banks you log into, where you shop, travel and who your doctor is. *And all that data can be collected on people who have never used TikTok*.

Overall, collection of data isn't new to social media companies or data brokers. But, because TikTok is governed by China's Cybersecurity Law, which requires all Chinese companies to share data with China's authorities which are under Communist Party control, data collected by TikTok, and other companies from China, can be shared with the actors in China. Based on publicly available information it appears to have been shared already.

For example: in 2023, TikTok admitted to using the application's data to spy on journalists. Specifically, employees of TikTok's Chinese parent company ByteDance, accessed users' personal data including location data to track the reporters' physical movements.

This act of surveilling journalists appears to have been authorized by the highest level at ByteDance. Chris Lepitak, the chief internal auditor, led the team responsible for the spying. Lepitak's boss—based in China—reported directly to ByteDance's CEO Rubo Liang.

Additionally, on January 30, 2024, the WSJ reported that TikTok workers are sometimes instructed to share data with ByteDance workers without going through official channels, according to current and former employees and internal documents.

That data sometimes includes private information such as a user's email, birth date and IP address. Additionally, ByteDance workers in China update TikTok's algorithm so frequently that TikTok's U.S. employees struggle to check every change, and fear they won't catch problems if there are any.

Why surveillance by software connected hardware is also a national security risk

I will now turn to the second point I would like to make, which is how software connected hardware has the potential to do equally damaging surveillance.

Another channel for China's surveillance are *backdoors* in "smart" devices and appliances. Backdoors act as hidden passages that can be used to covertly gain access and allow someone to turn on cameras and microphones, and silently modify software without the consumers' knowledge or permission.

For instance, TCL Smart TVs were found to have a wide-open backdoor that enabled its Chinese operators to silently modify software on TVs, take screenshots and upload them to mainland China.

On January 25, 2024, Radio Freedom published findings that various CCTV cameras manufactured by Hikvision and Dahua still uploaded video to their servers even after users disable that service. Last but not least, these cameras were found to have been used by Russia to coordinate its January 2, 2024 bombing of Ukraine that killed 39 civilians.

Today many TVs, refrigerators, music speakers, cameras, tablets, even light-switches are considered "smart" because they are always on, connected to the internet, and are controlled by software that is manipulated by Chinese companies, which means they are particularly vulnerable to silent surveillance.

TikTok, ByteDance, or TCL are not the only threats. There are hundreds of companies and products from China with similar technology that can collect data on U.S. users.

What can we do about it?

The third part of my testimony provides the conclusion and suggestions for the Commission.

The Chinese Communist Party (CCP) has created powerful channels to collect data of U.S.-based users. They're doing this by embedding their software into the building blocks of smart, web and online products, which enables the CCP to perform mass surveillance of both online and offline lives.

China's tech giants including ByteDance, Tencent, Huawei, Alibaba, TCL Technology, and others, through their marketing and sale of highly popular tech products in the U.S., are gaining access to data of hundreds of millions of Americans. These are extremely popular applications like TikTok, CapCut, Lark, News Republic, Riot Games, WeChat, Tencent cloud, PUBG Mobile and countless online and smart products that collect data in the U.S.

The reason data collected by companies under China's jurisdiction can be used for surveillance is because, as you know, they are required to grant CCP's agencies access to the data they collect.

Our research overwhelmingly discovered that U.S.-based users' data are exposed to the CCP on websites that we all use on a daily basis.

If nothing is done about data collection by China in the United States, there will be a point where nearly all U.S. citizens could be surveilled by China's government.

While there have been a number of new data protection and privacy regulations introduced (noted below), they don't adequately protect data against surveillance by China, while creating a nightmare in terms of complexity and growing costs for honest businesses that follow the law.

Some examples include the European GDPR, multiple U.S. Federal and State Regulations: the Health Insurance Portability and Accountability Act, Gramm-Leach-Bliley Act's 2023 Safeguard Rules, California Consumer Privacy Act, Colorado Privacy Act, Washington My Health My Data Act and similar laws in Connecticut, Delaware, Iowa, Montana, Oregon, Tennessee, Texas, Utah, and Virginia.

I have five recommendations to conclude with:

Number One - establish clear rules for everyone.

Number Two - Make these rules compatible with other major regulations, such as the European GDPR.

Number Three - Prohibit granting access to and transfer of U.S.-based users' to entities under the jurisdiction of the government of China.

Number Four - Furthermore, companies should be required to secure their technology supply chain to protect the data of U.S.-based users at every stage, from the point of data creation and collection to the point of data destruction.

Number Five - Accountability: Companies, along with their executives, that collect data from U.S. users should be held accountable, in a manner similar to how companies and their executives are personally accountable for compliance with the Sarbanes-Oxley Act.

Thank you.

OPENING STATEMENT OF JACK CORRIGAN, SENIOR RESEARCH ANALYST, CENTER FOR SECURITY AND EMERGING TECHNOLOGY

MR. CORRIGAN: Co-chairs Wessel and Helberg, distinguished commissioners and staff, thank you for the opportunity to participate in today's hearing. It is an honor to testify alongside the experts on this panel and the two panels later in the day. I am currently a senior research analyst at the Center for Security and Emerging Technology at Georgetown University, where I study the U.S. innovation ecosystem, the flow of tech talent into and around the United States, and U.S. China technology competition. I would like to emphasize that the views I express today are my own.

Today my testimony will focus on how the United States regulates the use of Chinese manufactured information and communications technology and services, or ICTS, across U.S. digital networks. I will begin with a brief overview of existing U.S. policies related to the procurement and use of Chinese ICTS, I will discuss the challenges of implementing these policies, and I will conclude with a few recommendations for the commission.

U.S. policy makers have long voiced concerns that ICTS produced by certain Chinese technology companies pose significant risk to national security, as my fellow panelists have described. In recent years, policy makers have enacted various measures intended to keep these potentially compromised technologies out of government and commercial networks, I will refer to these measures broadly as procurement bans.

I describe these policies in detail in my written testimony, but a few are worth briefly mentioning here. The first is Section 889 of the 2019 National Defense Authorization Act, which prohibits federal agencies and their contractors from using ICTS from five Chinese technology companies, including Huawei and ZTE.

The second is the Secure and Trusted Communications Networks Act, which tasks the FCC with maintaining a list of foreign companies that pose "unacceptable national security risks." Service providers must inform the FCC when equipment from these firms are deployed in their networks, and groups that received FCC funds are prohibited from using this equipment as well.

While these two laws are well intended, they are too narrow and rigid to protect U.S. digital networks in today's dynamic threat landscape. I am happy to elaborate on their shortcomings during the Q & A. Luckily there are two existing government bodies that already possess the authorities to implement the broad, flexible regulations necessary to keep unsafe foreign technologies out of critical U.S. networks. These include the Federal Acquisition Security Council, or FASC, which was created by the 2018 Secure Technology Act, and the Commerce Department's Office of Information and Communications Technology and Services, or OICTS, which traces its origins to a 2019 Executive Order.

The FASC has the power to block federal agencies from buying any foreign technologies it deems to present national security risks, and also order the removal of such technologies from federal networks. OICTS has even broader authorities, which include the power to block any U.S. person, business or government agency from purchasing certain types of technology from entities connected to designated foreign adversaries, which includes China.

Even though the FASC and OICTS have the authority to implement procurement bans, they have yet to issue any such orders. This is likely due in part to the legal difficulties of standing up a new regulatory regime. It takes time to ensure the processes and procedures that they are using are robust enough to hold up in court. However, both groups have recently taken

promising steps towards implementing their authorities. Once they begin exercising those authorities, these two government bodies can begin constructing the flexible, targeted nationwide policy framework needed to mitigate foreign technology risks.

That said, even once procurement bans are issued, policy makers will still face obstacles to effectively implementing them. One major challenge is the complexity of the ICTS supply chain, which includes tens of thousands of companies scattered across the globe. The relationships between these suppliers are often opaque, which makes it difficult to determine where a particular piece of equipment originated. Technologies produced by Chinese firms deemed to present national security risks may be sold under different brand names or incorporated into other companies' products. In a few isolated cases, federal agencies have been found purchasing prohibited Chinese products that were sold under different brand names. Enforcing procurement bans in such a murky product ecosystem will require close monitoring and oversight, especially when those regulations apply to both public and private entities.

The second major challenge to implementing effective procurement bans is their cost. Chinese technologies are often significantly less expensive than their counterparts produced in the United States and allied countries. A standard Hikvision security camera may cost two, three or even four times less than a similar product produced by companies in Japan, South Korea, or Canada. This low price tag makes Chinese technologies attractive to many U.S. customers, especially those facing tight financial constraints, such as state and local governments.

A cash strapped school in rural Illinois may, for example, find itself choosing between buying a Hikvision security camera to monitor its playground, or going without any camera at all. Prohibiting the use of this cheap technology could drive up IT procurement costs to levels these organizations simply cannot afford. Increasing funding for the FCC's Rip and Replace program, which currently faces major budget shortfalls, could help offset some of these costs.

Additionally, targeting procurement bans at the sectors and networks where the potential national security risks are highest would help avoid placing undue financial burdens on U.S. businesses, government agencies, and other organizations.

To conclude, I'd like to offer three recommendations for how policy makers can build a more effective policy framework for regulating Chinese ICTS in the years ahead. First, going forward, policy makers should rely on the FASC and OICTS to implement procurement bans on Chinese technology. These two government bodies have the authorities necessary to regulate the use of these technologies across virtually every public and private network in the country. Ensuring they have the resources to effectively wield that power will be crucial to securing U.S. digital networks. Additionally, requiring the FASC and OICTS to publish orders in a digital master list of procurement bans would make it easier for public and private entities to keep track of the regulations that they must follow.

Second, FASC and OICTS should design procurement bans that target the sectors, networks, and use cases where breaches present the greatest risk to national security and ensure these regulations do not impose unnecessary compliance costs on business, government agencies, and other organizations. Striking this balance will be critical for successfully mitigating the risks posed by designated foreign technologies. Congress should also expand and appropriate more funds to the FCC's Rip and Replace program to help offset the high cost of procurement bans.

Third, as new procurement bans are enacted, OICTS and other agencies should collect data to monitor the implementation and effectiveness of their regulations across different sectors, geographies, and product categories. This information would help inform policy makers on how

to proceed with future regulations, and highlight ways to make existing regulations more effective. This monitoring capability would also likely require additional staff funding and resources which could be allocated by Congress.

With these measures in place, the federal government can more effectively address the risks posed by certain types of Chinese technologies across both public and private networks. Thank you, and I look forward to your questions.

COMMISSIONER HELBERG: Thank you, Mr. Corrigan, we will now shift over to my colleagues, and we will start with Commissioner Friedberg.

PREPARED STATEMENT OF JACK CORRIGAN, SENIOR RESEARCH ANALYST, CENTER FOR SECURITY AND EMERGING TECHNOLOGY

Testimony before the U.S.-China Economic and Security Review Commission
Hearing on "Current and Emerging Technologies in U.S.-China Economic and National Security Competition"

Jack Corrigan
Senior Research Analyst
Center for Security and Emerging Technology (CSET), Georgetown University
February 1, 2024

Co-chairs Wessel and Helberg, distinguished commissioners and staff, thank you for the opportunity to participate in today's hearing. It is an honor to testify alongside the experts on this panel and the two panels later in the day. I am currently a senior research analyst at the Center for Security and Emerging Technology at Georgetown University, where I study the U.S. innovation ecosystem, the flow of domestic and international tech talent, and U.S.-China technology competition.

Today my testimony will focus on the last topic, and specifically U.S. policies related to the procurement of Chinese-manufactured information and communications technology and services (ICTS). For more than a decade, U.S. leaders have warned that ICTS produced by certain Chinese companies presents national security risks. In recent years, policymakers have enacted a variety of measures intended to purge this technology from U.S. digital networks and supply chains. These measures (which I refer to broadly as "procurement bans") grant policymakers the authorities necessary to restrict the use of technologies deemed to present national security risks ("designated ICTS") across U.S. digital networks. While federal and state government agencies have slowly started to implement these procurement bans, there remain economic and bureaucratic factors that could impede the effectiveness of these policies.

My testimony will 1) provide a brief overview of the various risks posed by designated Chinese ICTS; 2) detail existing regulations related to foreign ICTS procurement; 3) discuss the prevalence of designated Chinese ICTS in the United States and barriers to implementing effective procurement bans; and 4) conclude with recommendations for how policymakers can begin developing a more targeted and cohesive nationwide framework for regulating Americans' use of foreign ICTS. These four recommendations include:

- Prioritizing broad, flexible federal authorities
- Fully funding "rip and replace" programs and related measures
- Targeting procurement bans to high-risk sectors, networks, and use cases
- Monitoring the implementation and effectiveness of procurement bans

Understanding the Risks Posed by Designated Chinese ICTS

Policymakers have long expressed concerns that ICTS produced by certain Chinese technology companies could pose significant risks to national security.[1] Their apprehension has grown over the last decade as the Chinese Communist Party (CCP) enacted measures that more closely linked the Chinese private sector to the government's intelligence operations. For instance, China's 2017 National Intelligence Law mandated that "any organization or citizen shall support, assist, and cooperate with state intelligence work according to law."[2]

While there are numerous specific concerns regarding the use of Chinese ICTS in U.S. digital networks, for the purposes of this hearing, we can think of these risks as falling into two broad categories: cybersecurity risks and economic risks.

Cybersecurity Risks

For years, national security leaders have warned that certain types of Chinese ICTS may contain backdoors or other vulnerabilities that could allow Chinese actors to gain unauthorized access to critical U.S. networks, platforms, and data. Technologies compromised in this way could potentially function as conduits for various Chinese actors to conduct espionage, cyberattacks, and other nefarious activities on users' networks. There is evidence that the CCP has indeed used Chinese-manufactured technology to conduct intelligence operations abroad. In 2019, the CCP was accused of using Huawei equipment to spy on the headquarters of the African Union.[3] An FBI investigation also revealed that Huawei equipment deployed near military bases in the United States was "capable of capturing and disrupting highly restricted Defense Department communications," although investigators did not disclose any evidence that such breaches had occurred.[4]

While federal policymakers seem generally aware of the cybersecurity risks posed by certain types of Chinese ICTS, the extent to which state and local government officials and commercial organizations recognize these risks remains unclear.[5] Only a handful of states have enacted policies to restrict the purchase of designated ICTS from China and other countries, and virtually no local governments have done so. While many government officials may be aware of the risks these technologies pose on an abstract level, in many cases their agencies lack the in-house technical expertise to fully assess and address those risks within their networks.

It is important to note that the actual risks posed by designated Chinese ICTS are highly context dependent. Integrating a piece of compromised equipment into the network of a military base presents very different risks to national security than using that same piece of equipment at an elementary school in rural Illinois, for example. To date, discussions of the cybersecurity risks posed by designated Chinese ICTS have largely ignored this distinction. Moreover, it is worth noting that Chinese-manufactured ICTS is not the only avenue through which Chinese actors

could gain unauthorized access to U.S. digital networks. The last decade has provided numerous examples of security breaches involving ICTS produced by U.S. companies. In 2023, for instance, Chinese actors exploited a vulnerability in Microsoft Outlook to access email accounts at the U.S. State and Commerce departments, as well as dozens of other U.S. organizations.[6] Clarifying the specific threats Chinese-manufactured ICTS pose in different contexts would help policymakers craft more targeted procurement bans and avoid placing undue financial burdens on public and private organizations.[7]

Economic Risks

The Chinese technology companies that have faced scrutiny on national security grounds have generally been market leaders. In 2018, the year U.S. policymakers began cracking down on the domestic proliferation of certain types of Chinese ICTS, Huawei was the top provider of telecommunications equipment and the second largest smartphone producer in the world.[8] Even today, Hikvision and Dahua, which have also been subject to U.S. procurement bans, remain the world's top two providers of digital surveillance equipment by revenue.[9] In many cases, firms achieved this market dominance with the help of Chinese industrial policy measures, which enabled companies to expand their global reach and offer lower prices than competitors headquartered in the United States and U.S.-allied countries.[10] This affordability has made certain types of Chinese ICTS popular among U.S. consumers, particularly those who make purchasing decisions primarily based on cost (such as financially constrained state and local governments). These buyers often cannot afford to pay higher prices for alternatives to designated Chinese ICTS. For example, a rural school district may find itself in a situation where it must decide between using a Hikvision or Dahua security camera to monitor a school playground or going without security cameras altogether.[11] Even in situations where consumers are aware of the cybersecurity risks posed by these technologies, they may determine that vulnerable equipment is better than no equipment.

On the whole, these economic dynamics have created a situation in which many consumers in the United States and allied countries rely almost entirely on Chinese companies for access to key technologies. The persistent demand for cheap ICTS has helped Chinese technology companies to entrench their market position and made it more difficult for non-Chinese competitors, whose products are often higher quality but more expensive, to achieve economies of scale that could ultimately drive down prices.

U.S. Policies on Chinese ICTS

To date, U.S. policies related to the procurement and use of Chinese ICTS have focused almost exclusively on mitigating cybersecurity risks rather than addressing economic risks of dependency on Chinese technology. These measures largely involve blocking various public and

private U.S. entities from integrating certain foreign ICTS ("covered ICTS") into their networks and authorizing certain U.S. government bodies to develop and implement procurement bans. While existing policies provide the policymakers with the authorities necessary to regulate the procurement, those authorities have not always been implemented effectively. Here I provide an overview of the major policies policymakers have enacted to mitigate the risks posed by certain types of Chinese ICTS:

Section 889 of the 2019 National Defense Authorization Act (2018)

Section 889 prohibits federal agencies from:

1. Using ICTS produced by five Chinese companies deemed to pose national security risks: Huawei (华为), ZTE (中兴通讯), Hikvision (海康威视), Dahua (大华), and Hytera (海能达);
2. Working with contractors that use covered ICTS anywhere in their networks; and
3. Awarding grants or loans to any entity for the purchase of covered ICTS.[12]

The potential impact of Section 889 is significant, as it would eliminate covered ICTS from the networks of federal agencies and the tens of thousands of companies with whom they do business. However, given the breadth of the federal contracting ecosystem and the ubiquity of certain types of covered ICTS, agencies may lack the capacity to enforce the law, which could limit its effectiveness.[13]

SECURE Technology Act (2018)

Title 2 of the SECURE Technology Act authorizes federal agencies to withhold contracts from vendors whose technologies present national security risks and creates the interagency Federal Acquisition Security Council (FASC) to evaluate those risks and implement mitigation strategies.[14] Those mitigation strategies may include exclusion orders (banning future procurement of covered ICTS) or removal orders (directing agencies to purge covered ICTS from their networks). The FASC has not yet issued any such orders. However, as of December 4, 2023, federal contractors are required to check for new FASC orders on SAM.gov.[15] This recent development indicates the FASC may soon begin to exercise its authorities.

Commerce ICTS Rule (2019)

The ICTS Rule authorizes the Commerce Department to restrict the purchase and use of foreign ICTS by any U.S. person (individual, business, government, etc.).[16] Specifically, the authority allows the department to block or unwind certain ICTS transactions that:

1. Pose "undue or unacceptable" national security risks, and
2. Involve U.S. persons and designated "foreign adversaries."*

The Commerce Department will consider more than a dozen criteria when determining whether to prohibit certain ICTS transactions and offer interested entities the opportunity to contest those determinations.[17] While no such rulings have been issued to date, the Bureau of Industry and Security (BIS) stood up an Office of Information and Communications Technology and Service (OICTS) to implement the rule and is reportedly conducting an investigation into the Russian security firm Kaspersky Lab.[18]

Secure and Trusted Communications Networks Act (2020)

The Secure and Trusted Communications Networks Act, enacted in 2020, authorized the Federal Communications Commission (FCC) to create a list of companies that pose "unacceptable" national security risks.[19] Organizations that receive FCC funds—a group that includes hundreds of public and private entities—are prohibited from buying ICTS from firms on the list. The law also created a program (the Secure and Trusted Communications Networks Reimbursement Program) through which small U.S. telecom providers could receive funding to "rip and replace" covered ICTS already deployed in their networks.† Though promising, the program currently faces a major budget shortfall.[20] Additional funding from Congress is required to support an effective rip and replace initiative.

FCC Equipment Authorization (2022)

In November 2022, the FCC voted to block new equipment authorizations for ICTS produced by the five Chinese firms listed in Section 889 (i.e., Huawei, ZTE, Hikvision, Dahua, Hytera).[21] The decision effectively outlaws the import, sale, and use of this covered ICTS across the United States, marking a significant step toward removing technology deemed to present national security risks from U.S. digital networks. However, the measure will take time to achieve its desired effect. The ban only applies to new authorizations, meaning products from Huawei and other companies that have already received FCC authorization can still be legally bought and sold in the United States. The FCC is reportedly exploring how restoring its net neutrality regulations might impact its authorities to purge designated ICTS from U.S. networks.[22]

State Procurement Bans (2019 – Present)

* Executive Order 13873, from which the ICTS Rule originated, explicitly names China, Russia, Iran, North Korea, Cuba, and Venezuela as foreign adversaries.
† The program is initially focused on replacing equipment from Huawei and ZTE.

Over the years, a handful of state governments have also enacted measures to restrict the procurement of foreign ICTS deemed to present national security risks.[23] However, the scope and effectiveness of these procurement bans vary widely. While some states have aligned their regulations with federal procurement bans, others have attempted to create their own procurement blacklists. These custom lists often target different companies than the federal regulations and are, in some cases, too broad to be meaningfully enforced.[24] Some state regulations also focus on prohibited vendors rather than prohibited technology, which creates major loopholes that allow covered ICTS into government networks.[25]

Final Thoughts on ICTS Procurement Authorities

Today, U.S. policymakers possess the authorities necessary to eliminate Chinese ICTS deemed to present national security threats from U.S. networks. However, these authorities have not always been implemented effectively and, given the overlap between various authorities, the current regulatory landscape can often be difficult to navigate. Going forward, policymakers should work to build a more targeted and cohesive nationwide framework for regulating the use of designated Chinese ICTS. This framework would rely on federal orders—namely those issued through the FASC and OICTS—to govern the use of Chinese ICTS across the private and public sector. The FCC could also play a critical role in supporting efforts to replace the designated ICTS already deployed in U.S. networks if provided more funding for its existing rip and replace program. I will offer more details on how this framework could be implemented in the final section of this testimony.

The Challenges of Eliminating Designated Chinese ICTS from U.S. Digital Networks

Despite the aforementioned policies and discourse highlighting the risks posed by certain types of Chinese ICTS, these technologies are still prevalent across the United States. A study from the Center for Security and Emerging Technology (CSET) found that between 2015 and 2021, at least 1,681 U.S. state and local government entities purchased equipment produced by the five companies listed in Section 889, and while these transactions decreased after federal bans went into effect, they did not stop altogether.[26] The CSET analysis should be viewed as a low-end estimate of the number of state and local governments using this equipment—the actual number is likely much higher.

To be clear, these transactions, by and large, were perfectly legal. Few state governments and virtually no local governments have implemented procurement bans on Chinese ICTS, and federal policymakers have not yet used the authorities at their disposal (ICTS Rule) to regulate state and local governments' procurement behavior. At the federal level, there is no evidence to suggest wide-scale use of designated Chinese ICTS. However, these technologies remain popular in the commercial sector due to their relatively low cost.

There are a number of factors that help explain why the country's existing regulatory framework has not been wholly effective in removing designated Chinese ICTS from U.S. digital networks. These include:

Supply Chain Complexity

The ICTS supply chain includes tens of thousands of companies scattered across the globe. ICTS produced by Chinese firms designated as national security risks may be sold under different names and brands, or they may be integrated into products and services from otherwise trustworthy suppliers.[27] In a few isolated cases, federal agencies have reportedly purchased covered Chinese ICTS that was sold under different brand names.[28] ICTS is also often sold through third-party vendors, who may further obscure the technologies' origin. This complexity makes it difficult to determine the provenance of a particular piece of equipment, which in turn complicates the process of identifying and excluding particular types of ICTS from untrustworthy sources.

Incohesive Policy Strategy

Today, U.S. policy towards Chinese ICTS consists of a patchwork of overlapping, complicated regulations. In this environment, it is not always clear to organizations which rules and regulations they ought to follow. Developing a more cohesive regulatory framework—and communicating those policies clearly—will allow businesses, governments, and other organizations to make informed ICTS procurement decisions. Given its broad jurisdiction and unique intelligence capabilities, the federal government is in the best position to lead this effort. The regulations implemented through the FASC and OICTS can serve as the backbone for this policy framework. Aggregating and publishing orders issued by these bodies in a publicly available "master list" of federal regulations on foreign ICTS procurement would further clarity on legal obligations and best practices for different public and private organizations.

Slow Implementation

While federal policymakers have the necessary authorities for keeping designated foreign ICTS out of U.S. digital networks, many of their most powerful authorities have yet not been used. The FASC, for instance, has not issued a single order to block or remove designated ICTS from government networks. The Commerce Department's OICTS, which has the authority to regulate all public and private ICTS transactions, has also not issued any rulings or decisions. To some extent, these delays are understandable—foreign technology procurement bans are a relatively new type of regulation, and implementing them effectively takes time and resources. These regulations have proven to be legally contentious, so it is important that the processes and

procedures involved in their implementation are transparent, fair, and airtight.[29] However, without FASC or OICTS orders to block the procurement of designated ICTS, this technology will continue to proliferate across U.S. digital networks.

Looking to the future, even after government bodies begin issuing orders, enforcing those regulations will likely prove challenging. The domestic ICTS market is expansive, touching virtually every person, commercial business, and government agency in the United States. As such, providing staff, funding, and other resources to support effective oversight will be critical to the successful implementation of these policies. Without such a commitment, we will see potentially risky technologies and services continue to proliferate across the U.S. digital networks.

Underfunded Rip and Replace Programs

Purging designated Chinese ICTS from U.S. digital networks is a resource-intensive endeavor. These high costs make it unlikely that organizations will be able to undertake rip and replace efforts without the financial support of the government. Today, the FCC's rip and replace program faces a budget shortfall of roughly $3.1 billion, and that funding gap will only grow if the program expands to cover Chinese ICTS beyond Huawei and ZTE. Providing additional funds for rip and replace programs will be critical to ensuring their effectiveness.[30]

The High Costs and Ambiguous Benefits of Procurement Bans

Procurement bans can impose significant costs, and for a lot of organizations, the benefits of complying with these regulations are not always clear. As previously noted, there are often few alternatives to designated Chinese ICTS available at comparable prices. As such, forgoing cheap Chinese technology often drives up procurement costs to levels that many organizations cannot afford. Insufficient funding for existing rip and replace programs, as well as proactive funding for future ICTS procurement initiatives, has only exacerbated this problem.

Furthermore, while paying more for increased security is justifiable for some organizations (government agencies, critical infrastructure operators, etc.) for others, the costs of such measures likely outweigh their benefits. Overall, the risks associated with specific types of foreign ICTS vary widely based on how and where that technology is deployed. Banning these technologies may not be warranted in situations where security breaches present few potential national security risks. Analyzing the costs and benefits of procurement bans in light of the full threat landscape is crucial for ensuring government resources are efficiently distributed and regulations on foreign ICTS procurement target the sectors, networks, and use cases where the risks to national security are highest.

Looking Ahead

Addressing the risks posed by certain types of Chinese ICTS will require a targeted and cohesive nationwide policy framework on foreign technology procurement. The federal government is well-positioned to develop and implement this framework, and policymakers already have the necessary authorities to do so. Going forward, agencies should seek to design procurement bans that target the sectors, networks, and use cases where breaches present the greatest risks to national security and ensure these regulations do not impose unnecessary compliance costs on businesses, government agencies, and other organizations. Striking this balance will be critical for successfully mitigating the risks posed by designated foreign ICTS. To conclude, I offer four recommendations for policymakers looking to design such a framework:

1. **Prioritize broad, flexible federal authorities**

The federal government is well-positioned to lead the development of a nationwide regulatory framework for the purchase and use of foreign ICTS. Agencies have various policy levers they can use to keep designated ICTS out of U.S. digital networks, but the FASC process and ICTS Rule are the most promising and should be prioritized in the years ahead. If implemented effectively, these two authorities could govern ICTS procurement across every economic sector: the FASC process would allow federal agencies to keep designated technology out of their networks, and the ICTS Rule would enable the Commerce Department to regulate ICTS deployed across the networks of non-federal entities (state and local governments, commercial businesses, etc.). These two authorities also offer policymakers the flexibility to tailor bans to particular applications of particular technologies (e.g. outlawing certain Chinese-manufactured surveillance cameras on the networks of financial institutions) and update regulations as the threat landscape changes.‡ Existing federal procurement bans could eventually be incorporated into these two frameworks (e.g. OICTS could issue orders prohibiting U.S. telecom companies from using ICTS from the entities on the FCC covered list). Once successfully implemented, the FASC process and ICTS Rule could eliminate the need for other procurement bans.

Additionally, orders issued by the FASC and OICTS should be aggregated and published in a publicly available "master list" of federal regulations on foreign ICTS procurement. This list could be modeled on the Treasury Department's "Sanctions List Search" portal.[31] Publishing these orders in an accessible, easy-to-search online format would make it easier for other public and private entities to keep track of the regulations they must follow and better understand the landscape of foreign ICTS risks. This list could also serve as a baseline for any organization that wishes to implement its own restrictions on foreign ICTS procurement.

‡ Procurement bans that enshrine designated companies in federal statute, like Section 889, are less flexible than these executive branch authorities.

2. **Fully fund "rip and replace" programs and related measures**

Rip and replace programs will play a critical role in keeping designated foreign technology out of U.S. digital networks. Replacing this equipment is a costly endeavor, and organizations are unlikely to undertake these efforts without financial support. Ensuring programs like FCC's Secure and Trusted Communications Networks Reimbursement Program are fully funded would ensure businesses, government agencies, and other organizations have the resources to comply with relevant procurement bans. As new regulations go into effect, these programs could be expanded to offset the higher procurement costs that certain resource-constrained entities will face as they transition away from covered ICTS.

3. **Target procurement bans to high-risk sectors, networks, and use cases**

Eliminating all designated Chinese ICTS from every U.S. network would be prohibitively expensive, if not impossible. Furthermore, overly broad bans (such as those enacted by some state governments) can impose enormous costs across the economy, particularly when there are few cost-competitive alternatives from trusted sources. As such, it is crucial that policymakers target procurement bans and rip and replace funding at the sectors, networks, and use cases where breaches present the greatest risks to national security. The intelligence community, Cybersecurity and Infrastructure Security Agency, and other federal bodies can inform these decisions on how to target bans so as to maximize their impact and avoid imposing undue compliance costs.

4. **Monitor the implementation and effectiveness of procurement bans**

Finally, as new procurement bans are enacted, OICTS and other agencies should collect data to monitor the implementation and effectiveness of their regulations across different sectors, geographies, and ICTS categories. This information would help inform policymakers on how to proceed with future regulations and highlight ways to make existing regulations more effective. This monitoring capability would likely require additional staff, funding, and resources, which could be allocated by Congress.

[1] Mike Rogers and Dutch Ruppersberger, "Investigative Report on the U.S. National Security Issues Posed by Chinese Telecommunications Companies Huawei and ZTE," (U.S. House of Representatives, October 8, 2012), 3, https://republicans-intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf#page=11.
[2] Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare, July 20, 2017, https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.
[3] Salem Solomon, "After Allegations of Spying, African Union Renews Huawei Alliance," Voice of America News, June 6, 2019, https://www.voanews.com/a/after-allegations-of-spying-african-union-renews-huawei-alliance/4947968.html.

[4] Katie Bo Lillis, "CNN Exclusive: FBI investigation determined Chinese-made Huawei equipment could disrupt U.S. nuclear arsenal communications," CNN, July 25, 2022, https://www.cnn.com/2022/07/23/politics/fbi-investigation-huawei-china-defense-department-communications-nuclear/index.html.
[5] Jack Corrigan, Sergio Fontanez, and Michael Kratsios, "Banned in D.C." (Center for Security and Emerging Technology, 2022), https://cset.georgetown.edu/wp-content/uploads/CSET-Banned-in-D.C.-1.pdf#page=11.
[6] Raphael Satter and Zeba Siddiqui, "Chinese hackers stole emails from US State Dept in Microsoft Breach, Senate staffer says," *Reuters*, September 27, 2023, https://www.reuters.com/world/us/chinese-hackers-stole-60000-emails-us-state-department-microsoft-hack-senate-2023-09-27/.
[7] Corrigan et al., "Banned in D.C."
[8] "Key Takeaways – Worldwide Telecom Equipment Market 2018" Dell'Oro Group, March 4, 2019, https://www.delloro.com/telecom-equipment-market-2018-2/; Jeb Su, "Huawei Fortifies #2 Spot in Global Smartphone Market, Beating Apple Again," Forbes, November 2, 2018, https://www.forbes.com/sites/jeanbaptiste/2018/11/02/huawei-fortifies-2-spot-in-global-smartphone-market-beating-apple-again/?sh=541020fd1305.
[9] "2023 Security 50 Industry Report," *ASMag.com*, Accessed January 2024, https://www.asmag.com//2023_security50_industry_report.pdf.
[10] Kim Sutter, "Made in China 2025" Industrial Policies: Issues for Congress (Washington, DC, Congressional Research Service, 2020), https://sgp.fas.org/crs/row/IF10964.pdf; Alex Rubin, Alan Omar Loera Martinez, Jake Dow, and Anna Puglisi, "The Huawei Moment" (Center for Security and Emerging Technology, 2021), https://cset.georgetown.edu/publication/the-huawei-moment/.
[11] Corrigan et al., "Banned in D.C."
[12] Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment, Pub. L. No. 115-232, 132 Stat. 1917 (2018).
[13] Corrigan et al., "Banned in D.C."
[14] Federal Acquisition Supply Chain Security Act of 2018, Pub. L. No. 115-390, 132 Stat. 5178 (2018).
[15] FAR 4.2303 (2024).
[16] Securing the Information and Communications Technology and Services Supply Chain, 86 FR 4909 (2021).
[17] Securing the Information and Communications Technology and Services Supply Chain; Connected Software Applications, 88 Fed. Reg. 39353-39358 (June 16, 2023), https://www.federalregister.gov/documents/2023/06/16/2023-12925/securing-the-information-and-communications-technology-and-services-supply-chain-connected-software
[18] John D. McKinnon and Dustin Volz, "Biden Administration Weighs Action Against Russian Cybersecurity Firm," *The Wall Street Journal,* April 7, 2023, https://www.wsj.com/articles/biden-administration-weighs-action-against-russian-cybersecurity-firm-b84afcd7; "Office of Information and Communications Technology and Services (OICTS)," *BIS.gov*, Accessed January 2024, https://www.bis.doc.gov/index.php/oicts.
[19] Today, the FCC's covered list includes 10 companies: the five Chinese firms covered by Section 889, four other telecommunications companies with direct or indirect ties to the CCP, and Kaspersky Lab. For more, see: Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020).
[20] Linda Hardesty, "FCC approves some Huawei rip and replace extensions, sends letter to Congress," *Fierce Wireless*, October 13, 2023, https://www.fiercewireless.com/wireless/fcc-approves-some-huawei-rip-and-replace-extensions-sends-letter-congress.
[21] Protecting Against National Security Threats to the Communications Supply Chain through the Equipment Authorization Program, 37 FCC Rcd 13493 (2022).
[22] David Shepardson, "FCC says it could boost authority over Huawei, ZTE equipment," *Reuters*, September 28, 2023, https://www.reuters.com/business/media-telecom/us-telecom-board-says-it-could-boost-authority-over-huawei-zte-equipment-2023-09-28/.
[23] Corrigan et al., "Banned in D.C."
[24] Ibid.
[25] Ibid.
[26] This includes the five Chinese companies identified in Section 889 (Huawei, ZTE, Hikvision, Dahua, and Hytera Communications). See: Corrigan et al., "Banned in D.C."
[27] In most cases, OEM relationships are not intended to deceive customers or mask the provenance of a particular product, but rather to create market synergies. For example, most of the personal computers sold by Dell use chips produced by Intel, graphics cards produced by NVIDIA, and software (Windows)

produced by Microsoft. In this case, Intel, NVIDIA, and Microsoft are all OEMs.
[28] Zack Whittaker, "US government agencies bought Chinese surveillance tech despite federal ban," TechCrunch, December 1, 2021, https://techcrunch.com/2021/12/01/federal-lorex-surveillance-ban/.
[29] For instance, the federal government engaged in a protracted legal battle with the Russian cybersecurity firm Kaspersky Lab after the Department of Homeland Security (DHS) banned the company's products from federal networks. Kaspersky alleged that DHS violated the company's constitutional rights by issuing a ban before giving it a chance to defend itself, among other things. The current FASC and OICTS processes attempt to avoid this issue, requiring policymakers to justify their actions against particular vendors and giving companies the chance to appeal. For more information on the Kaspersky ban, see: Joseph Marks, "DHS, Kaspersky Resume Court Battle Over Government Ban," Nextgov, February 6, 2018, https://www.nextgov.com/cybersecurity/2018/02/dhs-kaspersky-resume-court-battle-over-government-ban/145774/; Aaron Boyd, "U.S. Finalizes Rule Banning Kaspersky Products From Government Contracts," Nextgov, September 9, 2021, https://www.nextgov.com/cybersecurity/2019/09/us-finalizes-rule-banning-kaspersky-products-government-contracts/159742/.
[30] Hardesty, "FCC approves some Huawei rip and replace extensions, sends letter to Congress."
[31] "Sanctions Search List," Office of Foreign Assets Control, accessed October 2022, https://sanctionssearch.ofac.treas.gov/.

COMMISSIONER FRIEDBERG: Thank you very much, thank you for your excellent testimony. Ms. Nikakhtar, you really gave a very compact description, I think, of the problem. As you pointed out, the legal authorities exist to deal with it, you have argued that the capability exists to deal with it, but you said the will doesn't exist. And I'd like you to expand on that. What is the source of the obstacle? It seems that in the last five to ten years we have come to a recognition as a country of the magnitude of this problem, and yet all of you are describing a situation which very little has been done to deal with it.

MS. NIKAKHTAR: Yeah, thank you, I mean it is so frustrating knowing that we have the Information Communications Technology Services Executive Order come out in 2019, we are in 2024. We have done nothing. Agencies should not take that long to implement laws and develop regulations, CFIUS, FIRRMA, right? We got that up and running very quickly. We have IEEPA authority, right? It's broad, it's flexible, it can be used, that's been around since the 1970s, and yet we still don't use this.

To your question, though, we often hear industry advocates to -- they usually advocate for doing this in a nuanced way. Well, you've got to identify the companies first, you've got to identify the sectors, et cetera. It creates a whack-a-mole problem for the U.S. government when we are already out, we are already expending so many resources playing this whack-a-mole game with China and Russia and et cetera and et cetera.

So let's think about what is a more streamlined way, how would we effectively do this? I am an advocate of just -- and I will also sort of put my trade lawyer hat on and say that every time we have nuanced laws, the Chinese exploit them, they work around. So nuance doesn't work anymore. We have got to have concrete laws. IEEPA, ICTS, we ban Chinese components and software in our goods.

Okay, I can hear the argument about well, there is going to be compliance costs. This is nothing like -- I think it is astounding that the EPA feels so comfortable putting out environmental regulations. Of course, it increased compliance costs for everybody, but everybody does it, right? National security, compliance costs, that should be a given. Much like people complain -- relatively don't complain that much about environmental regulations, national security regulations, let's just move forward, not listen to the complaints, because it is fundamentally no different than the other regulatory bodies that impose burdens on companies.

The other point is that the economy, people will say well, the economic impact. The economy adjusts. Look at the Section 301 tariffs. We imposed tariffs on 350 plus billion dollars of goods, collecting revenue of 50 plus billion dollars a year, and in those first few years of the initial short-term shock, the upper end estimates of the economic impact is .25% of GDP. So my point is this, we can do it. I wouldn't listen to the -- we have the laws I mentioned, and I wouldn't listen to the cost headache, because it's a fraction and it's overstated.

COMMISSIONER FRIEDBERG: Okay, thank you. What about possible legal objections? I guess I would ask this to Mr. Corrigan, you suggested that one of the reasons why existing laws haven't been implemented fully is that there's concern over legal challenges. Could you say more about that?

MR. CORRIGAN: Yeah, 100%. So back in, I believe it was 2017, don't quote me on the year, DHS tried to ban Kaspersky Labs from federal networks, and it, Kaspersky, I think sued the government in two separate cases, and that just extended the process of getting rid of this technology for two to three, four years. So I think the folks that I have talked to within

Commerce, particularly, they seem -- it sounds like they are just dotting their I's and crossing their T's, they want to make sure they have all the authorities, and the processes and procedures are airtight enough that they could be implemented effectively.

I think that recently, like they conducted an investigation -- they started conducting an investigation into TikTok, and they found that TikTok sued, and there was some discrepancies over whether or not IEEPA authorities and some of the exceptions to those authorities would preclude Commerce from regulating TikTok, so I just think there's a lot of like, it's difficult to implement this stuff, and I think they're just trying to do their diligence before they do so.

COMMISSIONER FRIEDBERG: Okay, thank you very much.

COMMISSIONER HELBERG: Commissioner Glas?

COMMISSIONER GLAS: I just want to take a moment and thank all of you for your testimony. This obviously is a very hot and timely topic, with hearings on the Hill and a lot of discussions.

I am going to start with you, Mr. Tsarynny, a couple questions for you. In your testimony you noted that Chinese companies are required to share data, under their law, with the Chinese government on the data that they collect, and the risk to American consumers and our national security. Just yesterday in CNBC, there was an article about Meta's future, may be dependent on the growth of ecommerce websites like Shein and Temu, which this commission did a report last year related to those sites.

How do we manage this moving ahead, and what are the risks to American consumers by using these kinds of Chinese ecommerce websites? What are the risks to our national security, what's the kind of data you believe that some of these companies may be sharing with the Chinese government, and what is the liability?

MR. TSARYNNY: Thank you for your question. There is a lot of really important topics that you raised, I will try to address one by one. Firstly, why it is a risk is that information and then data that is collected about all of us, Americans and everyone else in the West, probably, is accessible to any government agent or any entity in China, and it has been used, or it has been reported to have been used for spying already.

Secondly, beyond just spying, calling it "just spying," it can be used, and probably I am speculating, is being used to train AI, and know more about us than we know about ourselves. And what can happen at one point is that they will know more about us than we know about themselves, and then they will always win, because just like a chess game.

Thirdly is what kind of information we have seen, and would information they can collect, and we have seen them collecting. It's everything, for example, online that you type into forms, that you see on a page, can be collected, and we've seen it being collected. So they know everything about you or all of us, maybe already today or sometime in the near future, they will know everything, and how that can be used against us, just like in the opening remark. I heard obviously about President Eisenhower's remark that the next war will not look like the previous war. And we might as well be already in the middle of a war which we don't realize it we are in the middle of a war, but in their eyes, we are their enemies, and they're already using that information against us.

COMMISSIONER GLAS: Thank you, I have a follow up for Nazak. I can sense your frustration having worked on these issues for the last 20 years or so, related to the fact that we have a lot of laws and mechanisms in place, and the either inability to enforce or the willingness to effectively enforce. And I was reading over your recommendations about our various laws related to the prohibition of certain high-risk Chinese hardware or software, and thinking about

the globalized supply chain, especially as the economy in China is transitioning, how difficult this would be to fully implement. I am also thinking about American consumers who are purchasing items that are internationally direct mail shipped through de minimis, where these items aren't inspected, how challenging this can be to really addressing the problems. Can you comment on that?

MS. NIKAKHTAR: Yeah, thanks, I mean I should say even items that are inspected, right, we are not doing the kind of inspection we need to, to make sure that they're not embedded, right, with hardware, software, interfacing threats. But I think one of the ways that makes sense to do this -- we can't pull the rug out from under us over night, and this problem has been in the making for years and years and years, and the Chinese are lying in wait. They have the laws that mandate that every company in China carry out orders of the CCP, do what's in the CCP's best interest, and there is a lot of sticks that the Chinese government has if companies don't comply.

So I want to touch on a worst case scenario to really underscore the fact that these threats are real and they exist. China has written about what cities to bomb in the United States, to wipe out how much of the population. They can easily turn off all the chips in our cars so we can't get away, turn out the power grid, contaminate the water, and have a captive population so they can bomb us, right? Like this is not unrealistic to think about.

But I also want to underscore that the government is stalling rather than dotting the I's, crossing the T's. And the best example of that, and I promise I will be quick, is the fact that everybody's really keen on sort of yelling about TikTok, but we don't even use the litigation proof legal authority that we have to put the ByteDance on the entity list, which will then atrophy the app over time. This is stalling, this is punting, because the government doesn't want to be the one responsible for causing, sort of economic harm. And the only way to mitigate that is phase-in restrictions. Do blanket restrictions, these sectors we can't have the Chinese components anywhere, and phase it in over time so the economy adjusts.

COMMISSIONER HELBERG: Thank you Commissioner Glas, I have a lot of questions, so in the interest of time, I kindly ask our witness to keep their responses to yes, no, or one sentence where appropriate.

According to Pew Research, 43% of TikTok users get their news from TikTok. Pro-Palestinian content has received more impressions and views on TikTok alone than the total number of views on all topics combined on the New York Times, USA Today, Fox News, The Guardian, The New York Post, The Washington Post, CNN, and The Wall Street Journal combined. Wouldn't you say it's time we started treating TikTok as a news platform in this country?

MS. NIKAKHTAR: Should we be treating it, you mean, was that the question?

COMMISSIONER HELBERG: Given the fact that a majority of Americans now get their news from TikTok, instead of viewing TikTok as a purely social media platform, wouldn't you think it's time for us to view TikTok and treat TikTok legally as a news platform?

MS. NIKAKHTAR: One thing, the news outlets also figure out what to cover because of what's trending on TikTok, which is terrifying. I think the only treatment TikTok deserves is an ultimate ban, I don't want to treat it as anything except prohibition. Thank you.

COMMISSIONER HELBERG: Would it have been the right decision to allow the Soviet Union to own NBC and CNN during the Cold War? Haven't we historically had restrictions on the foreign ownership of TV and news stations in this country? Because we know foreign dictators use media as propaganda to hurt us, and what's the difference between social media and

media? Isn't it a national security threat to allow our country's largest news platform to be manipulated and controlled by the Chinese Communist party?

MS. NIKAKHTAR: We shouldn't allow it, we should have the outright prohibition, and this is also I want to underscore where CFIUS is falling short. The approach that they take is unnecessary, it's a weaker approach, and we need to go in with a stronger hand. These are real threats.

COMMISSIONER HELBERG: And Ms. Nikakhtar, as an attorney, is perjury a felony punishable by time in prison, yes or no?

MS. NIKAKHTAR: Yes.

COMMISSIONER HELBERG: The CEO of TikTok said under oath that "American data has always been stored in Virginia and Singapore." A May 2023 Forbes investigation showed that substantial U.S. user data on TikTok has in fact been stored in China, including the financial information and social security numbers of U.S. based creators. Doesn't that sound like perjury to you?

MS. NIKAKHTAR: 100%.

COMMISSIONER HELBERG: Audio tapes obtained by Buzzfeed contain 14 statements from nine different TikTok employees indicating that engineers in China had routine access to U.S. user data between September of 2021 and January of 2022. Help me understand why that is not perjury?

MS. NIKAKHTAR: It is perjury. TikTok just knows that the U.S. government doesn't have the backbone to prosecute it, so it feels emboldened to continue with the misinformation.

COMMISSIONER HELBERG: In one tape discussing access to U.S. user data, a TikTok employee also referred to one Beijing based engineer as quote "a master admin" who quote "has access to everything." Seems to me like perjury, sounds like perjury, smells like perjury. Does this panel agree?

MS. NIKAKHTAR: Absolutely.

MR. TSARYNNY: Yes.

COMMISSIONER HELBERG: China has banned every American content platform in China and yet we give them unfettered access to our market. Our data goes in, their propaganda, our data goes out, and their propaganda comes in, which doesn't sound like a great deal for the American consumer. Does this panel support unanimously a ban of Chinese social media app companies in this country?

MS. NIKAKHTAR: Absolutely.

MR. TSARYNNY: Yes.

MR. CORRIGAN: With all due respect, Commissioner, this is outside of my area of expertise and I don't care to comment.

COMMISSIONER HELBERG: Does this panel agree that our reliance on Chinese supply chains makes our country vulnerable to the Chinese embedding back doors into our electronic products, and does the panel believe that the Congress should consider concrete steps to incentivize U.S. tech companies to re shore their supply chains outside of China?

MS. NIKAKHTAR: We only know the tip of the iceberg, and yes, the Congress needs to move, the Executive Branch needs to move.

MR. TSARYNNY: Yes. 100%, I agree.

MR. CORRIGAN: I agree the Executive Branch should look to re-shore technology supply chains.

COMMISSIONER HELBERG: Do you believe that tariffs should be part of the consideration for the solutions for the policy makes that Congress should consider?

MS. NIKAKHTAR: Tariffs are part of the solution, because it still allows the importation, but just at a higher cost, but yes, the threats are grave, every single tool in our tool chest should be taken out and used.

MR. TSARYNNY: Tariffs is outside of my area of expertise.

MR. CORRIGAN: They are also outside my area of expertise.

COMMISSIONER HELBERG: Thank you. Commissioner Price?

VICE CHAIR PRICE: Good morning and thank you all, your testimonies were very, very helpful. My colleagues have asked some of my questions, so I am going to go back to a few of them, but before I do that, Mr. Tsarynny, I hope I said that right, I need the remedial explanation, the remedial course about the pixels and TikTok and how it gathers information from people who don't have those apps on their computers, on their phones.

MR. TSARYNNY: Thank you for asking. What is a pixel? It is a term to a piece of code that is loaded by the page when you open your browser and you go to your doctor's appointment page to book an appointment, or you are buying something online, or logging into your bank account. And companies use pixels to advertise and understand if money is actually working properly for them, if the advertising campaigns are effective or not effective, and there are many other purposes for pixels.

What they specially do is they are loaded into the page and they have ability and they do observe what users do. Are you scrolling down through the page, are you clicking on any particular buttons, are you typing in your password to your email address, are you entering your credit card information, and so on. So they do see that information. Often they collect and send a copy of that information to themselves. So therefore they will know, or they know which websites you visited. If you use the same email address to log into two different websites, they now know which websites you visited. It is just a simple example, hopefully that was clear.

VICE CHAIR PRICE: I think the confusing part is how if you don't access it, how it comes to you anyway?

MR. TSARYNNY: Let me clarify that part. So pixels are running on websites, and they send information back to TikTok, or any other data blockers. Now, if you've never used TikTok app, they still track you on every one of those websites you visited that they have a pixel, and they know that you visited each of the websites, and you never have to use TikTok itself, because they now know your email address, maybe your first last name, your address, your IP address, and everything else around you as a digital entity, as a digital persona.

VICE CHAIR PRICE: And those websites that have those pixels hanging out, for lack of a better word, do those who administer those websites, are they aware? Do they get compensation because it's through ads, or does it just happen by itself?

MR. TSARYNNY: Sometimes they are aware, sometimes, and in most cases they are actually not aware, because those pixels are loaded by intent and are forgotten, they become like orphan pieces of technology that are always on and active, and sometimes they are loaded by an accident or by incident, or without website owner's knowledge.

VICE CHAIR PRICE: Thank you. And to everyone, I think that as we continue to have conversations about concerns over all of this technology and collecting all of this data, I think it is clear to most Americans why this matters on the security realm, but how would you address this so that they were concerned about what it means for their personal information? What is the impact of others having, or the Chinese Communist Party having this kind of information on

them? Like where they shop, and what kinds of things they buy, or what music they listen to, or what have you?

MS. NIKAKHTAR: So our adversaries have talked about years of that sort of information, warfare information campaign. It stems all the way from what children are exposed to, the kind of news we get. Most fundamentally what I see is sowing a lot of discord into the United States. If we are fighting within each other, and the laundry list of what we are fighting about keeps growing because they are infusing sort of inflammatory sentiment into our ecosystem, the more we let that happen, the more we are at each other's throats, and this is by design so that we don't form a united front against the common adversary.

MR. TSARYNNY: I completely agree with that statement, and what the information even collected on pixels can provide and has been providing is information of what do teenagers or anyone else are reading, which pages they follow and which pages they visit, that creates a lot of powerful insights and data about creating discord or other conflicts in our societies.

MR. CORRIGAN: I don't really have much to add; I think everything they have said I would agree with.

VICE CHAIR PRICE: Okay, thank you all.

COMMISSIONER HELBERG: Commissioner Schriver?

COMMISSIONER SCHRIVER: Thank you, and thank you to all our witnesses for your excellent statements and your contributions today.

If there's time, I have a quick question for each witness. Ms. Nikakhtar, nice to see you again, and thanks for your service. I want to follow up on a line of questioning of Professor Friedberg about the will, and you made an interesting observation, nobody cares about compliance costs when it's in the realm of environmental protection versus security, is it in fact sui generis? Is this the only area of compliance where we are sort of overly burdened by the thought of the cost that we are not taking action? It goes well beyond environmental, there is ADA compliance, all kinds, does this strike you as sui generis?

MS. NIKAKHTAR: I mean there is a lot of compliance, there's expert controls, right, sanctions, all that, so there's always sort of compliance, but it's just the FDA, is another example. There's areas where there's regulations and for like for human safety, and it is astounding to me how industry accepts it. They complain slightly about it, but they accept that this is a necessity to get to X, Y, and Z.

Juxtapose that in terms of national security, and it is astounding. And I think the industry does that because the narrative works, so they keep doing it. They know it doesn't work with the FDA, they know it doesn't work with customs very much, it doesn't work on the national security front, so we're emboldening industry with this narrative, and we don't have the capability to understand it, that there's nothing wrong with compliance costs if there's an endgame, and here it's national security.

COMMISSIONER SCHRIVER: Thank you, thank you. Mr. Tsarynny, I am going to paraphrase one of your recommendations. You said something to the effect that any entity that will store personal data should bear the responsibility of security and protection of that data. Given what we've already discussed about the relationship between the Party, government, and Chinese entities in China, is there any conceivable scenario that a Chinese entity could meet your standard of, we guarantee protection of this data?

MR. TSARYNNY: Thank you for the question. The kind of follow up question will be, what if there's clash of rules? Chinese law requires company to disclose that information --

COMMISSIONER SCHRIVER: That's exactly the point.

MR. TSARYNNY: And another law prevents it. Which one will prevail? And just hypothetical scenario, the CEO of company X is in Chinese office, and people from PLA come in and knock on the door, what will that CEO do or that engineer do? And I think that answer is pretty clear here.

COMMISSIONER SCHRIVER: Well that is the point I wanted to draw out, you are making a recommendation which in essence says, really the Chinese are not going to be able to meet the standard for Chinese entities.

MR. TSARYNNY: Exactly.

COMMISSIONER SCHRIVER: Thank you. Mr. Corrigan, again paraphrasing one of your recommendations, you said when it comes to procurement bans and other regulations, focus on particular critical sectors while not impinging or harming non-sensitive business areas, again paraphrasing. That conceptually makes sense, it is a bit of a goldilocks, you know the right entities, and protect the others, but can you give us a sense of what that would look like? What in your mind the critical sectors, and yeah.

MR. CORRIGAN: Sure. DHS has identified 16 critical infrastructure sectors, I think that would be a good place to start. I think that these determinations, I am an outsider looking in, I think that a lot of the regulatory entities would have a better understanding of specifically what the risks are in different situations, and I think that the determinations should be based on like the real risks that are being faced and the evidence that is out there for them.

I think that just, to kind of going back to some of the compliance costs and not presenting undue financial burdens, I can't speak as much to the private sector, but I know that with state and local governments for instance, like these are organizations that are vastly, vastly, resource constrained, and I would argue that they do think about security, they just have a limited budget with which they can approach those issues, and when they are figuring out how to allocate those resources, from the folks that I've talked to, a lot of them are pouring those into defending against like very pressing, immediate threats like ransomware. And while they are aware in some cases, not all cases, but in some cases, of the risks that foreign technology presents, to them those risks are fairly abstract, and I think that that is why you see them allocating the resources the way that they do.

And if I could just add one other point, I think that a low, like procurement bans, I think should be viewed as once policy lever that can be used to address some of these risks. We've seen Chinese actors access government networks, unauthorized, through U.S. made technologies as well, and I think that advocating for basic cyber hygiene, two factor authentication, strong passwords, that kind of thing, will also help to address the risks in a much lower cost way.

COMMISSIONER SCHRIVER: Thank you. I'd just say, if the risks are viewed as abstract that we need to do more of this type of hearing, and thank you to our co-chairs for doing this. Thank you.

COMMISSIONER HELBERG: Thank you Commissioner Schriver. Commissioner Wessel?

COMMISSIONER WESSEL: Thank you all for your testimony, for your long-term work, it's deeply appreciated. Look, we all know complex this is. We have been pushing for years in various ways, each of you has been pushing for years to try and enhance security, abate risks, et cetera, but you know we are still having this hearing today, and you know, there's a lot of action that needs to occur and this is sort of like trying to nail Jell-O to the wall in some ways.

You know, in thinking about what were the collection issues, and pixelated surveillance, and I am reminded of pixelated viruses, which hasn't been discussed for a while, we could go

into that today as well, but it seems to me that where the old line of capitalists will sell the rope to hang themselves. In looking at these issues for this hearing, it seems that we are also creating the problem ourselves, and by that I mean I looked at data brokers. So here we have, again, you talk about TikTok and the ability through pixels to collect information without knowledge. We have data brokers who are selling this data to the Chinese, and we also have now an entirely new threat vector that's rising, which is autonomous vehicles, which, you know, some liken to, you know, you are sitting inside an iPhone, where your eye movements, all the, whoever you're talking to, whatever you're collecting et cetera, or communicating with is being collected.

Help us understand what acts of commission we're engaged in, and Mr. Tsarynny I will turn to you first, because of your work on pixelated collection. Where do data brokers and the actual sale or just transmission of U.S. data, where does that come into this, healthcare or otherwise?

MR. TSARYNNY: Thank you for the question. You're correct, TikTok is one of the vendors, one of the ways data brokers, industry broadly, collects information, and yes --

COMMISSIONER WESSEL: But we have U.S. data brokers that are collecting tens of thousands of data points on each of us, and they are able to sell that to the Chinese or anyone, correct?

MR. TSARYNNY: That is correct, and also, like you said, we are creating our own problem. We are here because of the previous 20 years of keeping blind eyed on that issue, and waking up in today's world where we are all tracked, we are all surveyed through various data broker technologies. Some of them are owned by TikTok, the collection pixels, but many others are not TikTok, but other companies that we've seen. We've seen Kaspersky, we've seen other technologies on the Executive Order's ban list, being embedded into websites as well. So it is self, kind of, created problem, by ignoring it and not preventing it in the past. So my recommendation would be to act sooner rather than later.

COMMISSIONER WESSEL: And would a system -- and let me also say, I am speaking for myself, and not my colleagues. I am asking questions to gather data, not to impose anything on this Commission.

We, I think, appreciate the fact that most of our reports are unanimous and the recommendations usually reflect broad consensus. But we have, for example, I use a VPN and usually use, I don't know that I should divulge this, usually use European websites because then I know that I am going to be covered by GDPR, and so I get pop ups to be able to stop all of the collection of, other than pure analytic data, you know, anything else. What kind of system -- is there a systemic way that we can guard against what is happening with TikTok but also our own data brokers? Should we be treating data as a greater intelligence, military security, economic security asset, than we are today?

MR. TSARYNNY: I would say that there's two main parts to it. Part one is the technology part. Anything technology wise can be eventually solved; we have a lot of smart people that can solve it over time, sooner or later. The second part is accountability. When companies don't have consequences, they don't act. If they have a consequence, such as a hefty penalty, like under GDPR, or prison time, like under Sarbanes Oxley Act, CEOs, CFOs and others, they read the financial statements. That is why Enron didn't happen since Enron happened, because of the personal responsibilities executives carry.

COMMISSIONER WESSEL: Okay, I see my time has lapsed. I hope we, I think we have time for second round, so back to you.

COMMISSIONER HELBERG: And since Commissioner Cleveland just joined us, I want to give her the opportunity to speak.

All right, so we can move on to second round of questions. Does anyone have further questions, Commissioner Friedberg?

COMMISSIONER FRIEDBERG: Thank you very much. Mr. Tsarynny, I wanted to follow Commissioner Wessel's line of questioning and make sure that I understand what you are saying. Am I correct in understanding, first, that TikTok is not unique in the techniques that it's using or the kinds of data that it's collecting on Americans. Is that right?

MR. TSARYNNY: It is very similar to others. There is some uniqueness that we observed, is that it tends, it sometimes collect more information than other vendors or other data brokers do collect.

COMMISSIONER FRIEDBERG: So, but principally what seems to be different about it or concerning about it is the volume, you said, I don't know, 7.5%, I don't remember what the number was. Are there other companies or platforms that are in the same league in terms of the volume of information that they collect?

MR. TSARYNNY: Absolutely, yes. Other companies collect on even more websites. There's dominant players such as Alphabet, and Meta and others. The concern with TikTok or ByteDance specifically is that everything they collect is accessible to CCP and China.

COMMISSIONER FRIEDBERG: So it's more where it goes and who might exploit it at the other end than the fact that they're collecting it or the mechanism that they're using to collect?

MR. TSARYNNY: And the impact of that use of the data, yes.

COMMISSIONER FRIEDBERG: Right. And further, if I understand correctly, what they're doing is not illegal under current laws. Is that right?

MR. TSARYNNY: Mostly -- that's why I am pausing, it's like every industry has different regulations. Mostly it is legal and often companies, from our experience, when we are speaking with an organization that has to comply with HIPAA, they tell me and us, tell us if we have an analytics tool or if you have pixel on any of these pages, we have to get rid of them. So they are paying a lot of attention. And other industries are almost ignorant, they are not paying attention to that issue at all.

COMMISSIONER FRIEDBERG: But if tomorrow we wanted to get rid of this, it would have to either be through blanket regulations that would prohibit the collection of this kind of information, or specifically targeted at a company like TikTok, because it is linked to a country of concern?

MR. TSARYNNY: I think there are two very related issues, but they are separate. One is general information privacy, and that applies to blanket, all data brokers, and the second one is information security when it comes to espionage and foreign parties, that, like for example, the TikTok example.

COMMISSIONER FRIEDBERG: The collection of information, for example, you mentioned passwords or bank account numbers, regardless of who is doing it, whether it's TikTok or another company, that is not illegal?

MR. TSARYNNY: Depending on the industry, and depending on which law or which jurisdiction company operates in. For example, in the U.S., I think 17 states brought out their own privacy regulations because there's no single blanket privacy regulations, and sometimes it is illegal, sometimes it is legal, and sometimes organizations are not even aware of what is happening, that their information is being collected without their permission.

COMMISSIONER FRIEDBERG: One last question on this to make sure I understand. You said that there are things that TikTok is doing that are different than others. Can you say a little more about that?

MR. TSARYNNY: Yes, what we have seen is, for example, not to put Meta on the spot, I will just compare the two. Meta or a company like that will collect information related to marketing campaigns, broadly, did you see the ad, and did you visit the page? What we've seen TikTok do is do the same, plus also send a copy of everything that is presented to you on a page, including whatever companies that you're, whatever page is displaying, maybe it is your sensitive information, could be your purchasing history, could be your transactions, or anything else, and they send that copy back to themselves.

COMMISSIONER FRIEDBERG: Okay, time is short, but I wanted to ask another question about hardware, and this goes to Mr. Corrigan and Ms. Nikakhtar. The obstacles to making the kinds of changes that you've described, we talked about cost, we talked about possible legal obstacles, but it does seem that there's another, which I guess is related to cost, and that's simply alternative sources of supply, the lack of capacity to produce the things that are now being purchased in such volumes from China. Is that correct, I mean how big a part of the problem is this, Mr. Corrigan?

MR. CORRIGAN: I think that's a huge part of the problem. I think that's why the costs are so high, is when you don't have an alternative source that's within, you know, 50% of the price, that's where the cost comes from.

COMMISSIONER FRIEDBERG: So we are just not making a lot of this stuff?

MR. CORRIGAN: Yeah, yeah, and I think that is, again a bit outside of my area of expertise, but I think that it varies a lot when you look at different product categories. So I, in some of the research that I've done, looked specifically at Hikvision and Dahua security cameras, and there is nothing within at comparable performance within the same price range.

COMMISSIONER FRIEDBERG: Okay, thank you.

MS. NIKAKHTAR: May I just quickly add that this is a chicken or egg problem. The more we allow the Chinese goods in the United States, the less we are -- we are preventing innovations, right? We are preventing companies from getting into the marketplace. So that's part of the problem.

And I also just very quickly on the data transfer, the legal aspect of it, everybody knows export control laws extends to goods, software, and technology. Data doesn't have legs, it doesn't just walk, it is transferred through software, so we can actually use export controls to prevent the export of sensitive information, and privacy laws are all mainly consent based, and so people don't know what they're consenting to. The average -- that's why it depends on the lawmakers to protect them. And so I am not a fan of consent based national security measures, we should be using export controls. Thank you.

COMMISSIONER FRIEDBERG: Thank you.

COMMISSIONER HELBERG: Thank you. Commissioner Cleveland, did you have something to share?

ACTING CHAIRMAN CLEVELAND: Thank you. Now that I've recovered from traffic, I gathered Commissioner Price asked about the pixel tracker, but I'd like to follow up I could just to understand it a little better. I gather it is something that is embedded on a webpage, email, or an ad. Could you explain the process of how TikTok would have access to a non TikTok platform? That's the piece that I'm lost on.

MR. TSARYNNY: So how TikTok gets onto the websites. Here's an example. Company X wants to buy advertising campaign on TikTok, they pay money to TikTok, and TikTok and company like them tells Company X, you will install this little pixel, and that will track effectiveness of the marketing campaign or advertising campaign, to tell you if actually your dollars made are worth the spend. The company installs that pixel and that pixel usually remains on the website for way beyond the end of the campaign, and because it's still there, it still collects all of that information that is accessible -- that it has access to.

So that's how pixels usually get through a legitimate way, and we often have seen where it gets there by accident, or through other unintended consequences such as, somebody loads a tool called a tag manager that loads many, many other tools, and that's a dynamic nature of the websites we all use today, is that they're not coded by the developers, they are almost like assembled in real time from pieces of code that are loaded from any country in the world, so from multiple countries, and that's the reality of the internet we live in today. It is not coded or prepared, it's loaded dynamically at the moment you load the page into your browser.

ACTING CHAIRMAN CLEVELAND: Okay. My experience in marketing is virtually every company does the same thing, but as you point out, it is where it is going in the end.

MR. TSARYNNY: Yes, yes.

ACTING CHAIRMAN CLEVELAND: Which raises -- the Commission has looked at Temu and Shein in terms of the way they approach the American market, and so I am curious whether or not you've looked at other large marketing platforms that sell products, other than TikTok, because I think TikTok's the problem of the day, but I think there are other ones on the horizon. So I'd be interested in all of your perspectives on -- while we are obsessed with TikTok and what it does or doesn't do, what other companies do you see as emerging as similar kinds of risks?

MR. TSARYNNY: Outside of national security risks, broadly data security, data privacy risks, this is public information, Google or Alphabet's technologies, Meta's or Facebook technologies, are the top two, amongst with Microsoft Bing, and other advertising platforms. I can add there's Snapchat, there's Adobe Cloud or Adobe marketing technologies are also very popular and very common. That is the norm, this is how internet works today. Do they collect a lot of information? Absolutely, they do collect a lot of information, and do they collect more information in the U.S. or of Americans than for example, of when you compare to Europe? Yes, they do collect more information on Americans than in Europe, because Europe has more stricter regulations and laws around it.

ACTING CHAIRMAN CLEVELAND: Well, the United States is also a bigger market, so that makes sense. But I think I was interested in Chinese companies that are potentially the same kind of -- they provide a consumer product, like TikTok does. Have you looked at any other company, or have any of you looked at other companies that present similar data risks in terms of the U.S. consumer?

MR. TSARYNNY: Yes, we've seen other companies that are Chinese or are associated with China. TikTok specifically just the giant amongst them in terms of the volume of data they collect, but yes, other also companies are also present.

ACTING CHAIRMAN CLEVELAND: And what might those other companies be?

MR. TSARYNNY: To be honest, the names are escaping me, specific brand names are pretty hard to pronounce and remember them.

ACTING CHAIRMAN CLEVELAND: Perhaps you can provide it for the record. Yes, that would be helpful.

MR. TSARYNNY: Yes.

MS. NIKAKHTAR: May I add also --

ACTING CHAIRMAN CLEVELAND: We're behind the curve on TikTok, right? It had massively infiltrated the, whatever age, demographic, and market, and so it's a question of closing the barn door after the horse is out, as it were. I'm just curious what's on the horizon in terms of the next company that's a problem.

MS. NIKAKHTAR: May I just add that, so it's the apps. It's the photo editing apps, right? It's the video games app. Every time I see them on somebody's phone I look up the ownership. It's the clothing app marketing. But let me say, it goes beyond what those apps do. Those apps can actually drop code into your phone, and that code can then extend to all of the activities of your phone, your microphone, your camera. And it's in your phone, and that code can also transfer malicious additional code beyond your phone into the router into your home, and then that router connects to the telecom infrastructure and it spreads. So just by one app being able to drop code in your phone, the malicious code can spread across the systems like cancer.

ACTING CHAIRMAN CLEVELAND: And who's assessed the risk? That's very, very helpful, that sort of chain of, or sequence of events. Who's assessed the risks of say the top 10 Chinese companies that are engaged in this kind of marketing and then obviously respond to the CCP's guidance? Has anybody looked at?

MS. NIKAKHTAR: I would also flag Alipay. You go into --

ACTING CHAIRMAN CLEVELAND: Every CVS --

MS. MIKAKHTAR: Right? I mean that's a problem, and you have that app on your phone, and it works beyond a payment app, right, with all of the other threats that I mentioned, so it's certainly these dominant ones, but man, they're the little ones too, Alipay, that's another one to look at.

MR. TSARYNNY: And I can add a few companies' names, actually I realized I have some of them. Tencent, Alibaba, Alipay obviously, CapCut, Lark, News Republic, Riot Games, WeChat, Tencent Cloud, PUBG Mobile, and there's many, many other apps that are doing that.

ACTING CHAIRMAN CLEVELAND: When we looked at Alipay two years ago, and we did a paper on this, at the time the Administration assessed that it was a problem largely contained to Chinese citizens that were here studying, traveling, and therefore using Alipay, because like you, I had that reaction when I walked into CVS. Has it changed, do you think, in terms of who's actually using Alipay? Or any of these other, all the ones you just listed, I don't think of having access to the American market the way TikTok does.

MS. NIKAKHTAR: I'll also say from a legal standpoint, and I haven't done the forensics to see if it's happening, but of course one would say of course it is one CCP mandates, the laws that we know about, but there's no legal prohibitions. So if there's no legal prohibitions, and China has the desire, the motivations, and laws to command its companies to do that, let's just make our lives easier, assume that it's happening and get on with it and try addressing the problem through solutions.

COMMISSIONER HELBERG: Thank you for those excellent comments. I have a follow up question for our witnesses. Isn't it true that ByteDance has an internal CCP committee, and isn't it also true that the TikTok CEO reports to the ByteDance CEO, and therefore is also accountable to that ByteDance CCP committee?

MS. NIKAKHTAR: Yes.

COMMISSIONER HELBERG: Is there a single other large social media platform in this country that's internally governed by a CCP committee?

MR. NIKAKHTAR: WeChat is going to be certainly one them, Alibaba, Alipay is certainly one of them. In fact, any company that is of any relevance to the CCP is going to have CCP board members, that is part of the Chinese laws. It's a mandate.

COMMISSIONER HELBERG: And is the ByteDance CCP Committee there to maximize shareholder value, or do you think it is there to advance the CCP's political objectives?

MS. NIKAKHTAR: 100% without question the CCP's objectives. The CCP does not care about money, it cares about power and influence.

COMMISSIONER HELBERG: So there is a substantive difference between the corporate incentives at American tech companies like Alphabet, Snapchat, and the like, and Chinese companies, which have a dual mandate to also advance the CCP's political objectives?

MS. NIKAKHTAR: America's motivation is money, China's motivation is to infiltrate and then cripple our systems and gain the upper hand, without question.

COMMISSIONER HELBERG: And do you think the CCP Committee is instructing the executive management of TikTok to make sure that it's fully compliant with the unfair and deceptive practices clause of the FTC Act?

MS. NIKAKHTAR: Absolutely. And I should also say that they know that they're insulated in large part from legal recourse. One, we don't have the will to do much about it, but two, if the Chinese individuals are there, they know that we can't bring them to justice here.

COMMISSIONER HELBERG: Some of you said earlier, that, Mr. Tsarynny, I think it was you that mentioned earlier that there's a contradiction in our laws, and the expectations that we have on personal privacy and free speech with the laws of the Chinese Communist Party, the expectations that they have on the extraterritorial applications of their censorship norms as well as their surveillance norms.

Can you elaborate a little bit more on that and could you walk us through a potential scenario if you are a TikTok operating in the U.S. but accountable to a foreign government? And Ms. Nikakhtar, I'd love to hear your thoughts as well, and Mr. Corrigan, if you have thoughts, feel free to weigh in.

MR. TSARYNNY: So thank you for the question. I will share from personal experience first. I was born in a Communist country. I grew up in Soviet Union, I remember what it was like under Communism. My family tried to escape and finally escaped. So from my personal experience, I will tell you that in a Communist country, no laws make difference, except for what the Communist boss wants to get done.

And under that premise, I am now going to suggest or speculate that in a scenario where a CEO of ByteDance or of TikTok is in a room with the CCP officials, and they want that person to do whatever they want, what the CEO will comply with, does he or she have a choice? So and I believe no, they don't have a choice, they will comply with the Chinese law.

COMMISSIONER HELBERG: Thank you.

MS. NIKAKHTAR: And I will add, to the earlier question about sort of profitability. I mean, the Chinese government owns the Radisson hotel chain, okay? It's publicly available. Do we think for a second that the CCP is interested in hotel profitability, or is this sort of another surveillance capability?

But China has the corporate credit rating system, which is the like social credit rating system. Corporations cannot function in China, much like the rest of world, but there's more

hurdles for corporations, without the government's approval for X, Y, and Z. And in China it's extensive.

Even if the Chinese government doesn't go to a corporation and say I need you to behave in line with these goals, when it's the corporation's time to come in and ask for something, they're going to look at what have you done for the CCP, what have you done in the CCP's best interest? That is an enormous coercive tool, when the company knows that it can't get certain licenses, permits, et cetera, from the government if it doesn't comply in any respect to advance the CCP's agenda, of course it's going to engage in nefarious behavior. That's what's expected, companies know what's expected, even if the CCP doesn't directly tell them, do X, they know they have to if they want permits, et cetera.

COMMISSIONER HELBERG: Mr. Corrigan, anything to add?

MR. CORRIGAN: Nothing to add.

COMMISSIONER HELBERG: Would you say that it would be accurate to characterize that effectively the claim by the TikTok CEO with Project Texas amounts to him trying to describe that he created a one company, two systems approach with Project Texas, and do we -- should our policy makers have any more faith in the one company, two systems model he is professing to have created than the one country, two systems model that epically failed in China?

MS. NIKAKHTAR: You know something fun that would be worth doing that you just flagged? The U.S. government has the Defense Production Act Survey Authority, right, it's compulsory. It would be kind of fun if the U.S. government decided to issue that survey to TikTok and ask all of these sort of, like if I'm going to believe you on your Texas Project, what are all of the things you're doing? Get the responses, and then follow up by doing audits, because if the responses are compulsory, the government can go audit whether the responses are true, and the government should take some forensic auditors, and I think it would be really fun to see what the government finds, and of course we're going to find a lot of violations with the U.S. law, which then means you're not going to comply with other prohibitions that we're putting on you.

But that's another instance where the government actually has the legal authority to assess safety of a high-risk actor that's already operating in the United States. Nobody's decided to do it; we're still waiting for somebody to step up and take action. But yes, they have the authority, and I think it would be fun actually to exercise it in the way that your question was getting at, and I had just mentioned.

COMMISSIONER HELBERG: Thank you. Any further questions? Commissioner Price?

VICE CHAIR PRICE: Hi, I just have one other question for Mr. Corrigan. Going back to some of your recommendations, which are very helpful, one of them, number two, is fully fund Rip and Replace programs. How much money are we talking about?

MR. CORRIGAN: So the Rip and Replace program, which initially focused simply on replacing Huawei and ZTE equipment in commercial networks, was funded at 1.9 billion dollars. The initial wave of applications for Rip and Replace funding was around five billion, and this was after they reviewed everything. The ones that got approved was five billion. So that's a 3.1 billion dollar budget shortfall for the first round of applications for two companies.

If procurement bans were expanded and the government was going to use the Rip and Replace program to help offset those costs, as I think that they should, we would be talking in the order of at least tens of billions of dollars to do so.

VICE CHAIR PRICE: I have one more question. And your third one was to target procurement bans in high risk sectors. How would you triage where to start?

MR. CORRIGAN: That's a great question. Again, this is a bit outside of my area of expertise. We have a lot of great people who work in the national security apparatus who would be able to figure that out. I would say that it's probably somewhere between a local government parks department and like a nuclear power plant, and I think it's really context dependent. I think it depends on what the specific technology is, the kinds of capabilities that it would offer bad actors who were able to breach it and access the networks of wherever it's deployed, and I think that those are determinations that need to be made by the regulators that oversee these entities.

And right now the way that the ICTS authority is set up, there is a wide range of variables that can be taken into account when they are making a determination. These orders that they can issue can be as targeted or as broad as they see fit, and same with the Federal Acquisition Security Council when they're looking federal networks.

And there's one thing that I would add. I do think -- I don't mean to come off as saying that procurement bans aren't warranted, I think that they are warranted in these situations, I just think that when we are doing so we need to be thinking about the impact that it will have on the organization that needs to comply. And in some cases, I mean there's going to be compliance costs everywhere, in some cases those costs are going to be very warranted, and I think that those are the areas where we want to be targeting and where we want to have potentially federal funding coming in to make up any of that gap. But if you add a situation where, say, you have a public transit authority, and in complying with a procurement ban they are going to have to shut down 50% of their bus lines, their rail lines, like that's a really large cost. They can comply with it, but there's going to be massive cost to them and the users of that service, and I think in those cases you want to see some government stepping in. I hope that answers your question.

COMMISSIONER WESSEL: Thank you, and you know, I think we probably have hours of questions, so you may be expecting some written questions after, and I hope that you'll be able to help us. I share the concern about TikTok, I mean the volume of collection and the CCP authorities written, unwritten, persuasive as they are, you know, to me, it creates a real risk vector.

But I think we have to look at this in two ways, one, what is the platform risk? And TikTok poses an enormous platform risk. Mr. Tsarynny, you talked about again, pixelated interception, I mentioned pixelated viruses, you know, we have the Car Whisperer platform that can listen in on any Bluetooth conversation. And a high gain Bluetooth antenna works for a mile, not just 30 feet, so there are so many opportunities and vectors and attack surfaces, et cetera, to collect data. Shouldn't we also be looking at whether there are kinds of data that should not be subject to mass collection? Or should be anonymized? Geolocation data, for example, which, you know, when you have a security clearance, you can't wear a FitBit into a secure location because that data can be collected and then they can determine, you know, where you live and follow you, et cetera, et cetera.

So, should we be looking at this from two angles? One, what are the platforms for collection, but two, what kind of data gives us the biggest concern? And how can that data be aggregated to create profiles and risks? Risks, in a very real sense, in terms of intelligence gathering, in terms of, Ms. Nikakhtar, as you pointed out about water systems, all the various things, it seems we have an incomplete matrix now. We're playing catch up, and we're not doing it very well.

This Commission four years ago identified LOGINK as an example of a CCP sponsored platform being used in ports around the globe that collects all data on ship cargos, and 90% of U.S. military cargo travels on commercial ships. It seems to me, and again, I want to stop

TikTok's collection, but I don't think that is success, I think success is much broader. Any comments from the panelists?

MR. TSARYNNY: Thank you, yes, definitely. Like you mentioned, there's a couple of issues; they are kind of layered type of issues. One is, what kind of information is collected or should be collectable or uncollectable or prohibited from being collected? Second, what is that information should it be collected used for? What's the impact, and then what's the likelihood that it's going to be used for that impact, what kind of harm can it cause us? And the third is actually, should there be any kind of rules to govern the first two, that actually controls and ensuring that those rules are followed? No rules are useful unless they are followed, or no regulation is useful unless it is really followed.

So to answer the first one, yes, a lot of information is collected, and you can call it broadly -- the way data brokers or any other companies look at it, they want to collect as much as possible to monetize it for commercial purposes and then for some cases it can be used for espionage. What can it be used for? Like you mentioned, the cameras in the ports tracking the cargo. Now the cameras, like in a school district or out on the streets they can track personnel, they know where everyone is at any point in time, so if somebody wants to strike, to find the best time to strike, they can find it, because they know where the least personnel is present.

The third point is, there's really at this time very little accountability, very little to no accountability, most jurisdictions or most aspects of data collection.

MS. NIKAKHTAR: Commissioner Wessel, may I also add that, you know, if anybody's been a victim of the OPM breach, I have zero faith in the government's ability to keep our information secure, and sort of Clear screening at the airport now, the information at the Social Security Administration, the Department of Motor Vehicles, et cetera. The government systems have a lot of Chinese hardware and software in it, and our government can't even safeguard our information.

And then, you know, genetics has been covered a lot, but the other thing I wanted to mention is just demographic information. If the Chinese, for example, get information from a sporting goods store, they'll know the amount, likely the number of children in that population by how many kid's bikes and kid's t shirts and stuff. We don't want the CCP to have that kind of information. It could target attacks based on demographic information.

COMMISSIONER WESSEL: Mr. Corrigan?

MR. TSARYNNY: May I add one more point?

COMMISSIONER HELBERG: Go ahead.

MR. TSARYNNY: One point to add is, like you mentioned, discord, in creating discord. We have seen information being collected about health conditions, miscarriages, abortion information, and so on, which is very sensitive and can be used to create discord.

COMMISSIONER WESSEL: I think that all bleeds into our next panel as well as we look at AI and large language models et cetera. So, my time has elapsed, I think, the panel. I will turn it back to the Chair.

COMMISSIONER HELBERG: Thank you. Thank you to our witnesses for the excellent testimonies today. We're at time, so we are now going to go ahead and break for 10 minutes, and then we will resume with panel two.

(Whereupon, the above entitled matter went off the record at 11:11 a.m. and resumed at 11:26 a.m.)

PANEL II INTRODUCTION BY COMMISSIONER MICHAEL R. WESSEL

COMMISSIONER WESSEL: Thank you. Our second panel will address the military applications of China's significant investments in artificial intelligence and quantum science. Breakthroughs in these fields could potentially lead to a paradigm shift in the way war is wa—, with wide-reaching ramifications for the regional and global balance of power. We'll start with Jacob Stokes, senior fellow for the Indo-Pacific security program at the Center for a New American Security. Mr. Stokes previously served in the White House in the national security staff of then-Vice President Joe Biden, where he was senior advisor to the national security advisor, as well as acting special advisor to the vice president for Asia policy. He will provide testimony on the battlefield applications AI, as well as the broader geo-strategic implications of AI development for U.S-China strategic competition. This is Mr. Stokes first time testifying before the Commission.

Next, we'll hear from Mr. Nathan Beauchamp-Mustafaga, policy researcher at the RAND Corporation. Prior to joining RAND, Mr. Beauchamp-Mustafaga was the editor of China Brief at The Jamestown Foundation. He will examine China's efforts to leverage large language models (LLMs) in its approach to cognitive warfare, particularly for the purpose of manipulating information flows on social media. This is Mr. Beauchamp-Mustafaga's first time testifying before the Commission.

Then we'll hear from Dr. Edward Parker, is a physical scientist at RAND, where his current research focuses on emerging quantum technologies, AI, and cybersecurity. Prior to joining RAND, Dr. Parker received his Ph.D. in theoretical solid-state physics at the University of California, Santa Barbara. His testimony will address China's aspirations to integrate quantum technologies into its military and draw comparisons between the U.S. and Chinese quantum industrial bases. This is also Dr. Parker's first time testifying before the Commission.

Thank you all very much for your testimony. I would like to remind all our witnesses to please keep their remarks to seven minutes to preserve time for questions and answers.

Mr. Jacob Stokes, we'll begin with you, but I do want to just quickly comment, as with our last panel, we're learning a lot. If, Dr. Parker, you can describe for me quickly later on – quantum physics – I'd appreciate it. I attend a full disrupted technology course up at MIT for three days and still don't know. So, I appreciate it. Mr. Stokes.

OPENING STATEMENT OF JACOB STOKES, SENIOR FELLOW, CENTER FOR A NEW AMERICAN SECURITY

MR. STOKES: Well, good morning. Thank you, Chairman Wessel, Chairman Helberg, and the Commissioners for inviting me to provide testimony on this critical topic. It's a special honor for me as a former member of the Commission's staff.

My presentation will assess China's progress in developing and fielding military artificial intelligence within the People's Liberation Army. I'll focus on applications related to uncrewed autonomous systems and battlefield functions and support. I'll also talk about implications for the military and security aspects of U.S.-China strategic competition.

At the broadest level, China takes an expansive view of military AI's potential to help the PLA become a world class military by mid-century, if not sooner. Beijing considers military AI to be an essential component of its campaign to reach the level of military technological development it calls intelligentization where AI and other emerging technologies supercharge the PLA's combat power. In October 2022, General Secretary Xi Jinping called on the PLA to, quote, speed up the development of unmanned intelligent combat capabilities, unquote.

Beijing's efforts could be bolstered by its military-civil fusion program which allows the PLA to harness commercial sector technologies for military uses. With regard to implementation in the PLA, Beijing is engaged in extensive military AI research, development, and experimentation. But so far, open source information about the PLA actually fielding military AI systems at scale remains fairly sparse.

On uncrewed autonomous systems, often referred to as drones, China has a large and sophisticated drone industry for both the civilian and military sectors. But those systems appear to possess only partial forms of autonomy and cannot yet execute the most advanced types of autonomy that would be enabled by artificial intelligence. In other words, they still rely heavily on human operators.

As the Department of Defense's 2023 China Military Power Report says, the PLA is, quote, pursuing greater autonomy, unquote, across a range of uncrewed systems for various battlefield purposes. Regarding AI in the PLA's battlefield functions and support, China is likely already -- China likely already uses AI for some cyber applications where the technology is mature as well as some intelligence, surveillance, and reconnaissance or ISR tasks that already have high levels of automation. The next stage for AI implementation in the PLA in this part of the PLA will likely be adopting the technology for low-risk uses like logistics, maintenance, and training, particularly when similar commercial AI systems exist and can be easily adapted for those purposes.

Eventually the PLA could implement AI into more of its decision-making and command and control functions to move towards what Chinese analysts call a "command brain" where machines and humans are seamlessly integrated. Those applications would necessarily start more at the tactical level where the tasks are more formulaic and only move up to handle more complex tasks at the operational and strategic levels later on. It's important to note, though, that China could fall short of its military AI ambitions for multiple reasons.

These include technological shortfalls, a lack of trained personnel, bureaucratic competition, rampant corruption, the CCP's need for tight control, and even a lack of funding as PLA priorities compete -- or PLA priorities in other areas compete for resources. To be clear, none of these obstacles mean Washington can be complacent. Far from it.

But they should remind us that effectively developing and fielding cutting-edge military technology takes much more than grand plans, even for China. That said, if Beijing manages to overcome those obstacles, military AI systems could pose risk to the United States across several categories. I'll highlight four.

The first is potential shifts in the military balance of power as small improvements add up. And later on, if China achieves fundamental breakthroughs in military AI that give it an advantage over the United States. The second risk relates to uncrewed autonomous systems that might have new capabilities or which Beijing might see as more acceptable to use because they don't risk human operators directly.

The third area of risk is in command, control, and communications, or C3, both through improved C3 for the PLA itself and then conversely the use of AI to degrade U.S. and allied C3. The fourth area of risk relates to nuclear weapons. If AI capabilities enable new nuclear tracking or counterforce options, or if states integrate AI into their nuclear complexes in dangerous ways.

So those are the risks. I'll go ahead and conclude with five recommendations for U.S. policymakers as they respond to China's pursuit of military artificial intelligence. They are, first, take bold action to constrain China's progress in AI for military and repressive purposes. But do so in a relatively narrow way that avoids self-defeating steps.

Two, build U.S. military AI capabilities to stay on the cutting edge. A key part of which will be robust testing and evaluation to make sure military AI systems are safe, reliable, and effective. Third, continue to shape global rules, norms, and institutions around the deployment and use of military AI.

And I would note here that China is already actively trying to shape the rules here and proposed a global AI governance initiative last October. Fourth, the U.S. should engage with China in a clear-eyed way on military AI risks. And then fifth and finally, the U.S. should prioritize intelligence gathering and analysis on as well as a net assessment of China's military AI capabilities, which as I said are evolving quite quickly. So I'll wrap it up there. Thank you for your attention, and I look forward to your questions.

COMMISSIONER WESSEL: Thank you. Please.

PREPARED STATEMENT OF JACOB STOKES, SENIOR FELLOW, CENTER FOR A NEW AMERICAN SECURITY

FEBRUARY 1, 2024

TESTIMONY BEFORE THE U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Hearing on Current and Emerging Technologies in U.S.-China
Economic and National Security Competition

Military Artificial Intelligence, the People's Liberation Army, and U.S.-China Strategic Competition

BY

Jacob Stokes

Senior Fellow, Indo-Pacific Security Program
Center for a New American Security

I. Introduction

Thank you Co-Chair Wessel, Co-Chair Helberg, and the Commissioners for inviting me to provide written and oral testimony on this critical topic.[1] My comments draw on my own research as well as technical insights from my colleagues in CNAS's Artificial Intelligence (AI) Safety and Stability Project (although the policy views are solely mine). It should be noted up front that this field poses special analytical challenges: it is mostly intangible, the technology is complex and evolving rapidly, and China's applications of AI in a military context are still shrouded in secrecy.

My testimony covers China's military applications of AI, as well as the broader geostrategic implications of AI development for U.S.-China major power competition. It starts by examining the role of AI in China's overall military modernization plans. Then, it explores AI implementation to date in China's military, the People's Liberation Army (PLA). Next, my testimony considers obstacles that could block the PLA from reaching its military AI ambitions and explores some of the risks that military AI could pose in the U.S.-China security relationship. Finally, my testimony assesses U.S. responses to date and offers recommendations for American policymakers.

II. The Role of AI in China's Overall Military Modernization

China sees AI playing a central role in advancing its military power. Chinese Communist Party (CCP) General Secretary Xi Jinping has set ambitious goals for the PLA to "basically complete" its modernization by 2035 and transform into a "world-class" military by the middle of the century.[2] In March 2023, Xi called on the PLA to "raise the presence of combat forces in new domains and of new qualities."[3] As part of those goals, Xi wants the PLA to continue to move through stages of military-technological development, from *mechanization* to *informatization* and ultimately *intelligentization*. Broadly, mechanization refers to fielding modern platforms and equipment; informatization refers to linking those systems to networks such as GPS; and intelligentization refers to integrating artificial intelligence, quantum computing, big data, and other emerging technologies into the joint force.[4] In 2020, China set a new goal to "accelerate the integrated development of mechanization, informatization, and intelligentization" by 2027.[5] In other words, Beijing aims to make progress on all three stages simultaneously rather than sequentially.

[1] This testimony is partly adapted from my CNAS report on the topic: Jacob Stokes and Alexander Sullivan with Noah Greene, *U.S.-China Competition and Military AI: How Washington Can Manage Strategic Risks amid Rivalry with Beijing* (Center for a New American Security, July 2023), https://www.cnas.org/publications/reports/u-s-china-competition-and-military-ai.

[2] Xi Jinping, *Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era: Report to the 19th National Congress of the Chinese Communist Party* (October 18, 2017), as reposted by *China Daily*, https://www.chinadaily.com.cn/china/19thcpcnationalcongress/2017-11/04/content_34115212.htm.

[3] "China's Xi calls for 'more quickly elevating' armed forces," The Associated Press, March 9, 2023, https://apnews.com/article/china-us-military-taiwan-xi-jinping-14f9c3d8fef26779f017d927aa352eeb.

[4] Kevin Pollpeter and Amanda Kerrigan, *The PLA and Intelligent Warfare: A Preliminary Analysis* (CNA, October 2021), https://www.cna.org/archive/CNA_Files/pdf/the-pla-and-intelligent-warfare-a-preliminary-analysis.pdf.

[5] Central Committee of the Communist Party of China, *Communiqué of the Fifth Plenary Session of the 19th Central Committee of the Communist Party of China* (November 17, 2021), as translated by the China Aerospace Studies Institute, https://www.airuniversity.af.edu/CASI/In-Their-Own-Words/Article-Display/Article/2834176/itow-communiqu-of-the-fifth-plenary-session-of-the-19th-central-committee-of-th/. For a useful discussion of other semi-authoritative Chinese sources explaining this new goal, see Zichen Wang, "Once-in-a-generation change in PLA guidelines: intelligentization added, mechanization declared 'basically accomplished,'" *Pekingnology* (blog) on Substack, December 8, 2020, https://www.pekingnology.com/p/once-in-a-generation-change-in-pla.

Beijing sees progressing through these stages as necessary to keep pace with changes in the technological character of warfare in the 21st century. Chinese scholars speak about the ongoing revolution in military affairs as one of weapons "systems confrontation" requiring "systems destruction warfare" to win.[6] To compete in this emerging era of conflict, the PLA is developing an overarching concept it calls "multidomain precision warfare."[7] In layman's terms, this concept posits that the very networking that gives the U.S. military its power creates interdependencies between its forces, which are also vulnerabilities that can be exploited. Thus, rather than needing to destroy U.S. enemy forces directly—ship-to-ship or tank-to-tank—China can attack the weak points linking U.S. systems and domains together and thereby neutralize or overwhelm U.S. advantages. Those weak points can include internet, satellite, or electromagnetic communications links as well as logistical supply systems.

AI is a critical part of this strategy because, in the dynamic environment of an actual conflict, identifying and targeting U.S. vulnerabilities will require sensing, relaying, and processing vast amounts of information at a speed only computers can match. AI is also key for uncrewed autonomous systems. In his speech to the CCP's 20th National Congress in October 2022, Xi called on China to "speed up the development of unmanned, intelligent combat capabilities."[8] In addition, China's program of Military-Civil Fusion—although its scope remains ambiguous in practice—seeks to appropriate select private technological advancements, including some developed in cooperation with international research partners, to augment the PLA's capabilities.[9]

III. AI Implementation in the PLA

China takes an expansive view of military AI's potential and is engaged in extensive research, development, and experimentation.[10] But so far, open-source information about the PLA fielding specific military AI systems remains sparse. The roles for AI within China's overall program of military modernization are still generally coming into focus. Researchers at the Center for Security and Emerging Technology analyzed 343 PLA equipment contracts and found seven areas of interest for current AI investments: (1) intelligent and autonomous vehicles; (2) intelligence, surveillance, and reconnaissance; (3) predictive maintenance and logistics; (4) information and electronic warfare; (5)

[6] Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (RAND Corporation, 2018), https://www.rand.org/pubs/research_reports/RR1708.html; Mark Cozad et al., *Gaining Victory in Systems Warfare: China's Perspective on the U.S.-China Military Balance* (RAND Corporation, 2023), https://www.rand.org/pubs/research_reports/RRA1535-1.html; and State Council Information Office of the People's Republic of China, *China's National Defense in the New Era* (July 2019), as reposted by the China Aerospace Studies Institute, https://www.airuniversity.af.edu/Portals/10/CASI/documents/Translations/2019-07%20PRC%20White%20Paper%20on%20National%20Defense%20in%20the%20New%20Era.pdf?ver=akpbGkO5ogbDPPbflQkb5A%3D%3D.

[7] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China* (2022), 39, https://media.defense.gov/2022/Nov/29/2003122279/-1/-1/1/2022-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

[8] Xi Jinping, *Hold High the Great Banner of Socialism with Chinese Characteristics and Strive in Unity to Build a Modern Socialist Country in All Respects: Report to the 20th National Congress of the CCP* (October 16, 2022), as reposted by Nikkei Asia, https://asia.nikkei.com/Politics/China-s-party-congress/Transcript-President-Xi-Jinping-s-report-to-China-s-2022-party-congress.

[9] Tai Ming Cheung, "The Promise and Peril of Military-Civil Fusion," in *Innovate to Dominate: The Rise of the Chinese Techno-Security State* (Ithaca: Cornell University Press, 2022), 83-141.

[10] For a detailed account of these activities, see Elsa Kania, Adjunct Senior Fellow at the Center for a New American Security, "Chinese Military Innovation in Artificial Intelligence," Statement to the U.S.-China Economic and Security Review Commission, June 7, 2019, https://www.uscc.gov/sites/default/files/June%207%20Hearing_Panel%201_Elsa%20Kania_Chinese%20Military%20Innovation%20in%20Artificial%20Intelligence_0.pdf.

simulation and training; (6) command and control; and (7) automated target recognition.[11] Those categories are illustrative but not necessarily exhaustive. Two areas of special focus are AI in the PLA's weapons systems and AI in the PLA's battlefield functions and support:

AI in the PLA's Weapons Systems (Uncrewed Systems, LAWS). Assessing China's progress in developing and fielding uncrewed autonomous vehicles (i.e., drones) for air, ground, sea surface, and subsea applications is difficult. Beijing clearly has a large and sophisticated drone industry and is the world's largest exporter of military drones.[12] But the fact that those systems can operate without an onboard crew indicates little about the degree to which they can act autonomously; autonomy would be enabled by AI and is therefore highly dependent on the quality of the AI. Uncrewed systems possess varying levels of autonomy. These range from essentially no autonomy in fully remote-controlled systems, to completely autonomous systems that can navigate, choose targets, and even fire without human control, with multiple levels in between.[13] As DOD's 2023 *China Military Power Report* states, the PLA is "pursuing greater autonomy for unmanned aerial, surface, and underwater vehicles to enable manned and unmanned teaming, swarm attacks, optimized logistic support, and distributed ISR [intelligence, surveillance, and reconnaissance], among other capabilities."[14]

China's commercial drone companies have exhibited a world-class ability to operate in AI-dependent swarms, which is likely to be a key capability for military applications.[15] Swarming is an area where capabilities developed in the private sector could be applied to the military sector quickly. Additionally, China is developing a system called the FH-97A, which is similar to the U.S. "loyal wingman" concept, where an autonomous aircraft flies in a team alongside a crewed aircraft.

Separately, China's drone capabilities link directly to the global debate about lethal autonomous weapons systems (LAWS) or, less formally, "killer robots." The PLA possesses plenty of lethal military power, but right now none of it appears to have meaningful levels of autonomy enabled by AI. Beijing's official policy on regulating LAWS is ambiguous, leaving open the possibility that China could develop and field such systems if the technology matures.

AI in the PLA's Battlefield Functions and Support. Tracking implementation of military AI in the categories of battlefield functions and support is even more difficult. That is because those capabilities are primarily software-based and therefore harder to observe through tools such as satellite imagery. That said, the PLA is likely to start using AI for predictive maintenance and logistics systems relatively early given similarity to commercial applications. Further, the PLA likely already uses basic forms of AI for some types of ISR tasks. AI promises to be particularly useful for combing through huge amounts of information from many different types of sensors. ISR is another field where

[11] Ryan Fedasiuk, Jennifer Melot, and Ben Murphy, *Harnessed Lightning: How the Chinese Military Is Adopting Artificial Intelligence* (Center for Security and Emerging Technology, October 2021), 13, https://cset.georgetown.edu/wp-content/uploads/CSET-Harnessed-Lightning.pdf.

[12] Stockholm International Peace Research Institute (SIPRI) data as cited in Zaheena Rasheed, "How China became the world's leading exporter of combat drones," Al Jazeera, January 24, 2023, https://www.aljazeera.com/news/2023/1/24/how-china-became-the-worlds-leading-exporter-of-combat-drones#:~:text=Data%20from%20the%20Stockholm%20International,exporter%20of%20the%20weaponised%20aircraft.

[13] No single universal framework for measuring autonomy in uncrewed systems exists, but one example of a framework can be found at "Breaking Down The Levels of Drone Autonomy," cloudfactory, November 23, 2021, https://blog.cloudfactory.com/levels-of-drone-autonomy.

[14] U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China* (2023), 97, https://media.defense.gov/2023/Oct/19/2003323409/-1/-1/1/2023-MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA.PDF.

[15] Emilie Stewart, *Survey of PRC Drone Swarm Inventions* (China Aerospace Studies Institute, October 9, 2023), https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2023-10-09%20Survey%20of%20PRC%20Drone%20Swarm%20Inventions.pdf.

China's AI innovations for, and vast training data from, its domestic repression apparatus, including biometrics and image recognition, likely aid progress in the PLA's systems.

Next, China will pursue AI systems for use in command, control, and communications (C3) and decision-making purposes, likely advancing over time through three levels of sophistication. The first level is using AI for counter-C3; that is, to improve China's cyber capabilities with the objective of trying to disrupt the opponent's C3. The use of AI in cyber operations is relatively mature and will likely grow more capable over time. Better offensive cyber capabilities will enable the full range of cyber operations, including "adversarial AI," or trying to disrupt the opponent's AI systems.[16]

The second level of military AI for C3 applications is tactical- and operational-level C3 for the PLA's physical weapons systems. The PLA is likely to use AI to control uncrewed systems, either individually or coordinated in a swarm. Improving targeting and allocation of scarce artillery and munitions might be another use. A news report from April 2023 showed the PLA testing an AI system to help with artillery targeting.[17] Further, Beijing is likely to use AI to help develop plans for the tactical and operational level of warfare with the goal of cutting through the fog of war and gaining decision-advantage—a version of what Chinese military experts have called a "command brain."

The third level of sophistication for military AI for C3 purposes would be for strategic- or political-level decisions. In the near- and mid-terms, China will likely hesitate to put in place AI systems for these types of decisions, because the technology will still be immature. Moreover, PRC leaders insist on tight political control, particularly of strategic capabilities such as nuclear weapons.

The future trajectory of military AI in the PLA. While China has ambitious plans for infusing military AI throughout the PLA, the technology's ultimate trajectory is not currently clear. Beijing will have to overcome multiple obstacles to fulfill its objectives, as I will lay out in the next section. At the same time, AI is a general-purpose technology (like electricity or railroads), so analysts cannot yet know all of its potential uses or implications.[18] In the near- and mid-terms, most of the changes AI will usher in will be incremental and narrow. But in the mid- to long-term, some could be revolutionary and general. China provides little transparency on its military modernization efforts, including for AI, which could someday lead to strategic surprise for the United States if Beijing manages to make breakthroughs in secret.

IV. How the PLA Might Fall Short of Its AI Ambitions

Neither articulating lofty goals nor simply throwing money and people at the issue will ensure Beijing fulfills its ambitions for integrating AI into the PLA. China could fall short of, or at least face delays in reaching, its goals due to several obstacles, including:

Technology. The technology itself might prove difficult to master, even with abundant resources. Technology controls imposed by the United States and its allies could hamper Beijing's ability to develop and operate AI-enabled systems at scale. Additionally, China could simply lack the capacity to innovate at the leading edge of military technology. In earlier stages of its military modernization, China could imitate

[16] Apostol Vassilev et. al, *Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations* (National Institute of Standards and Technology, January 2024), https://csrc.nist.gov/pubs/ai/100/2/e2023/final.
[17] Stephen Chen, "China tests AI-powered long-range artillery that can hit a person 16km away," *South China Morning Post*, April 17, 2023, https://www.scmp.com/news/china/science/article/3217334/china-tests-ai-powered-long-range-artillery-can-hit-person-16km-away.
[18] Jeffrey Ding and Allan Dafoe, "Engines of Power: Electricity, AI, and general-purpose, military transformations," *European Journal of International Security*, 8 no. 2 (February 7, 2023): 1-18, https://doi.org/10.1017/eis.2023.1.

and/or steal technology from the United States, Russia, and other advanced militaries. However, intelligentization requires pioneering totally new military technologies and operational concepts for how to use them—a much more difficult task.

Personnel, bureaucracy, and corruption. Impediments related to personnel, bureaucratic structure, or political control could further constrain the PLA's AI ambitions. These include a lack of skilled personnel needed to operate AI systems and stovepiped military bureaucracies. The PLA's Strategic Support Force (SSF)—a stand-alone military service created in 2015 to focus on space, cyber, and electromagnetic warfare—appears to control the lion's share of AI development resources and authority within the PLA.[19] While the SSF may have been created in part to enable jointness through advanced networking and now AI, it may be loath to relinquish control of its creations to the rest of the PLA, or other services might resist relying on capabilities run by the SSF.[20] The PLA's efforts to implement AI across the joint force could also fall prey to corruption, as has reportedly been the case for parts of China's nuclear missile forces.[21]

Political control. The CCP values political control above other aims. The dictum that "the party controls the gun"—first stated by Mao Zedong and reaffirmed by Xi—and the prominent role of political commissars in the PLA reflect that fact.[22] Even for expert researchers, today's state-of-the-art AI models present challenges for predictability, "explainability," and transparency. This opacity could make PLA commanders reluctant to trust it for fear that they do not control its actions.[23] Alternatively, however, Chinese leaders might be more willing to place trust in programmable machines over people. Given these contradictory impulses, it is not yet clear to what extent China's military leadership and operational-level commanders will embrace or avoid AI in practice.

Funding. Some obstacles might be material. The PLA officially declared that it achieved full mechanization in 2020, is making rapid progress on informatization, and is pushing to develop cutting-edge capabilities necessary for intelligentization. But as large numbers of once-new ships, aircraft, and other weapons systems age, the cost to operate and maintain them will rise quickly, potentially crowding out investments in next-generation AI-enabled capabilities. Should China's domestic economy face sustained headwinds, fewer resources might be available for advancing AI within the PLA.

[19] John Costello and Joe McReynolds, "China's Strategic Support Force: A Force for a New Era," in Phillip C. Saunders et al., eds., *Chairman Xi Remakes the PLA: Assessing Chinese Military Reforms* (Washington: National Defense University Press, 2019), 437-515, https://ndupress.ndu.edu/Media/News/News-Article-View/Article/1748555/chinas-strategic-support-force-a-force-for-a-new-era/.

[20] Amy Nelson and Gerald Epstein, *The PLA's Strategic Support Force and AI Innovation* (The Brookings Institution, December 23, 2022), https://www.brookings.edu/techstream/the-plas-strategic-support-force-and-ai-innovation-china-military-tech/.

[21] Peter Martin and Jennifer Jacobs, "US Intelligence Shows Flawed China Missiles Led Xi to Purge Army," Bloomberg, January 6, 2024, https://www.bloomberg.com/news/articles/2024-01-06/us-intelligence-shows-flawed-china-missiles-led-xi-jinping-to-purge-military?srnd=undefined.

[22] Minnie Chan, "Communist Party 'controls the gun,' PLA top brass reminded," *South China Morning Post*, November 5, 2014, https://www.scmp.com/news/china/article/1632136/communist-party-controls-gun-pla-top-brass-reminded; and Timothy Heath, Senior International Defense Researcher, "The Consolidation of Political Power in China Under Xi Jinping: Implications for the PLA and Domestic Security Forces," Statement to the U.S.-China Economic and Security Review Commission, February 7, 2019, https://www.uscc.gov/sites/default/files/Heath_USCC%20Testimony_FINAL.pdf.

[23] Kelley M. Sayler, *Artificial Intelligence and National Security* (Congressional Research Service, November 10, 2020, update), 30-33, https://crsreports.congress.gov/product/pdf/R/R45178/10.

V. Risks that China's Military AI Poses to the United States

Given the emerging nature of, and sprawling potential applications for, military AI in the PLA, it is too early to know all the risks those capabilities might pose to the United States. It is possible, though, to develop a provisional list, which would include the following:

Shift in the military balance of power. Perhaps the most likely source of strategic risks in the U.S.-China security relationship stemming from military applications of AI will be one that is difficult to measure precisely and cannot be solely attributable to AI: the overall military balance. Many of the most practical uses for military AI in the near term will be for purposes that are relatively mundane but could help the PLA use resources more efficiently and therefore generate more military capabilities per renminbi or dollar spent. These include helping to improve processes for maintenance, logistics, training, and decision-support. Such "back office" functions rarely receive the sustained attention devoted to "tip of the spear" capabilities that appear on the front lines of combat. However, the strength of modern militaries depends as much on their enabling bureaucracies as their frontline troops and weapons.

In addition, some emerging military AI applications will improve the PLA's combat capabilities. Initially, those improvements are likely to be *evolutionary* rather than *revolutionary*. Consider the air domain, to name just one of many examples. "Loyal wingman"-type systems where uncrewed aircraft fly with crewed aircraft could improve on what human pilots could do on their own.[24] But uncrewed and fully autonomous air systems—capable of greater persistence, maneuverability, and other attributes due to their lack of human bodily limitations—will likely be necessary for a complete paradigm shift in air combat operations. A similar story is playing out across nearly every aspect of military affairs. If the totality of improvements in military AI across every area tip the U.S.-China military balance in Beijing's favor, then the risks of conflict could rise.

Decision-making. Military AI tools could increase strategic risks emanating from the decision-making and information domain in three main ways: by compressing the time policymakers have to make high-stakes decisions, by generating bad inputs to decision-making processes, and by tempting actors to try to undermine states' deliberations through large-scale information operations. (My co-panelist will cover China's "cognitive domain operations," so I am skipping over them despite their clear relevance in this area.)

Autonomous uncrewed systems. Autonomous uncrewed systems could lead to deliberate escalation in a crisis if leaders see them as less dangerous to deploy, either because of lower expected human casualties or merely because the systems are more capable. Drones could also cause inadvertent escalation if either state takes an action using an autonomous system that the other state sees as provocative and escalatory. Finally, autonomous uncrewed systems could lead to an accident due to error or malfunction.

Intelligence, surveillance, and reconnaissance (ISR). AI is likely to be particularly effective for ISR applications given its ability to identify patterns in massive amounts of data. Additionally, it could enable new ISR capabilities, such as some surveillance balloons, in areas where norms are non-existent or weak.

[24] Liu Xuanzun, Cao Siqi, and Fan Wei, "Exclusive: China's new loyal wingman drone to greatly change air combat: designer," *Global Times*, November 7, 2022, https://www.globaltimes.cn/page/202211/1278930.shtml; Tom Ward, "The US Air Force Is Moving Fast on AI-Piloted Fighter Jets," *Wired*, March 8, 2023, https://www.wired.com/story/us-air-force-skyborg-vista-ai-fighter-jets/.

Command, control, and communication (C3). AI could empower better PLA C3 as China pursues multi-domain precision warfare, its analog to the U.S. Joint All-Domain Command and Control (JADC2) concept. Conversely, AI could empower attacks against U.S. or allied C3 systems. AI-assisted C3 and counter-C3 together have the potential to create "use or lose" pressures on decisionmakers in both countries during a crisis or contingency that could drive escalation.

Nuclear weapons. In the nuclear arena, AI systems could enable large-scale processing of data from various sensors to track mobile missile systems on land and even submarines at sea, especially if combined with other emerging technologies, such as quantum sensors.[25] Those applications are still only theoretical but could be feasible in the medium term.[26] If they come to pass, they could create transparency with destabilizing effects by undermining the *survivability*—the property of a military system that makes it hard for adversary forces to find and destroy—of components of two legs of the nuclear triad by enabling adversary tracking and targeting of those assets for counterforce strikes.

Additionally, PRC experts have expressed concerns that these same capabilities, if fielded by the United States, could undermine China's nuclear deterrent.[27] Those experts also worry that uncrewed autonomous systems could create new nuclear counterforce options. Such concerns could be one among several reasons China is expanding its nuclear arsenal.

VI. Assessing U.S. Policy Toward China's Military AI Activities

How the United States and its allies and partners respond to China's military AI ambitions will be an important factor shaping the balance of military AI capabilities specifically and military power generally. Washington's approach to date can be assessed along three lines of effort: improving U.S. and allied military AI capabilities, taking steps to hinder China's progress on developing military AI, and diplomacy with China related to military AI. This section will cover each in turn.

Improving U.S. and allied military AI capabilities. The U.S. Department of Defense has prioritized developing and fielding cutting-edge AI for military applications, including unilaterally through the Chief Digital and Artificial Intelligence Office (CDAO), the Replicator Initiative, and the first-ever National Defense Industrial Strategy. Washington is also working with allies on military AI through the advanced capabilities (pillar 2) of the Australia-United Kingdom-United States (AUKUS) partnership and the creation of an AI Strategy for NATO.[28] American defense officials recognize the possible ramifications of maturing AI technologies for the international security environment. That said, any revolution in military affairs that AI might create is still in its infancy, if it happens at all. There is a long road ahead where the United States

[25] Paul Bracken, *The Hunt for Mobile Missiles: Nuclear Weapons, AI, and the New Arms Race* (Foreign Policy Research Institute, September 21, 2020), https://www.fpri.org/article/2020/09/the-hunt-for-mobile-missiles-nuclear-weapons-ai-and-the-new-arms-race/; and Edward Geist and Andrew Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War* (RAND Corporation, 2018), https://www.rand.org/pubs/perspectives/PE296.html.
[26] Kelley M. Sayler, *Defense Primer: Quantum Technology* (Congressional Research Service, November 15, 2022, update), https://crsreports.congress.gov/product/pdf/IF/IF11836; and Edward Parker, *Commercial and Military Applications and Timelines for Quantum Technology* (RAND Corporation, 2021), https://www.rand.org/pubs/research_reports/RRA1482-4.html.
[27] Chen Qi and Zhu Rongsheng, *Uncertainties: Why Are We Concerned about the Impact of AI on International Security?* (Center for International Security and Strategy at Tsinghua University, 2019), 5, https://ciss.tsinghua.edu.cn/info/eyjdt/1363.
[28] Patrick Parrish and Luke Nicastro, *AUKUS Pillar 2: Background and Issues for Congress* (Congressional Research Service, June 20, 2023), 5-6, https://crsreports.congress.gov/product/pdf/R/R47599.

could be held back by an R&D and acquisition system that is still too often stuck in the 20th century, military service cultures sometimes reluctant to embrace major changes, and fierce resource competition. More broadly, in competition with China over military AI, U.S. officials will have to pursue competitive policies across all the constituent parts of AI: chips for "compute" power, data, algorithms as well as the talent and institutions to develop and scale them.[29]

Slowing down China's progress on developing military AI. Washington has also taken significant steps to slow down Beijing's acquisition of advanced AI, particularly for military applications. These include aggressive semiconductor controls; restrictions on outbound and inbound investment into the sector; and placing entities with ties to the PLA on various sanctions lists.[30] Those are all smart actions, but they will have to be updated over time as China continually develops workarounds. Most of the enforcement action so far has focused on chips, but U.S. policymakers will have to monitor action on all the constituent parts of AI mentioned earlier.

Specifically, protecting algorithms and data controlled by U.S. and allied organizations from PRC espionage will be critical. Taking steps to improve the physical and cyber security of key U.S. and allied firms that possess or make inputs for AI will be a logical imperative in this context. And while there have not been any blatantly obvious copies of U.S. AI technology like those seen in the advanced fighter aircraft field, it is reasonable to surmise that major data sets stolen by China—such as the 2015 theft of data from the U.S. Office of Personnel Management—could be used to train AI models.

Engaging China on stability and norms related to military AI. Washington has also sought to engage Beijing on developing norms for military AI and potentially even arms control measures in the future. The U.S. readout of President Biden's November 2023 meeting with General Secretary Xi said the two leaders "affirmed the need to address the risks of advanced AI systems and improve AI safety through U.S.-China government talks."[31] Beijing seeks to shape the agenda for both civilian and military AI governance globally. China proposed the Global AI Governance Initiative in October 2023, although details of what that initiative entails are sparse, and attended the November 2023 AI Safety Summit in the United Kingdom and signed the resulting Bletchley Declaration.[32] The United States has similarly been active in putting forward principles for governing AI domestically and internationally, notably through the "Political Declaration on

[29] My colleague Paul Scharre has called computing power, data, talent, and institutions the "four battlegrounds" of global AI competition. Paul Scharre, *Four Battlegrounds: Power in the Age of Artificial Intelligence* (New York: W.W. Norton & Company, 2023).

[30] Emily Kilcrease and Michael Frazer, *Sanctions by the Numbers: SDN, CMIC, and Entity List Designations on China* (Center for a New American Security, March 2, 2023), https://www.cnas.org/publications/reports/sanctions-by-the-numbers-sdn-cmic-and-entity-list-designations-on-china.

[31] White House, "Readout of President Joe Biden's Meeting with President Xi Jinping of the People's Republic of China," press release, November 15, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/15/readout-of-president-joe-bidens-meeting-with-president-xi-jinping-of-the-peoples-republic-of-china-2/.

[32] Ministry of Foreign Affairs of the People's Republic of China, "Global AI Governance Initiative," Communique, October 20, 2023, https://www.mfa.gov.cn/eng/wjdt_665385/2649_665393/202310/t20231020_11164834.html; United Kingdom, "The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023," January 16, 2024, https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023.

Responsible Military Use of Artificial Intelligence and Autonomy" that has been endorsed by 47 states.[33] Ultimately, U.S.-China dialogue on these issues is important but just one pillar of a comprehensive strategy to govern AI, including for military applications.

VII. Recommendations for Policymakers

1. Take bold action to constrain China's progress in AI for military and repressive purposes, but do so in a narrow way that avoids self-defeating steps. Washington should continue to take aggressive steps to constrain China's progress in these areas. But U.S. leaders must also ensure those efforts are coordinated with allies and close partners, and that they account for technical and market dynamics given that the primary source of innovation in AI is in the commercial rather than the government sector.

2. Build U.S. military AI capabilities to stay on the cutting edge. AI could define the future of military power. Washington will need to move quickly to stay on the cutting edge. This will require pushing forward reforms to the Pentagon's acquisition process and, in some cases, prioritizing funding for future capabilities over buying and operating already-mature capabilities. Deterring China today should be balanced with what will be necessary for deterrence 5-15 years down the road.

3. Continue to shape global rules, norms, and institutions around the deployment and use of military AI. Congress should support U.S. efforts to build consensus around rules, norms, and institutions to govern the use of military AI. U.S. foreign policy's core objective is upholding a rules-based global order. Unlike in many other areas, though, there are no legacy rules and norms for military AI. Instead, they are being written in real time. It is therefore important to develop and promulgate norms in this emerging area and build a coalition of states in support them. Moreover, such norms should address links to other key strategic areas like nuclear weapons, cyber, and space.

4. Engage with China in a clear-eyed way on military AI risks. Talks with Beijing about the risks of AI and how to bolster safety and stability are worthwhile and should move forward. The key, however, will be keeping expectations modest for what those talks can achieve. Early topics could include working toward a risk hierarchy for military AI applications; exchanging select information about test, evaluation, validation & verification (TEVV) processes; and implementation of the principle of always keeping humans in the loop for actions related to nuclear weapons.

5. Prioritize intelligence-gathering and analysis on, and net assessment of, China's military AI capabilities. China has ambitious plans for military AI and is pursuing them at a rapid pace. But whether the PLA can develop and field military AI capabilities for real-world use at scale remains to be seen. U.S. officials should allocate additional resources to tracking Beijing's progress (or lack thereof) across the full range of military AI applications. As part of that effort, U.S. intelligence should assess China's access to important data sets—for example, data Russia has gleaned from Moscow's combat systems operating in Ukraine and Syria—and algorithms that could help train AI systems for combat applications.

[33] U.S. Department of Defense, "U.S. Endorses Responsible AI Measures for Global Militaries," press release, November 13, 2023, https://www.defense.gov/News/News-Stories/Article/Article/3597093/us-endorses-responsible-ai-measures-for-global-militaries/.

OPENING STATEMENT OF NATHAN BEAUCHAMP-MUSTAFAGA, POLICY RESEARCHER, RAND CORPORATION

MR. BEAUCHAMP-MUSTAFAGA: Thank you -- try again. Thank you for the opportunity to testify today about how the Chinese military views the prospects of generative AI for social media manipulation and more broadly on the evolution of cyber enabled influence operation efforts. I'm especially honored also as former Commission staff.

I want to make three key points for the Commission today. First, generative AI has the potential to revolutionize cyber enabled influence operations and supercharge malign actor's ability to undermine the democratic process in the United States and around the world. The key breakthrough of generative AI is a dramatic improvement in authenticity and scale at a lower cost while also reducing human labor requirements and the probability of detection.

Second, the PLA is already known to be one of several Chinese Communist Party state actors engaged in cyber enabled influence operations. And there are many reasons we should be concerned that the Chinese military will incorporate generative AI for improved effectiveness at scale.

Third, Congress and the broader U.S. government need to be prepared to live in a world with a much worse information environment, more convincing and more pervasive malign influence operations.

And this now includes the risk of Chinese election interference. I want to briefly touch on three main topics: Chinese military strategy, capabilities, and intent as well as some potential policy options for U.S. policymakers. First, on Chinese military strategy, the PLA has long targeted and tailored influence operations.

Social media gave them targeted IO and generative AI has the potential to give them tailored IO. The Chinese military's new overarching operational concept for influence operations is cognitive domain operations which DOD explains as, quote, combining psychological warfare with cyber operations to shape adversary behavior and decision-making, end quote, with the likely intention to, quote, deter U.S. or third-party entry into our future conflict or as an offensive capability to share perceptions or polarize a society, end quote. Cognitive domain operations is a technologically driven update to the more traditional three warfare concept you may be familiar with.

But it more fundamentally reflects a shift in how the Chinese military thinks about the battle space from the traditional air, sea, and land with space and cyber and to now viewing warfare as occurring in the physical domain, information domain, and cognitive domain. This view is not yet formally PLA doctrine. But it's a very important trend for Congress and the broader U.S. national security community to watch.

Generative AI fits in cognitive domain operations by supercharging the PLA's performance. But so far, there does not seem to be a significant shift in PLA tactics. To summarize broadly the PLA writings I reviewed for this testimony, PLA researchers absolutely recognize the potential for generative AI to dramatically improve content generation and content distribution and recognize benefits for scale, speed, and reduced cost, among others. I observed PLA researchers discussing three main uses of generative AI for influence operations.

First, influencing public opinion will be a large-scale social bot networks. Second, producing intentionally biased publicly available models. Third, specifically degrading support for adversary leadership.

This aligns with existing explicit interest by PLA researchers to produce inauthentic content, sometimes called synthetic information, as well as large-scale social bot networks. I want to note here that PLA writings on the topic of generative AI and influence operations express immense concern about the potential use by the United States against the CCP to, in so many words, undermine its regime security. Public reports of U.S. government activities, especially those distributed to the Department of Defense, are very closely watched by PLA researchers and taken as validation of U.S. intent against China.

This is not just an academic point. Some PLA researchers explicitly call for adopting cyber enabled IO to respond to perceived U.S. activity. On the topic of Chinese military capabilities and adoption, so far, we have no direct evidence that PLA is specifically adopting generative AI for its ongoing cyber-enabled influence operations.

However, I argue the PLA is certainly currently capable of doing so if it chooses. Moreover, our recent RAND report highlights a PLA affiliated researcher named Li Bicheng who has been working on a system for online public opinion struggle since at least 2016 and has been envisioning an end to end automated online influence system since at least 2019. Basically, the technology he envisioned in 2019 have come true with generative AI breakthroughs over the past year plus.

Recent public reporting suggests other party-state actors have likely begun adopting generative AI. And early evidence suggests it may be improving their performance. Lastly, on intentions, generative AI is likely to supercharge existing PLA objectives such as shaping foreign and public -- foreign and domestic public opinion, deterring U.S. involvement in a future Taiwan conflict, and degrading U.S. and Taiwanese will to fight, among other objectives.

However, I want to specifically flag the risk of Chinese election interference now that we're entering the 2024 election season. A recently declassified U.S. National Intelligence Council report on foreign election interference in 2022 found that, quote, China tacitly approved efforts to try to influence a handful of midterm races involving members of both U.S. political parties, end quote. In ODNI's 2023 worldwide threat assessment said that Beijing, quote, has shown a willingness to meddle in select election races that involve perceived anti-China politicians, end quote.

A 2021 article by PLA researchers that I found suggest at least some in the PLA are also already using social media to identify politicians who are pro- or anti-China to, in my analysis, back for election interference. I provide more details in my written statement. But in summary, they used Twitter data from sitting U.S. government officials with known views of China to train a deep learning model and then use it to predict how other U.S. politicians view China and validated the results by consulting intelligence analysts.

In the PLA author's own words, the capabilities intended to, quote, assist intelligence analysts in their assessment of U.S. political inclinations and future paths for U.S.-China relations, end quote. For policy options to consider, I'll highlight several and I have more in my written testimony. First, require social media platforms to label generative AI content and redouble their efforts to combat fake accounts.

Second, commit now to publicly releasing a nonpartisan declassified assessment by the U.S. intelligence community following the U.S. 2024 election. Third, encourage Taiwan to increase its information sharing, both publicly and privately, about Chinese cyber enabled influence operations. And support Taiwan's engagement with other democracies to share its lessons learned and best practices for combating Chinese IO.

Fourth, engage in dialogue with China on AI-driven cyber enabled influence operations to explore the possibility for an agreement of prohibiting state use of such capabilities. Fifth, conduct an independent assessment of the net benefit of U.S. government information efforts, including whether DOD combat and command activities align with DOD stated priorities and strategic messaging. Thank you again for the opportunity to testify. I look forward to your questions.

COMMISSIONER WESSEL: Thank you. Mr. Parker.

PREPARED STATEMENT OF NATHAN BEAUCHAMP-MUSTAFAGA, POLICY RESEARCHER, RAND CORPORATION

Testimony

NATHAN BEAUCHAMP-MUSTAFAGA

Exploring the Implications of Generative AI for Chinese Military Cyber-Enabled Influence Operations

Chinese Military Strategies, Capabilities, and Intent

CT-A3191-1

Testimony presented before the U.S.-China Economic and Security Review Commission at the hearing "Current and Emerging Technologies in U.S.-China Economic and National Security Competition" on February 1, 2024

For more information on this publication, visit **www.rand.org/t/CTA3191-1**.

Testimonies

RAND testimonies record testimony presented or submitted by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies.

Published by the RAND Corporation, Santa Monica, Calif.

Limited Print and Electronic Distribution Rights

Exploring the Implications of Generative AI for Chinese Military Cyber-Enabled Influence Operations: Chinese Military Strategies, Capabilities, and Intent

Testimony of Nathan Beauchamp-Mustafaga[1]
The RAND Corporation[2]

Before the U.S.-China Economic and Security Review Commission at the hearing "Current and Emerging Technologies in U.S.-China Economic and National Security Competition"

February 1, 2024

Co-chair Helberg and co-chair Wessel, thank you for the opportunity to testify today about how the Chinese military views the prospects of generative artificial intelligence (AI) for social media manipulation, and more broadly on the evolution of its cyber-enabled influence operations (IO) efforts. My testimony will provide an overview of Chinese military strategy, capabilities, and intent, including on the topic of potential Chinese interference in U.S. elections via social media.

Overview

There are many reasons to be concerned that the Chinese military will incorporate generative AI into its existing cyber capabilities to augment its ability to conduct cyber-enabled influence operations, including operations that seek to undermine the democratic process in the United States and around the world.[3] The key breakthrough with generative AI is the dramatic

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research.
[2] RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND's mission is enabled through its core values of quality and objectivity and its commitment to integrity and ethical behavior. RAND subjects its research publications to a robust and exacting quality-assurance process; avoids financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursues transparency through the open publication of research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. This testimony is not a research publication, but witnesses affiliated with RAND routinely draw on relevant research conducted in the organization.
[3] William Marcellino, Nathan Beauchamp-Mustafaga, Amanda Kerrigan, Lev Navarre Chao, and Jackson Smith, *The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0: Next-Generation Chinese Astroturfing and Coping with Ubiquitous AI*, RAND Corporation, PE-A2679-1, September 2023, https://www.rand.org/pubs/perspectives/PEA2679-1.html.

improvement in authenticity and scale at a lower cost—while also reducing human labor requirements and the probability of detection. Taken together, the "critical jump forward . . . is in the plausibility of the messenger rather than the message."[4] This potential applies to any malign actors, domestic or foreign, because of the open-source nature and very low bar to adoption of generative AI technology.

Beijing has long sought targeted and tailored IO, and while social media has enabled *targeted* IO, generative AI has the potential to enable *tailored* IO. Based on an initial review of Chinese military writings, there is clear awareness by at least some in the People's Liberation Army (PLA) of generative AI's revolutionary potential. We are beginning to see some adoption of generative AI technologies by Chinese Communist Party (CCP)-state actors for cyber-enabled IO, and there is early evidence that this new technology is improving CCP IO performance. However, although we know that the PLA is already engaging in cyber-enabled IO, we have no direct evidence that the PLA is specifically adopting generative AI for this purpose yet. Regardless, I argue that the PLA is currently capable of adopting generative AI if it so chooses, and I point to a case study of a PLA-affiliated researcher, Li Bicheng, to illustrate the PLA's likely readiness for adoption. For the PLA, this could support its IO objectives of shaping foreign (and domestic) public opinion, deterring U.S. involvement in a future Taiwan conflict, and degrading U.S. and Taiwanese will to fight, among other objectives.

This testimony and supporting research are based on open-source Chinese language primary source research and builds on two recent RAND reports.[5] My research focuses mainly on how the Chinese military develops its strategy and capabilities for social media manipulation, with an effort where possible to address technical-level details to provide greater clarity. Broadly, my research is interested in the *inputs* into Chinese efforts for social media manipulation versus the *outputs* of observed Chinese behavior, which is inherently an incomplete and retrospective reverse engineering of Chinese intent and capabilities.

Chinese Military Strategy for Cyber-Enabled Influence Operations

The Chinese military's strategy for cyber-enabled influence operations is evolving to incorporate new technologies and keep up with broader PLA strategic thinking. Historically, the PLA's influence operations generally fell under the concept of the "Three Warfares" (三种战法), which were developed in the mid-2000s and included "psychological warfare" (心理战), "public opinion warfare" (舆论战), and "legal warfare" (法律战). Cyber-enabled influence

[4] Marcellino et al., 2023, p. 1.
[5] Nathan Beauchamp-Mustafaga, *Chinese Next-Generation Psychological Warfare: The Military Applications of Emerging Technologies and Implications for the United States*, RAND Corporation, RR-A853-1, 2023, https://www.rand.org/pubs/research_reports/RRA853-1.html; Marcellino et al., 2023.

operations generally fell under public opinion warfare, specifically "online public opinion warfare" (网络舆论战).[6]

The Chinese military has increasingly adopted "cognitive domain operations" (认知域作战) (CDO) as the primary operational concept for cyber-enabled influence operations since the late-2010s.[7] This evolution reflects a fundamental shift in the Chinese military's conception of the battlespace from the traditional air, sea, and land domains—with space and cyber added in the 1990s—into now viewing warfare as occurring in the physical domain (物理域), information domain (信息域), and cognitive domain (认知域). There is a group of PLA researchers, often focused on IO, who argue that the cognitive domain is the new focus of warfare.[8] However, this is not yet the official PLA view, and there are alternative conceptions within the PLA; for example, the 2020 PLA National Defense University version of *Science of Military Strategy* lists space, network, deep sea, polar regions, biology, and intelligence as new domains of warfare.[9] To summarize this group's perspective, the logical conclusion of the PLA's system-of-systems warfare is to win a conflict with as little kinetic destruction as possible and force the adversary to accept defeat short of total destruction—and thus, fundamentally, a psychological or cognitive decision to surrender, as compared with the 20th century construct of total warfare and complete physical exhaustion of adversary military capabilities and resources.[10] Within PLA military theory, the identification of a new domain thus drives the exploration of the required aspects for each domain: "cognitive warfare" (认知战), "cognitive confrontation" (认知对抗), "cognitive deterrence" (认知威慑), and "command of cognition" (制认知权), among others. None of these terms are officially defined in standard PLA authoritative texts, such as the PLA dictionary (军语), because they gained popularity after the dictionary's publication in 2011, but future editions are likely to include these now key concepts for the PLA.[11]

---

[6] Beauchamp-Mustafaga, 2023. For an authoritative PLA source, see Wu Jieming [吴杰明] and Liu Zhifu [刘志富], *An Introduction to Public Opinion Warfare, Psychological Warfare, and Legal Warfare* [舆论战心理战法律战概论], National Defense University Press, 2014.

[7] For more on CDO, see Beauchamp-Mustafaga, 2023; Nathan Beauchamp-Mustafaga, "Cognitive Domain Operations: The PLA's New Holistic Concept for Influence Operations," *China Brief*, Vol. 19, No. 16, September 6, 2019.

[8] See, for example, Chen Dongheng [陈东恒], "Command of Cognition: An Important Support for Winning the War" ["制认知权: 战争制胜重要支撑"], *PLA Daily*, April 19, 2022; Zhao Quanhong [赵全红], "Cognitive Domain Operations: The Key to Winning Modern Warfare" ["认知域作战：现代战争的制胜关键"], *PLA Daily*, July 14, 2022; Pu Duanhua [濮端华], Li Xiwen [李习文], and Xiao Fei [肖飞], "Getting It Right on How Cognitive Penetration Influences Multi-Domain Operations" ["把准认知域渗透影响多域作战的规律"], *PLA Daily*, January 19, 2023.

[9] Xiao Tianliang [肖天亮], ed., *Science of Military Strategy* [战略学], National Defense University Press [国防大学出版社], 2020, pp. 142–180.

[10] Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare*, RAND Corporation, RR-1708-OSD, 2018, https://www.rand.org/pubs/research_reports/RR1708.html.

[11] All Army Military Terminology Management Committee [全军军语管理委员会], *Military Terminology of the Chinese People's Liberation Army* [中国人民解放军军语], Military Science Press, 2011.

PLA researchers often attribute to the U.S. military the conception of the cognitive domain as a domain of military struggle, but in reality, PLA interest is fundamentally about CCP regime security, which is the PLA's number one priority as the armed wing of the CCP.[12] This is part of a much longer trend of CCP concerns that information (typically foreign information) could undermine CCP regime control over the domestic Chinese population, sometimes euphemistically described as "ideological security," "cultural security," or, more recently, "cognitive security." Most directly, the Arab Spring and the wave of social media–driven overthrows of authoritarian regimes drove the PLA and broader CCP to view social media as a threat and led to renewed attention on how to influence perceptions and behavior.

CDO appears to be intended as a technologically driven update to bring the "Three Warfares" concept—developed in the information-driven era of informatization (信息化)—into the new AI-driven era of intelligentization (智能化). The U.S. Department of Defense (DoD) explains that CDO "combines psychological warfare with cyber operations to shape adversary behavior and decision making," with the likely intention to "use CDO as an asymmetric capability to deter U.S. or third-party entry into a future conflict, or as an offensive capability to shape perceptions or polarize a society."[13] DoD adds that

> [t]he PLA's goals for social media influence operations include promoting narratives to shape foreign governments' policies and public opinion in favor of the PRC's [People's Republic of China's] interests and undermining adversary resolve. The PLA views social media through the prism of information dominance, and during a crisis could use digital influence operations to undermine enemy morale and confuse or deceive adversary decision makers.[14]

As an overarching military operational concept for military activities in the cognitive domain, CDO includes four main aspects: "reading the brain" (读脑), "controlling the brain" (制脑), "resembling the brain" (类脑), and "strengthening the brain" (强脑).[15] "*Reading the brain*" focuses on understanding how others are thinking, "*resembling the brain*" is about using the human brain as inspiration for designing better computers, and "*strengthening the brain*" is about improving one's own cognition and performance. "*Controlling the brain*" focuses on influencing or even controlling adversary thinking and behavior. Although some PLA discussions of "*controlling the brain*" are futuristic, a more practical example is PLA interest in non-lethal, non-kinetic body-targeted weapons, such as directed energy capabilities like the U.S. military's Active Denial System.

It is clear that CDO is the most prominent operational concept for current PLA cyber-enabled IO. This is best represented in a 2018 article by researchers at the PLA Strategic Support Force's (PLASSF) Base 311, the PLA's only known operational unit dedicated to IO, which addressed

---

[12] For more on this threat perception, see Nathan Beauchamp-Mustafaga and Michael S. Chase, *Borrowing a Boat Out to Sea: The Chinese Military's Use of Social Media for Influence Operations*, Foreign Policy Institute at John Hopkins University School of Advanced International Studies, 2019; Beauchamp-Mustafaga, 2023.
[13] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China*, U.S. Department of Defense, 2023, p. 156.
[14] Office of the Secretary of Defense, 2023, p. 158.
[15] See Beauchamp-Mustafaga, 2023, pp. 52–67.

the hardware requirements for CDO and specifically focused on social media manipulation.[16] It is likely that this article reflected PLA preparations for social media interference in Taiwan's 2018 elections based on Taiwan's later claims of PLA involvement, Base 311's historical focus on Taiwan, and explicit references in the article to social media platforms popular in Taiwan.[17] PLA discussions of CDO dovetail with related PLA discussions of "intelligentized public opinion warfare" (智能化舆论战) that focus on leveraging AI, big data, social media, and social bots, among other emerging technology, for improved messaging and targeting effectiveness.[18] This also dovetails with broader Chinese Party-state efforts to become the leading AI power by 2030.[19]

Chinese Military Views on the Applications of Generative AI for Cyber-Enabled Influence Operations

PLA researchers recognize the potential improvement offered by generative AI for cyber-enabled IO, although most PLA discussions apply the new technology to existing tactics. Despite OpenAI releasing ChatGPT in November 2022, it appears that the PLA did not really pay attention until March 2023. PLA researchers generally focus on the advantages of generative AI for content (mostly text) generation but also address the benefits from automation to improve content distribution, as well as reduce labor requirements and cost. This aligns well with existing PLA interest in content generation—as the PLA sometimes describes it, "synthetic information" (合成信息)—namely, producing inauthentic content based on some amount of original information, as well as with content distribution using social bots (社交机器人)—namely, algorithmic agents for social media.[20]

Much of the surveyed PLA writings are focused on the potential cyber and AI-driven information threat from the United States. For example, there is a lot of euphemistic discussion about concerns for CCP regime security stemming from AI technology, ranging from the fact that Western large language models (LLMs) are inherently biased toward Western values to the risks of the United States and other Western countries using generative AI against the CCP. However, this focus on the threat is common for PLA writings, and this should not be exculpatory of potential future PLA embrace of generative AI for offensive purposes. The PLA

---

[16] Liu Huiyan [刘惠燕], Xiong Wu [熊武], Wu Xianliang [吴显亮], and Mei Shunliang [梅顺量], "Several Thoughts on Promoting the Construction of Cognitive Domain Operations Equipment for the Omni-Media Environment" ["全媒体环境下推进认知域作战装备发展的几点思考"], *National Defense Technology* [国防科技], Vol. 39, No. 5, October 2018.
[17] Nathan Beauchamp-Mustafaga and Jessica Drun, "Exploring Chinese Military Thinking on Social Media Manipulation Against Taiwan," *China Brief*, Vol. 21, No. 7, April 12, 2021.
[18] Sun Yixiang [孙亦祥] and Yu Yuanlai [余远来], "A Brief Discussion on 'Intelligentized Public Opinion Warfare'" ["刍议'智能化舆论战'"], *Military Correspondent* [军事记者], January 2022.
[19] "New Generation AI Development Plan," People's Republic of China State Council, July 20, 2017. Translation available via Graham Webster, Rogier Creemers, Elsa Kania, and Paul Triolo, "Full Translation: China's 'New Generation Artificial Intelligence Development Plan' (2017)," DigiChina, August 1, 2017.
[20] Marcellino et al., 2023.

is indeed already engaged in cyber-enabled IO and, at a minimum, these surveyed writings reveal an understanding by PLA researchers of generative AI's potential.[21] A more forward leaning article in June 2023 specifically argued that generative AI will make it easier to conduct offensive CDO because it enables broader scope and quicker operations that will thus make it easier to push one's desired narratives.[22] The article argues that "the improvement in deepfake technology brought by ChatGPT makes offensive operations in cognitive domain operations more covert" and will make it easier to "integrate offensive actions . . . into daily life."

PLA discussions of generative AI's potential for cyber-enabled IO mainly focus on the prospects for long-term subtle influence across several different tactics: influencing public opinion via large-scale bot networks, producing intentionally biased publicly available models, and specifically degrading support for adversary leadership.[23] First, the main tactic that PLA authors discuss to artificially influence public opinion is the prospect of running large-scale networks of social bots powered by automated content generation. For example, an April 2023 article coauthored by a leading researcher for the 28th Research Institute under the China Electronics Technology Group (CETC), which provides command-related systems to the PLA, argued that generative AI will enable

> nuanced, personalized content, and not only proactively post but also respond to other users' posts and engage in long-term conversations. Therefore, after social bots based on ChatGPT are instilled with personalities, positions and tendencies, they can become invisible on the Internet and become cognitive shaping tools. They are more influential and concealed than traditional [human-run] astroturfing [网络水军].[24]

This PLA interest in large-scale bot networks builds on PLA interest in social bots and manipulated content. At least two articles by PLA researchers explicitly call for PLA adoption of social bots, as one 2022 article said,

> In the face of Western countries taking the opportunity to smear and attack [us], we must have the courage to use social bots [社交机器人] to carry out public

---

[21] Office of the Secretary of Defense, 2023, p. 158.

[22] Chen Changxiao [陈昌孝], Li Hao [李浩], Wang Zihan [王梓晗], Jiang Wenbo [姜文博], "A New Weapon in Cognitive Domain Operations: ChatGPT Cognitive Analysis and Countermeasures" ["认知域作战新利器: ChatGPT 认知剖析及对策"], *Military Digest* [军事文摘], June 2023.

[23] Chen Dongheng [陈东恒] and Xu Yan [许炎], "Generative AI: A New Weapon for Cognitive Confrontation" ["生成式 AI: 认知对抗的新武器"], *PLA Daily*, April 4, 2023. For a similar argument, see Mao Weihao [毛炜豪], "Looking at the Military Applications of Artificial Intelligence from ChatGPT" ["从 ChatGPT 看人工智能的军事应用"], *PLA Daily*, April 13, 2023.

[24] Zhou Zhongyuan [周中元], Liu Xiaoyi [刘小毅], Li Qingwei [李清伟], "ChatGPT Technology and Its Impact on Military Security" ["ChatGPT 技术及其对军事安全影响"], *Command Information System and Technology* [指挥信息系统与技术], April 2023, pp. 7–16. The lead author self-plagiarized this article shortly after in Zhou Zhongyuan [周中元], "ChatGPT's Challenges to Military Security and Countermeasures" ["ChatGPT 对军事安全的挑战与应对策略"], *Defence Science & Technology Industry* [国防科技工业], July 2023, pp. 46–48. For related articles, see Chen et al., 2023; Hua Rui [华瑞], Yang Longxiao [杨龙霄], Yang Runxin [杨润鑫], "When Generative Artificial Intelligence Heads to the Battlefield" ["当生成式人工智能走向战场"], *PLA Daily*, December 1, 2023.

> opinion [struggle], and use relevant social bots to carry out information bombing [信息轰炸] against the enemy's social network to drown it out.[25]

PLA researchers have been interested in manipulated content since at least 2005 and manipulated video since at least 2011 and have more recently begun to specifically discuss deepfakes.[26] For example, one article explained that "generative AI can quickly generate or forge the appearance, voice, emotions, expressions, and other attributes of political targets" and that it can "generate personalized content based on the preferences of political targets," or even mobilize public opinion on a desire topic.[27]

Some PLA discussions focus on the prospects of generative AI for enabling "precision cognitive attacks" (精准认知攻击), specifically highly tailored or even personalized IO against small groups or individuals.[28] For example, one article noted that "ChatGPT's powerful data processing capabilities and high autonomy enable it to conduct preference analysis and subsequent related information production and information delivery," supporting "precision cognitive attacks" based on "personalized user portraits" using big data to analyze individual preferences.[29]

Another related method is creating or reinforcing "information cocoons" (信息茧房)—specifically, information bubbles—with the intention of undermining the influence of mainstream values, further polarizing and dividing society. One article acknowledges that the traditional approach before generative AI was costly, was easy to identify because it required seizing on existing trending topics, and, thus, was easy to defeat.[30] In comparison, ChatGPT greatly improves the efficiency because it is autonomous, cheaper, and quicker and can better distribute the desired content more subtly, making it harder to detect. As the article said, "ChatGPT's precision information delivery capabilities and crowd classification capabilities will effectively and efficiently promote the formation of various small groups."

---

[25] Long Yameng [龙亚蒙] and Zhou Yang [周洋], "Research on the Application of Social Bots in Public Opinion Struggle" ["社交机器人在舆 论斗争中的应用研究"], *Military Correspondent* [军事记者], 2022. See also Wu Xiaojian [武啸剑], "How Social Bots Manipulate Public Opinion in the Age of Intelligent Communication: An Analysis of Narrative and Cognition Under Crisis" ["危机下的叙事与认知: 智能传播时代社交机器人舆论干预研究"], *Journalism and Mass Communication* [新闻界], September 2023, pp. 88–96.

[26] For more, see Beauchamp-Mustafaga, 2023; Marcellino et al., 2023.

[27] Zhang Guangsheng [张广胜], "National Security Risks of Generative Artificial Intelligence and Countermeasures" ["生成式人工智能的国家安全风险及其对策"], *Frontiers* [人民论坛·学术前沿], July 2023, pp. 76–85. For another article linking generative AI with deepfakes, see Hu Kaiguo [胡开国], "When Generative Artificial Intelligence Plays a Role in War" ["当生成式人工智能作用于战争"], *Military Digest* [军事文摘], September 2023.

[28] This discussion of precision appears to be a popular concept in PLA IO circles. See Bu Jiang [卜江] and Jiang Rilie [蒋日烈], "How to Achieve Precision Strikes in Cognitive Domain Operations" ["如何实现认知域作战精准打击"], *PLA Daily*, March 16, 2023.

[29] Chen et al., 2023. The authors self-plagiarized this article to publish the same text shortly after in Chen Changxiao [陈昌孝] and Wang Zihan [王梓晗], "Characteristics, Application, and Countermeasures of ChatGPT from a Cognitive Perspective" ["认知视角下 ChatGPT 的特征、运用及应对之策", *Political Work Journal* [政工学刊], July 2023.

[30] Chen et al., 2023.

Second, another tactic discussed is the potential to covertly use a publicly available model, such as ChatGPT, to influence adversary public perceptions over time. Much of this discussion focuses on the risks of Western models, trained on Western data, being thus inherently biased toward Western values and surreptitiously inculcating users with Western values. As one article explained, ChatGPT will "widely penetrate into every corner of society," presenting opportunities to "subtly influence" users over time and "unknowingly change a person's cognitive logic and behavior."[31] Although I did not find any specific PLA writings calling for Beijing to develop its own open source models and intentionally building pro-CCP bias into them, a natural result of the CCP's current regulatory model of censoring political content for publicly available Chinese models is that they are very likely to hew, by design, toward CCP-approved narratives. This would represent a relatively new opportunity for Party-state IO, comparable perhaps only to Chinese-run social media platforms, such as WeChat and TikTok, which avoid takedowns of CCP disinformation and are vulnerable to CCP efforts to artificially push favored narratives.[32]

Third, PLA authors discuss the ability to degrade popular support for adversary leadership. As one article explained, "cognitive attacks" and "precision attacks against political targets" [精准攻击政治目标] are the "general trend of current hybrid warfare," based on "generative AI, cognitive neural methods, and social media" and provided as evidence U.S. efforts to leverage AI to "demonize" Nicolás Maduro in Venezuela, reflecting recent accusations by the Chinese Ministry of Foreign Affairs (MFA).[33] This aligns with longstanding PLA discussion of "public opinion decapitation" (舆论斩首), which the PLA views as a common U.S. tactic, as seen in the wars against Iraq and Libya.[34]

PLA researchers also acknowledge some shortcomings for generative AI. For example, in March 2023, Hu Xiaofeng, a famous PLA researcher, acknowledged that generative AI "should neither be underestimated nor overestimated" and has problems, such as challenges in training data, human confidence in the models, and lack of transparency, among other issues.[35] A similar list of issues has since been repeated by several other researchers.[36] Another article argued that "there are some more subtle things, including cultural symbols, historical allusions, the processing of ambiguity (such as puns), etc., which require high context information to help AI understand" and that generative AI "fictionalizes information."[37] However, in light of

---

[31] Chen et al., 2023. For another article, see Chen and Xu, 2023.
[32] See, for example, Sapna Maheshwari, "Topics Suppressed in China Are Underrepresented on TikTok, Study Says," *New York Times*, December 21, 2023.
[33] Zhang, 2023, pp. 76–85; Chinese Ministry of Foreign Affairs, "Fact Sheet on the National Endowment for Democracy," May 7, 2022.
[34] See Beauchamp-Mustafaga, 2023, p. 140.
[35] Hu Xiaofeng [胡晓峰], "How Should We View ChatGPT?" ["ChatGPT 我们该怎么看"], *PLA Daily*, March 21, 2023.
[36] Shen Zhengzheng [申峥峥] and Shu Zhe [束哲], "Generative AI: How Far Is It from Comprehensive Application in the Military Field" ["生成式人工智能: 距离军事领域全面应用有多远"], *PLA Daily*, April 14, 2023; Hua, Yang, and Yang, 2023.
[37] "Generative AI and Science Fiction Creation" ["生成式 AI 与科幻创作"], *PLA Daily*, May 24, 2023.

longstanding PLA complaints about poor foreign language capabilities and cross-cultural understanding, generative AI will almost certainly improve current PLA capabilities.[38]

Lastly, it is difficult to overstate the depth of concern held by PLA researchers about U.S. efforts to use generative AI to undermine CCP regime security. These concerns long predate the rise of AI, but AI's dramatically increased performance appears to have exacerbated these concerns. There is a widespread belief amongst PLA researchers that the U.S. government, often specifically the U.S. military, is either developing or has already deployed such capabilities and could, or already is, targeting them at Beijing. As DoD explains,

> From the PRC's perspective, all nations—especially the United States—that use digital narratives to undermine the CCP's authoritarian system in China employ offensive influence operations. Hence, the PRC considers its influence operations that counter this perceived subversion as defensive in order to protect the party and the military.[39]

For example, a July 2023 article argued that the U.S. government is working on an "influence machine" (影响力机器) that will "combine algorithm-generated content, personalized targeting, and intensive information dissemination" in order to "achieve [U.S.] political goals of corroding, infiltrating, influencing and subverting from inside [the target country] and discrediting, containing, and blocking from the outside [of the target country]."[40] These fears find validation in public reports of U.S. IO, which are frequently recounted in PLA writings.[41] Indeed, it is these concerns that are often used to justify Chinese efforts in response.[42]

This concern may be driven in part by fears of technological inferiority because at least initial Chinese appraisals acknowledged the U.S. lead in generative AI. For example, the April 2023 article by CETC researchers stated that

> [a]t present, domestic companies such as Baidu, ByteDance, and NetEase have accumulated relevant technologies and layouts, but in terms of technical capabilities, domestic experts judge that they are about 2 to 3 years behind ChatGPT. In the military industry, although relevant companies have

---

[38] See Beauchamp-Mustafaga, 2023, pp. 112–115.
[39] Office of the Secretary of Defense, 2023, p. 156.
[40] Zhang, 2023, pp. 76–85. For other recent concerns, see Ban Wentao [班文涛] and Xie Mingxiu [谢明修], "Three Reliances: Using Artificial Intelligence Technology to Innovate Public Opinion Warfare—Research and Enlightenment on the Application of Artificial Intelligence Technology to Public Opinion Warfare by the United States and Other Western Countries" ["三个依托: 利用人工智能技术创新舆论战: 美国等西方国家将人工智能技术应用于舆论战研究与启示"], *Military Correspondent* [军事记者], January 2023; Meng Haohan [孟浩瀚] and Lan Peixuan [兰培轩], "Strategies to Generate Capabilities in Public Opinion Warfare in the Cognitive Domain: Thoughts and Warnings Brought to Us by The Public Opinion Dissemination of American and Western media" ["认知域下舆论战的能力生成之策: 美西方媒体舆论传播带给我们的思考和警示"], *Military Correspondent* [军事记者], January 2023; Wang Hejing [王鹤静] and Wu Dan [吴丹], "Strategic Tactics of the U.S. Cyber Army" ["美国网军的战略战法"], *Military Digest*, July 2023.
[41] See, for example, Ellen Nakashima, "Pentagon Opens Sweeping Review of Clandestine Psychological Operations," *Washington Post*, September 19, 2022.
[42] See, for example, Long and Zhou, 2022.

> accumulated some experience in natural language processing technology, the relevant models and functions lag far behind those in the industry.[43]

This view might be outdated almost a year later, but it's an interesting data point from someone who is likely very familiar with PLA technical capabilities.

Current State of Chinese Adoption

Chinese Military

Despite the evident interest by PLA researchers, so far there is no direct evidence of specific PLA adoption to operationalize generative AI for cyber-enabled IO. This might simply be a limitation of open-source research or perhaps a reflection of slow adoption of this new technology, or it could suggest that the PLA has decided generative AI is not worth pursuing. One indication of a lack of apparent movement toward PLA development is the relative lack of publications so far on the topic by PLASSF researchers, who would likely support such efforts.[44]

Regardless, there are many reasons to believe that the PLA will be able to leverage generative AI for cyber-enabled IO if it so chooses. First, the PLA could leverage any one of the open-source LLMs available—including Falcon or the leaked version of Meta's LLaMA, or even OpenAI's services—because it almost certainly has the technical sophistication to circumvent the basic restrictions on users' Internet Protocol addresses. Second, China has a robust tech sector that is busily working on generative AI, with significant government support as part of its plan to lead the world in AI development by 2030. As of September 2023, there were an estimated 130 LLMs under development in China.[45] The inevitable political constraints imposed by the CCP will likely negatively affect the overall performance of Chinese models, but Chinese companies should not be counted out, and recent comparisons between top U.S. and Chinese models suggest relative improvement by Chinese models in the second half of 2023, although U.S. models still lead.[46] Moreover, the PLA will not need the best models, and certainly even the original version of ChatGPT would be more than adequate for the PLA's basic needs.

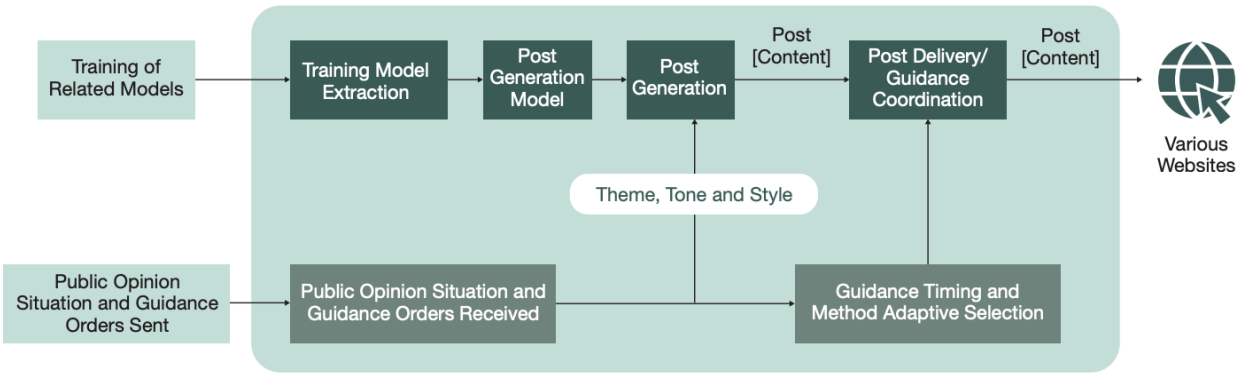
To better understand the potential of generative AI for the PLA, it is useful to explore the case study of Li Bicheng, a PLA-affiliated researcher who has focused on improving PLA cyber-

---

[43] Zhou, Liu, and Li, 2023, pp. 7–16.
[44] For one PLASSF article that recounts a familiar litany of issues but does not suggest research and development efforts, see Fu Xiang [付翔], Wei Xiaowei [魏晓伟], Zhang Hao [张浩], Xu Ning [徐宁], "Examining and Analyzing ChatGPT from the Perspective of Digital Security" ["数字安全角度下审视和剖析 ChatGPT"], *Aero Weaponry* [航空兵器], October 2023.
[45] Josh Ye, "China's AI 'War of a Hundred Models' Heads for a Shakeout," Reuters, September 21, 2023.
[46] "Chinese Large Model Benchmark Evaluation 2023 Annual Report" ["中文大模型基准测评 2023 年度报告"], SuperCLUE, December 31, 2023. For more on the political constraints on Chinese generative AI development, see Helen Toner, Jenny Xiao, and Jeffrey Ding, "The Illusion of China's AI Prowess: Regulating AI Will Not Set America Back in the Technology Race," *Foreign Affairs*, June 2, 2023.

enabled IO and is specifically working on how to leverage AI.[47] Li began designing a system for creating and distributing inauthentic content (disinformation) for "online public opinion struggle" by at least 2016, specifically calling for the ability to conduct "online information deception" and "online public opinion guidance."[48] In 2019, Li coauthored an article with a PLA researcher from Base 311 that focused on the applications of AI to overcome the PLA's current shortcomings that its "post [content] generation is mechanized without regard for personality, occupation, and age differences[, and] there is no individuality or simulation of human characteristics, so posts are easily identified and deleted."[49] Looking forward, Li essentially foresaw the rise of generative AI and its ability to support autonomous content generation and content delivery in an end-to-end system, illustrated in Figure 1. In light of this, at least some in the PLA are very likely ready to seize on generative AI's potential and could be working toward deployment outside the public eye.

Figure 1. PLA Researcher's Vision for AI-Driven Social Media Manipulation



SOURCE: Reproduced from Marcellino et al., 2023, p. 19. Originally adapted from Li Bicheng [李弼程], Xiong Yao [熊尧], Huang Tao [黄涛], and Pan Le [潘乐], "Simulation Deduction Model and System Construction for Intelligent Online Public Opinion Guidance" ["网络舆论智能引导仿真推演模型与系统构建"], *National Defense Technology* [国防科技], October 2020.

One potential key variable for PLA adoption of generative AI is likely to be the political pressures on the output from generative AI.[50] Chinese experts recognize that generative AI can produce either factually incorrect or political unacceptable outputs; some experts have recounted asking ChatGPT about the origins of COVID-19 only to find that it (accurately) answered

[47] For more, see Marcellino et al., 2023. After spending his entire career at PLA research institutions, Li no longer claims an affiliation with the PLA and is a professor at Huaqiao University. However, he continues to coauthor with PLA researchers and continues to receive PLA funding for his research, suggesting continued ties.
[48] Li Bicheng [李弼程], "Model for a System of Online Public Opinion Struggle and Countermeasures" ["网络舆论斗争系统模型与应对策略"], *National Defense Technology* [国防科技], October 2016.
[49] Li Bicheng [李弼程], Hu Huaping [胡华平], and Xiong Yao [熊尧], "Intelligent Agent Model for Online Public Opinion Guidance" ["网络舆情引导智能代理模型"], *National Defense Technology* [国防科技], June 2019.
[50] For more consideration, see Marcellino et al., 2023.

"China."[51] Given the apparent political constraints placed on Chinese IO (even Chinese covert foreign IO) to ensure that they ultimately fall within CCP-acceptable talking points, it is possible that the PLA and other Party-state actors will shy away from embracing generative AI for fear of internal backlash. Alternatively, these actors could spend additional time and energy on developing a politically reliable series of models that they could then leverage, but this is very likely to negatively affect the overall performance of the models.

There are two important caveats for this discussion of Chinese military cyber-enabled IO against Taiwan. First, the PLA is almost certainly one of many Party-state actors involved in cyber-enabled IO, although I assume the PLA is a relatively high performer based on its overall level of technical sophistication and general lack of attribution. Other Party-state actors that are likely involved include the CCP Propaganda Department, the MFA, the Ministry of State Security (MSS), the Ministry of Public Security, the Cyberspace Administration of China, and the United Front Work Department.[52] Second, social media manipulation is only one of many ways that Beijing can interfere in Taiwanese politics and broader society.[53]

In terms of what is known about past PLA cyber-enabled influence efforts, we have a very limited understanding because attribution to specific PRC actors is very difficult.[54] In 2016, Taiwan essentially accused the PLA Air Force of disinformation for posting a photo of Chinese bombers flying close enough to Taiwan to take a picture with what was suspected to be Jade Mountain.[55] Most notably, Taipei also specifically blamed the PLASSF for interfering with its 2018 election via social media, although it did not provide any specific public evidence.[56] In this case, the effectiveness is very uncertain, although available public evidence suggests that China's overall efforts in 2020 yielded minimal results.[57]

Broader Chinese Party-State

Our best understanding of Chinese Party-state efforts at cyber-enabled IO suggests growing effectiveness after previously middling performance and that this improvement might be at least partly due to adoption of generative AI. In an April 2023 review of publicly available reporting, the Australian Strategic Policy Institute (ASPI) found that PRC "operations are now more frequent, increasingly sophisticated and increasingly effective in supporting the CCP's strategic

---

[51] Zhou, Liu, and Li, 2023, pp. 7–16.
[52] Albert Zhang, Tilla Hoja, and Jasmine Latimore, *Gaming Public Opinion: The CCP's Increasingly Sophisticated Cyber-Enabled Influence Operations*, Australian Strategic Policy Institute, April 2023.
[53] Ben Blanchard, "Taiwan Says China Has 'Very Diverse' Ways of Interfering in Election," Reuters, October 4, 2023. For a recent broader examination of CCP IO, see U.S.-China Economic and Security Review Commission, "Hearing on 'China's Global Influence and Interference Activities,'" March 23, 2023.
[54] For the most recent U.S. government report on the topic, see Global Engagement Center, *How the People's Republic of China Seeks to Reshape the Global Information Environment*, U.S. Department of State, September 2023. For a good nongovernmental roundup, see Zhang, Hoja, and Latimore, 2023.
[55] Matthew Strong, "Military Denies Yushan in China Bomber Picture," *Taiwan News*, December 17, 2016.
[56] Chung Li-hua and William Hetherington, "China Targets Polls with Fake Accounts," *Taipei Times*, November 5, 2018.
[57] Aaron Huang, *Combatting and Defeating Chinese Propaganda and Disinformation: A Case Study of Taiwan's 2020 Elections*, Harvard Kennedy School Belfer Center for Science and International Affairs, July 2020.

goals. They focus on disrupting the domestic, foreign, security and defence policies of foreign countries, and most of all they target democracies."[58] The authors find that "[t]he CCP has developed a sophisticated, persistent capability to sustain coordinated networks of personas on social-media platforms to spread disinformation, wage public-opinion warfare and support its own diplomatic messaging, economic coercion and other levers of state power."[59] They continue that "[t]hose efforts have evolved to nudge public opinion towards positions more favourable to the CCP and to interfere in the political decision-making processes of other countries. A greater focus on covert social-media accounts allows the CCP to pursue its interests while providing a plausibly deniable cover."[60]

To date, there have been two nongovernment public reports and one foreign government report that suggest that the Chinese Party-state is beginning to adopt generative AI for cyber-enabled IO, reinforcing concerns outlined in recent RAND research about the ease of adoption for malign actors.[61] In September 2023, Microsoft reported that "[s]ince approximately March 2023, some suspected Chinese IO assets on Western social media have begun to leverage generative artificial intelligence (AI) to create visual content. This relatively high-quality visual content has already drawn higher levels of engagement from authentic social media users."[62] However, this appears to be more likely early, small-scale experimentation rather than reflect rapid broader adoption by known Party-state actors. More recently in December 2023, an ASPI report identified a "new campaign (which ASPI has named 'Shadow Play') [that] has attracted an unusually large audience and is using entities and voice overs generated by artificial intelligence (AI) as a tactic that enables broad reach and scale."[63] The report explained that the "coordinated inauthentic influence campaign originat[ed] on YouTube [and promotes] pro-China and anti-US narratives in an apparent effort to shift English-speaking audiences' views of those countries' roles in international politics, the global economy and strategic technology competition."[64] The campaign reportedly employed text-to-image and likely text-to-speech generative models to generate thumbnails and voiceovers for their videos, respectively. The ASPI report states that "the YouTube campaign is one of the first times that video essays, together with generative AI voiceovers, have been used as a tactic in an influence operation."[65] Most recently, Taiwanese officials claimed that the MSS was producing videos with "artificial intelligence (AI)-generated voiceovers and fake hosts," targeting President Tsai Ing-wen in the lead-up to Taiwan's January

[58] Zhang, Hoja, and Latimore, 2023, p. 1.
[59] Zhang, Hoja, and Latimore, 2023, p. 3.
[60] Zhang, Hoja, and Latimore. 2023, p. 1.
[61] Marcellino et al., 2023.
[62] Microsoft Threat Intelligence, *Sophistication, Scope, and Scale: Digital Threats from East Asia Increase in Breadth and Effectiveness*, Microsoft, September 2023, p. 6.
[63] Jacinta Keast, *Shadow Play: A Pro-China Technology and Anti-US Influence Operation Thrives on YouTube*, Australian Strategic Policy Institute, December 2023, p. 3.
[64] Keast, 2023, p. 3.
[65] Keast, 2023, p. 4.

2024 elections, validating earlier concerns, but that the campaign reportedly failed to garner much traction online.[66]

Regardless of foreign assessments of previous PRC IO efforts, the fact that Beijing continues to invest money, time, and resources into this behavior suggests that Beijing believes it is a worthwhile endeavor. This might be because Chinese propagandists believe that their overt public diplomacy and propaganda efforts are so poorly received that any covert efforts are helpful. It could also be that bureaucratic politics and Xi Jinping's centralization of power is driving Party-state IO efforts: Everyone is trying to please Xi and wasting money at ineffective efforts because that is what they think Xi wants, or because it allows them to argue to Xi that they are working toward his goals. Recent evidence that Chinese IO efforts are gaining more traction online suggest that the United States and other like-minded countries should not become complacent and should instead work to counter these activities.

What Generative AI Could Do for PLA Cyber-Enabled Influence Operations

Generative AI, as evident in the PLA writings surveyed above, is likely to improve existing overarching IO objectives and tactics, including in a conflict with the United States over Taiwan. I authored a recent RAND report that provides more detail on Chinese psychological warfare objectives, which very likely overlap with CDO: "degrading adversary decisionmaking, weakening adversary will to fight, undermining adversary support for war, undermining adversary government from within, along with supporting deterrence."[67] The report similarly details some relevant combat methods: "propaganda for persuasion, emotional manipulation, sowing discord, driving defections, as well as achieving deterrence and deception through psychological means."[68] Generative AI has the potential to improve PLA performance for all these objectives.

Specifically considering Chinese social media manipulation against Taiwan, the other recent RAND report forecast some potential changes under generative AI adoption, which is provided in Table 1 in an appendix at the end of this testimony.[69] For example, Beijing may be less interested in buying the accounts or otherwise bribing Taiwanese influencers to push pro-China narratives because generative AI would enable Beijing to create better viral content on its own. Beijing could also ramp up swarming—namely, creating content for spamming online discussions, such as comments or hashtags, like what Beijing has done on Xinjiang content.[70]

---

[66] Tsai Yung-yao and Jonathan Chin, "China Is Posting Fake Videos of President: Sources," *Taipei Times*, January 11, 2024; Shelley Shan, "China Might Use AI to Sow Chaos: NSB," *Taipei Times*, April 27, 2023.
[67] Beauchamp-Mustafaga, 2023, p. 12.
[68] Beauchamp-Mustafaga, 2023, p. 13.
[69] Marcellino et al., 2023.
[70] Global Engagement Center, "PRC Efforts to Manipulate Global Public Opinion on Xinjiang," U.S. Department of State, August 24, 2022; Global Disinformation Index, "Suspicious Twitter Hashtag Networks Promote Pro-China Line on Treatment of Uyghurs in Xinjiang," October 27, 2021.

Understanding Chinese Intent for U.S. Election Interference

There is growing concern by the U.S. government and broader national security community about the risks of Chinese election interference in the upcoming U.S. elections in November 2024. As the Office of the Director of National Intelligence (ODNI) said in its 2023 *Worldwide Threat Assessment*, "Beijing largely concentrates its U.S.-focused influence efforts on shaping U.S. policy and the U.S. public's perception of China in a positive direction, but has shown a willingness to meddle in select election races that involved perceived anti-China politicians."[71] This interference is not just at the federal level but also the subnational level: "Beijing has adjusted by redoubling its efforts to build influence at the state and local level to shift U.S. policy in China's favor because of Beijing's belief that local officials are more pliable than their federal counterparts."[72] This concern is furthered by a recently declassified U.S. National Intelligence Council (NIC) report on the 2022 U.S. elections that states that "China tacitly approved efforts to try to influence a handful of midterm races involving members of both U.S. political parties" and by nongovernment reports that such efforts continued into 2023.[73]

PLA research provides insights into how China may be targeting its election interference efforts. A 2021 article by PLA researchers from the National University of Defense Technology and PLASSF represented what was likely a proof of concept effort to use the social media activity of U.S. politicians to predict their favorability toward China.[74] The researchers used the activity of 21 high-profile U.S. politicians—including then-sitting senior officials in the Trump administration—on the X platform (formerly known as Twitter) as the training data to teach multiple deep learning models and then applied the models to predict the views of 20 then-sitting U.S. senators and governors, categorizing them into four U.S. political factions.[75] The researchers concluded that a fine-tuned pretrained Bidirectional Encoder Representations from Transformers (BERT) model performed best and then had "intelligence analysts" validate their assessments of individual U.S. politicians. The authors explained the value of their research as

---

[71] ODNI, *Annual Threat Assessment of the U.S. Intelligence Community*, February 6, 2023, p. 10.
[72] ODNI, 2023, p. 10.
[73] NIC, *Foreign Threats to the 2022 U.S. Elections*, December 23, 2022, declassified on December 11, 2023, p. i. This aligns with earlier nongovernment research. See, for example, Alden Wahlstrom, Jess Xia, Alice Revelli, and Ryan Serabian, "Information Operations Targeting 2022 U.S. Midterm Elections Include Trolling, Narratives Surrounding Specific Races, Politicians," Mandiant, December 19, 2022. For nongovernment reports since 2022, see Microsoft Threat Intelligence, 2023; Ben Nimmo, Nathaniel Gleicher, Margarita Franklin, Lindsay Hundley, and Mike Torrey, *Q3 2023 Adversarial Threat Report*, Meta, November 2023.
[74] Chang Chengyang [常城扬], Wang Xiaodong [王晓东], and Zhang Shenglei [张胜磊], "Polarity Analysis of Dynamic Political Sentiments from Tweets with Deep Learning Method" ["基于深度学习方法对特定群体推特的动态政治情感极性分析"], *Data Analysis and Knowledge Discovery* [数据分析与知识发现], Vol. 51, No. 3, May 2021, pp. 121–132. The authors' own translation is available in Chang Chengyang and Wang Xiaodong, "Research on Dynamic Political Sentiment Polarity Analysis of Specific Group Twitter Based on Deep Learning Method," *Journal of Physics: Conference Series*, 2020. Zhang is from the PLASSF Space Systems Department. This article was previously discussed with the commission by John Chen (John Chen, "Testimony Before the U.S.-China Economic and Security Review Commission," Hearing on "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States," February 17, 2022).
[75] The authors claim to more broadly also analyze 75 then-sitting U.S. senators and representatives, as well as 39 governors, suggesting a broader ambition.

"to assist intelligence analysts in their assessment of U.S. political inclinations and future paths for U.S.-China relations," by "using multiple types of deep learning technologies . . . to obtain relatively accurate dynamic political sentimental polarity from huge volumes of Twitter text data."[76]

To put it plainly, this research appears specifically targeted toward identifying politicians that might be favorable to China so that the PRC can support them, or likewise oppose politicians that they deem as anti-China. Indeed, this matches the NIC's assessment that "PRC intelligence officers, diplomats, and other influence actors probably viewed some election influence activities as consistent with Beijing's standing guidance to counter U.S. politicians viewed as anti-China and to support others viewed as pro-China."[77] This 2021 PLA article provides the first open-source evidence of how at least some Chinese Party-state actors could be leveraging social media not just to engage in IO but also to identify preferred candidates to support or oppose specifically for election interference. It also suggests that at least some in the PLA were considering such activities by at least 2020.

Implications and Recommendations for U.S. Policymakers

The PLA is one of China's premier actors for cyber-enabled IO already, and its adoption of generative AI would very likely improve its ability further while complicating detection and thus attribution. Furthermore, given CCP emphasis on the development of AI capabilities in general, the question is not whether the PLA will adopt generative AI in its cyber operations but how quickly and successfully it will integrate this capability. It is important to understand that Party-state actors, including the PLA, do not need to have access to *the best, cutting-edge* generative AI models to improve their cyber-enabled IO, making adoption and employment even easier. Lastly, the scope and ambition of PLA IO should be understood to likely go beyond mere military activities, such as deterrence and degrading adversary will to fight, to include foreign election interference.[78] In light of this fact, U.S. policymakers could consider the following recommendations.

Risk Reduction

Require social media platforms to label generative AI content and redouble their efforts to combat fake accounts. At a minimum, social media platforms could require users to label their own content as generated using AI. Ideally, social media platforms would lead the development of detection tools to automatically label uploaded content as appropriate. This could apply to all content on their platforms, not just political advertising.

---

[76] Chang, Wang, and Zhang, 2021.
[77] NIC, 2022, p. i.
[78] The PLA was also reportedly involved in previous efforts targeting U.S. elections. See David Jackson and Lena H. Sun, "Liu's Deals with Chung: An Intercontinental Puzzle," *Washington Post*, May 24, 1998; David Johnston, "Committee Told of Beijing Cash for Democrats," *New York Times*, May 12, 1999.

Invest in capabilities to detect generative AI-produced content, understanding that this technology will likely be a long-term investment. Although there are a growing number of tools available that claim to detect AI-generated content, tests suggest that their actual performance is inconsistent at best. However, the U.S. government should not adopt a fatalistic acceptance of the proliferation of such content and should instead invest widely in potential counters, with the goal that detection capabilities eventually catch up and surpass generative AI production. The U.S. government can also engage the private sector to support public-private collaboration. Congress could take a specific role by allocating dedicated resources to appropriate agencies' budgets and funding studies on the topic.

Promote Media Literacy and Government Trustworthiness

Mandate better media literacy training for U.S. government employees to identify inauthentic content and, especially, generative AI content. It is important for U.S. government employees to ensure that they are accessing accurate information, and generative AI makes this more challenging. This is especially true for national security agencies during a crisis or conflict, so preparations now by improving media literacy is very important. Congress could specifically take a role by incorporating this emphasis on training into relevant legislation.

Similarly, support media literacy for citizens' ability to recognize inauthentic content. The U.S. government can encourage broader educational initiatives to make the United States more resilient in the long-term against malign influence operations. Congress could specifically take a role by engaging with local organizations and constituents as part of constituent outreach, as well as by funding government agencies to similarly support such outreach.

Support blockchain, watermarking, or other similar technologies for media to improve the trustworthiness of authentic media, especially U.S. government public statements. If it is currently difficult to identify AI-generated content, then another approach would be to clarify the trustworthiness of important media. This could be pursued by the private sector, but at a minimum, the U.S. government should consider adoption if this proves promising. If this approach proves promising, then Congress could be an early adopter to ensure credible communication with constituents and the broader public.

Public Reporting

Commit now to releasing a nonpartisan declassified assessment by the U.S. intelligence community following the U.S. 2024 election. Given the heightened public attention to foreign election interference this year and the risks of politicalization, it will be very important to provide as much transparency as possible about the integrity of U.S. elections. The recent declassification of the NIC's 2022 report is useful but arguably too slow, given that it took over a year to release publicly.

Publish a yearly, dedicated report on foreign malign actors' efforts to influence U.S. public opinion, including via social media. The U.S. government's current reactive and selective approach to addressing foreign efforts risks inconsistency and incompleteness. A yearly report by the U.S. intelligence community or State Department's Global Engagement Center, modeled on the annual *Worldwide Threat Assessment*, would provide more details to the public

about foreign efforts and help baseline actual foreign activity over time for public discussions. This could also include specific sections focused on adoption of generative AI.

Take a more active approach to publicly calling out Chinese cyber-enabled influence operations, when attribution is available. There is certainly a balance between forcefully identifying malign activity by hostile actors versus calling more attention to their activities in the process, and the U.S. government can consider how to best weigh these trade-offs. Congress could specifically take a more proactive role by asking relevant executive branch officials about recent trends in malign activity during public hearings on a regular basis.

Diplomatically

Encourage Taiwan to increase its information-sharing, both publicly and privately, about Chinese cyber-enabled influence operations. This includes Taipei releasing a declassified report about Chinese efforts against their recent January 2024 election. Congress could take a role via its interactions with Taiwan interlocutors and also by encouraging the U.S. Department of State and other relevant government agencies to emphasize this interest in their own interactions.

Support Taiwan's engagement with other democracies to share its lessons learned and best practices combating Chinese IO. As Chinese efforts turn more global, Taipei is well-positioned to support other democracies as they work to counter Chinese malign influence, and Washington is crucial to providing appropriate platforms for such engagement. One option is the Global Cooperation and Training Framework, which provides opportunities for Taiwan to share its expertise on global issues of concern with other interested countries. Congress could take a role by supporting outreach to other global legislatures and elected officials.

Engage with allies and partners about the risks of Chinese cyber-enabled IO and cooperate on response options. This can include sharing information, publicly or privately, about Chinese malign activities, as well as sharing best practices on how to mitigate and respond to this growing threat.

Engage in dialogue with China on AI-driven social media manipulation. Despite the challenges of engaging Beijing in Track 1 or even Track 2 dialogue these days, it is worth considering whether there is any room for cooperation on limiting the adoption of generative AI for malign purposes. In October 2023, the Chinese MFA released its proposal for a "Global AI Governance Initiative" that specifically said that Beijing "[opposes] using AI technologies for the purposes of manipulating public opinion, spreading disinformation, intervening in other countries' internal affairs, social systems, and social order, as well as jeopardizing the sovereignty of other states."[79] Although this is a blatant lie, it provides an opportunity to begin a dialogue with Beijing, with the hope of reaching an agreement against such uses of generative AI.[80] The agreement on beginning a U.S.-China dialogue on AI, reached between President

---

[79] Chinese Ministry of Foreign Affairs, "Global AI Governance Initiative," October 20, 2023.
[80] Nathan Beauchamp-Mustafaga, "Biden Should Call China's Bluff on Responsible AI to Safeguard the 2024 Elections," *RAND Blog*, November 14, 2023, https://www.rand.org/pubs/commentary/2023/11/biden-should-call-chinas-bluff-on-responsible-ai-to.html.

Biden and General Secretary Xi Jinping in November 2023, lays this foundation, although it appears the current focus overlooks IO as a potential topic for inclusion.[81] Understanding that Beijing may well violate this agreement like it has in the past, a bilateral agreement would at least empower the United States to hold Beijing accountable publicly and better engage with allies and partners on the topic.

Additional Research

Fund additional research on Chinese strategy for cyber-enabled influence operations, including the PLA's CDO operational concept. There is very limited high-quality understanding of Chinese strategies, capabilities, and intentions, and public discussion would benefit from additional information on the topic.

Conduct an independent assessment of the net benefit of U.S. government information efforts. This could include DoD and other relevant agencies. At DoD, for example, this review could ensure that all DoD messaging—whether by combatant commands or others—aligns with stated DoD strategic priorities and relevant strategic messaging. The review could also consider whether U.S. activities against one adversary produced sufficient benefits weighed against potential downsides in behavior from other adversaries. Given the risk that Chinese observations of U.S. activities are driving Chinese malign activities, compared with an uncertain benefit from such U.S. activities, it is worth considering the net value.

Fund additional research evaluating the risk of malign influence operations presented by generative AI models from Chinese companies. Because this is a novel risk and currently uncertain, it is worth further consideration.

[81] Graham Webster and Ryan Haas, "A Roadmap for a US-China AI Dialogue," Brookings Institution, January 10, 2024.

Appendix. Potential Implications of Generative AI for PRC Social Media Manipulation Against Taiwan

Table 1. Potential Implications of Generative AI for PRC Social Media Manipulation Against Taiwan

Common PRC Tactic	Definition	Previous Shortcoming	Potential Implication with Generative AI
Advertising	Paid promotional content to support a cause or actor	PRC paid Taiwan influencers to promote pro-CCP content, but they sometimes were easy to identify with blatant one-off messages	May diminish; PRC no longer needs to pay others to create viral content if it is able to generate convincing, authentic text
Bots for astroturfing	Using large numbers of inauthentic (fake) accounts (bots) to create the appearance of a broad consensus on a topic	PRC has largely relied on human-generated comments, limiting quality and scale	Likely to increase dramatically; generative AI will give bots written voices that are near-indistinguishable from human-created content
Cheapfakes and recontextualized media	Supporting a campaign either with simple edits or by repurposing media (usually, images)	PRC attempts are relatively easy to identify and slow enough for Taiwan government to expose and debunk	May diminish; realistic, highly believable fakes will be far cheaper to make en masse and may not be able to be identified or may overwhelm Taiwan government response capabilities
Impersonation	Pretending to be another person in order to misrepresent their position or views	PRC relies on pressuring public individuals into creating misleading information (especially, confessions)	Now possible to (1) mass-generate text in the style of a given individual's writing (2) falsify images of an individual and produce those images en masse. There is no longer a need to actually coerce a targeted individual
Keyword squatting	Creating mass content to manipulate search engine results related to a given term, phrase, or hashtag	Past PRC campaigns on Xinjiang issues have lacked variety, making them easier to detect	Generative AI does not revolutionize keyword squatting's mechanism but permits squatters to automate mass content generation containing a given keyword
Swarming	Loosely organized groups coordinating to fill an information space (e.g., spamming a comment section)	50 Cent Army members are inconsistent in their ability to avoid detection or achieve specific narrative goals	Generative AI automates the process of creating mass unique content for spamming a comment section or otherwise drowning out a narrative

Common PRC Tactic	Definition	Previous Shortcoming	Potential Implication with Generative AI
Testimonials	Personal stories used to elicit emotional reactions or sway opinions	PRC manufactured testimonials have historically been presented on state media and appear to be relatively scripted	Generative AI is capable of writing short-form and long-form testimonials of wide-ranging content on a mass scale, representing various demographics for both broad and niche effects

SOURCES: Reproduced from Marcellino et al., 2023, p. 22. Originally adapted from Harvard Kennedy School Shorenstein Center for Media, Politics, and Public Policy, *The Media Manipulation Casebook Code Book*, version 1.4, updated January 7, 2022; Aaron Huang, *Combatting and Defeating Chinese Propaganda and Disinformation: A Case Study of Taiwan's 2020 Elections*, Harvard Kennedy School Belfer Center for Science and International Affairs, July 2020.

OPENING STATEMENT OF EDWARD PARKER, PHYSCIAL SCIENTIST, RAND CORPORATION

DR. PARKER: Co-Chair Helberg and Co-Chair Wessel, thank you for inviting me to testify before the Commission today. Quantum information science and technology has been recognized as a strategically important emerging technology by the highest levels of leadership within both the United States and the PRC governments. Most quantum technology applications are still early stage and there are still many unknowns regarding which ones will eventually prove useful.

But in the long run, quantum technology could greatly improve our capabilities to collect, process, and transmit information with significant implications for both national security and economic prosperity. Specific potential applications relevant to national security include positioning, navigation, and timing without GPS, material science, and decryption.
Quantum science is a highly international enterprise.

So focusing on the industrial bases of individual nations does not capture the complete picture. That having been said, the United States and China are the two clearly leading nations in quantum technology R&D by most relevant metrics, including patenting, scientific publishing, and demonstrated prototype systems. To summarize a complex story, I would say that of the three main quantum technology areas, the United States leads the world in two, quantum computing and quantum sensing, while China leads in the world in one, quantum communications.

But the two nations' governments appear to be pursuing somewhat different R&D priorities, so it is difficult to directly compare their progress. For example, the PRC has invested heavily in a technology known as quantum key distribution that the U.S. government has publicly identified as a low priority.

Overall, I'd say that for the most important national security applications of quantum technology, Chinese scientists are impressively fast followers but are rarely at the true forefront of innovation. The United States has the good fortune to lead in almost all of the most important areas of quantum technology. Moreover, it has a huge advantage that the PRC does not, a network of close alliances with many of the other leading nations in the field.

Neither country's military appears to have integrated any quantum technology other than atomic clocks into actual operational systems. But the U.S. military has begun field testing quantum inertial sensors and clocks in operational environments. That having been said, Chinese researchers appear to be fairly close behind in a few important areas such as superconducting quantum computing.

And there is a long road ahead. The highest impact quantum technology applications are probably still at least a decade away. So U.S. policy makers should not get complacent because there's still plenty of time for global technology leadership to change hands.

At the same time, I'd caution against framing quantum technology development in entirely zero-sum terms. The U.S. and China are each other's strongest research collaborators in quantum science and valuable scientific information and talent flows in both directions. The Biden administration recently issued an executive order restricting U.S. outbound financial investments in Chinese quantum technology firms.

I am not aware of any U.S. firms currently investing in Chinese quantum technology companies or considering doing so. Moreover, private industry plays a relatively small role in the Chinese quantum technology ecosystem. Most development there occurs in national laboratories.

So I suspect that the executive order will have little impact on Chinese quantum R&D efforts in the near term. I'd like to conclude with a few thoughts regarding steps that the U.S. government could take to help ensure continued U.S. strength in quantum technology. If Congress determines that this technology should be a strategic priority, then the most important step toward that goal would be to continue to invest in fundamental science research.

Another important step would be to strengthen the U.S. skilled workforce, including both the domestic and the foreign pipelines of skilled talent while ensuring that appropriate protections against intellectual property loss are in place. Also, broad export controls on quantum technology would run the risk of slowing scientific progress and stifling a nascent commercial industry. I believe that narrowly targeted export controls on specific Chinese organizations of concern are low risk.

But Congress should carefully consider the impacts on the U.S. commercial industry of any proposed broad export controls on quantum technology unless those export controls are directly tied to a concrete military capability. Finally, there are three aspects of the emerging quantum technology ecosystem that the U.S. government should consider understanding and monitoring: the financial health of quantum technology companies, the flows of skilled talent and intellectual property between the U.S. and competitor nations, and the supply chain for critical components and materials. I do not see any clear needs for immediate action regarding these topics, but all three of them represent potential risks to the long-term stability of the quantum -- emerging quantum ecosystem. Thank you. I look forward to taking your questions.

PREPARED STATEMENT OF EDWARD PARKER, PHYSCIAL SCIENTIST, RAND CORPORATION

Testimony

EDWARD PARKER

The Chinese Industrial Base and Military Deployment of Quantum Technology

CT-A3189-1

Testimony presented before the U.S.-China Economic and Security Review Commission at the hearing "Current and Emerging Technologies in U.S.-China Economic and National Security Competition" on February 1, 2024

For more information on this publication, visit **www.rand.org/t/CTA3189-1**.

Testimonies

RAND testimonies record testimony presented or submitted by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies.

Published by the RAND Corporation, Santa Monica, Calif.

Limited Print and Electronic Distribution Rights

The Chinese Industrial Base and Military Deployment of Quantum Technology

Testimony of Edward Parker[1]
The RAND Corporation[2]

Before the U.S.-China Economic and Security Review Commission at the hearing "Current and Emerging Technologies in U.S.-China Economic and National Security Competition"

February 1, 2024

Co-chair Helberg and co-chair Wessel, the governments of both the United States and the People's Republic of China (PRC) consider quantum science and technology to be strategically important for ensuring their respective countries' economic and military leadership. In the United States, quantum science has been a priority area for federal research and development (R&D) for both the previous and current administrations, and the passage of the bipartisan National Quantum Initiative Act (Pub. L. 115-368) in 2018 significantly increased U.S. government funding and coordination in this area.[3] National Security Advisor Jake Sullivan has identified quantum technology as one of a few technologies that he believes "will be of particular importance over the coming decade."[4] In China, President Xi Jinping held a group study session of the Chinese Communist Party Politburo dedicated to quantum science, in which he stated that "developing quantum science and technology is of great scientific and strategic significance."[5] The PRC is also investing huge resources into quantum science R&D.

---

[1] The opinions and conclusions expressed in this testimony are the author's alone and should not be interpreted as representing those of the RAND Corporation or any of the sponsors of its research.

[2] The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND's mission is enabled through its core values of quality and objectivity and its commitment to integrity and ethical behavior. RAND subjects its research publications to a robust and exacting quality-assurance process; avoids financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursues transparency through the open publication of research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. This testimony is not a research publication, but witnesses affiliated with RAND routinely draw on relevant research conducted in the organization.

[3] Public Law 115-368, National Quantum Initiative Act, December 21, 2018.

[4] The White House, "Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit," September 16, 2022.

[5] Zhang Zhihao, "Xi Highlights Crucial Role of Quantum Tech," China Daily, October 19, 2020.

I would like to begin with the caveat that there is very high international collaboration in quantum science research.[6] For example, most quantum science research produced by U.S. scientists is coauthored with foreign collaborators. In fact, the United States and China are each other's largest scientific collaborators.[7] Therefore, discussing nations' quantum industrial bases in isolation does not capture the complete picture.

That having been said, by most relevant metrics, the United States and China are clearly the two leading nations in quantum science and technology. They each produce far more public scientific research and patenting in this area than any other nation.[8] They probably invest far more government funding into quantum R&D as well, although China has produced widely conflicting public numbers for its investment levels, so reliable numbers are hard to come by.[9] The United States and China have also publicly demonstrated the world's most-impressive specific technical achievements.

Comparison of Scientific Achievements and Priorities

The U.S. government has produced a public national strategy for quantum science,[10] as well as more detailed reports on specific subareas.[11] To my knowledge, the PRC government has not, and its overall priorities, plans, and timelines for integrating quantum technology into operational military systems are much less clear than those of the U.S. government. Nevertheless, we can draw some tentative conclusions from Chinese public scientific activity.

Quantum science is a dual-use technology; it has both military and civilian-commercial applications.[12] It is often divided into three subfields that each have potential military applications:

---

[6] Edward Parker, Richard Silberglitt, Daniel Gonzales, Natalia Henriquez Sanchez, Justin Lee, Lindsay Rand, Jon Schmid, Peter Dortmans, and Christopher A. Eusebi, *An Assessment of U.S.-Allied Nations' Industrial Bases in Quantum Technology*, RAND Corporation, RR-A2055-1, 2023, https://www.rand.org/pubs/research_reports/RRA2055-1.html.

[7] Edward Parker, Daniel Gonzales, Ajay K. Kochhar, Sydney Litterer, Kathryn O'Connor, Jon Schmid, Keller Scholl, Richard Silberglitt, Joan Chang, Christopher A. Eusebi, and Scott W. Harold, *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology*, RAND Corporation, RR-A869-1, 2022, https://www.rand.org/pubs/research_reports/RRA869-1.html.

[8] Parker et al., 2023.

[9] Parker et al., 2022.

[10] Subcommittee on Quantum Information Science, Committee on Science, National Science and Technology Council, "National Strategic Overview for Quantum Information Science," September 2018.

[11] Subcommittee on Quantum Information Science, Committee on Science, National Science and Technology Council, "A Coordinated Approach to Quantum Networking Research," January 2021; Subcommittee on Quantum Information Science, Committee on Science, National Science and Technology Council, *Bringing Quantum Sensors to Fruition*, March 2022.

[12] Edward Parker, *Commercial and Military Applications and Timelines for Quantum Technology*, RAND Corporation, RR-A1482-4, 2021, https://www.rand.org/pubs/research_reports/RRA1482-4.html.

1. *Quantum sensing* could improve positioning, navigation, and timing (PNT) capabilities and robust communications in challenging (e.g., GPS-denied) environments, as well as long-distance sensing capabilities.
2. *Quantum computing* could improve military logistics, modeling and simulation, scientific research, and codebreaking capabilities.
3. *Quantum communications* could improve the security of communications against enemy interception.

My high-level summary assessment of the Chinese quantum innovation ecosystem is that Chinese researchers are impressively fast followers across many quantum technology areas, but are rarely at the true forefront of innovation. The one exception is quantum communications, in which Chinese researchers are the world leaders.[13] But even in that subfield, they have significantly different R&D priorities from the United States, and so the two nations are not necessarily in direct technical competition over the same applications. A more detailed discussion follows.

Quantum Sensing

Chinese scientists publish slightly less high-impact research in quantum sensing than U.S. scientists do, and the foremost Chinese quantum scientist has admitted that "there is a gap" between the United States and China in this area.[14] Much of China's open research in quantum sensing focuses on remote imaging technologies, such as *quantum radar*.[15] However, the U.S. military has publicly identified quantum radar as impractical, suggesting a possible difference in prioritization between the two nations.[16]

Quantum Computing

There are many different technical approaches to quantum computing being pursued in parallel. The United States is in the lead in almost all of them, but there is one leading approach (using what are known as *superconducting-transmon qubits*) in which the Chinese are close behind.[17] Therefore, the size of the United States' lead is debatable.

Quantum Communications

China is the world leader in quantum communications, as measured both by highly cited scientific publishing and by deployed systems.[18] China's quantum communications R&D focuses on an application known as *quantum key distribution* (QKD), which might improve communications security against enemy interception. Chinese scientists have built the world's

[13] Parker et al., 2022.

[14] Parker et al., 2022.

[15] Parker et al., 2023.

[16] Parker et al., 2023.

[17] Parker et al., 2022.

[18] Parker et al., 2022.

largest QKD network, known as the Jing-Hu Trunk Line, stretching 2,000 kilometers from Beijing to Shanghai.[19] They have also launched the only two known satellites capable of performing QKD from space,[20] which they have recently used to establish a secure communication link with Russia.[21] However, the U.S. National Security Agency has publicly assessed that QKD is not suitable for securing U.S. national security systems,[22] suggesting another difference in prioritization between the two nations.

Technology Transition and Military Operational Fielding

Broadly speaking, the field of quantum technology is still very nascent. The only quantum technology that is publicly known to be already deployed by any nation's military is atomic clocks, which underlie the Global Positioning System (among many other applications). The general expert consensus is that quantum sensing is the technology that is closest to useful deployment; in 2019, the Defense Science Board estimated that operational utility may arrive around the 2024–2029 time frame.[23] By contrast, the highest-impact applications of quantum computing, such as decryption, are unlikely to arrive before 2030.[24] It is therefore inherently challenging to discuss which country is currently "ahead," since one could defensibly argue that all players are still "tied at zero."

As I mentioned, there is very little public information about the PRC's plans for the operational military deployment of quantum technology. There is no public information on whether the People's Liberation Army (PLA) is using the national Chinese QKD network. One of the very few specifically *military* applications of quantum technology that the PRC is publicly pursuing is quantum radar[25]—but, as I mentioned above, the U.S. Department of Defense (DoD) considers that application to be fundamentally scientifically impractical.

The U.S. military has recently begun publicly testing quantum sensors in operational environments: U.S. and allied navies tested quantum gravimeters and inertial navigation systems

---

[19] Yu-Ao Chen, Qiang Zhang, Teng-Yun Chen, Wen-Qi Cai, Sheng-Kai Liao, Jun Zhang, Kai Chen, Juan Yin, Ji-Gang Ren, Zhu Chen, et al., "An Integrated Space-to-Ground Quantum Communication Network over 4,600 Kilometres," *Nature*, Vol. 589, January 14, 2021.

[20] Stephen Chen, "China Launches New Satellite in 'Important Step' Towards Global Quantum Communications Network," *South China Morning Post*, July 27, 2022.

[21] Victoria Bela, "China and Russia Test 'Hack-Proof' Quantum Communication Link for Brics Countries," *South China Morning Post*, December 30, 2023.

[22] National Security Agency/Central Security Service, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," undated.

[23] Department of Defense Defense Science Board, "Applications of Quantum Technologies: Executive Summary," Office of the Under Secretary of Defense for Research and Engineering, October 2019.

[24] National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects*, The National Academies Press, 2019.

[25] Liu Zhen, "China's Latest Quantum Radar Won't Just Track Stealth Bombers, but Ballistic Missiles in Space Too," *South China Morning Post*, June 15, 2018.

during the 2022 Rim of the Pacific (RIMPAC) naval exercises.[26] I am not aware of the PLA having conducted any comparable public operational tests of any quantum technology. Nor am I aware of any public Chinese research demonstrations of cutting-edge quantum sensors for PNT.

As I discussed, U.S. and Chinese researchers are focusing their research on different applications of quantum technology. This makes it challenging to assess which country is closer to military deployment, as they appear be to pursuing somewhat different R&D strategies—especially within quantum sensing and communications. My own assessment largely agrees with the U.S. DoD's position that QKD and quantum radar are unlikely to deliver significant military operational advantage. So, in my assessment, the United States is ahead of China—although not always very far ahead—in all quantum technologies that are likely to deliver an operational military advantage. However, the PRC government may have a different assessment.

Structure of China's Quantum Industrial Base

Like the United States, China has more than 100 universities and national laboratories that publish significant amounts of public research across all areas of quantum science.[27] China's military-affiliated universities are not at the forefront of Chinese public research in quantum science. The National University of Defense Technology is one of China's top 20 publishers of research in this field. But neither the PLA Academy of Military Sciences, nor the PLA National Defense University, nor the PLA Strategic Support Force's Aerospace Engineering University or Information Engineering University, nor any of the "Seven Sons of National Defense" universities are.[28] While many Chinese universities are active in quantum science, the single most important research institution is the Hefei National Laboratory for Physical Sciences at the Microscale in the city of Hefei in Anhui Province, which is affiliated with the University of Science and Technology of China.[29] This facility has a budget reported to be in the billions of dollars and has been the source of most of China's major public breakthroughs in the field.[30]

In the United States, private industry is at the forefront of most quantum technology deployment, but private industry appears to be a much less important component of China's industrial base. RAND research has identified a relatively small number of Chinese private companies that perform significant public R&D in quantum technology, and their total announced capital funding is a tiny fraction of the U.S. total. That having been said, there are a few notable Chinese companies, such as QuantumCTek and Origin Quantum Computing.[31] Most of these companies are located in Hefei, suggesting strong research collaboration with the

---

[26] Subcommittee on Quantum Information Science, Committee on Science, National Science and Technology Council, *National Quantum Initiative Supplement to the President's FY 2024 Budget*, December 2023.

[27] Parker et al., 2022.

[28] This assertion is based on English-language publications only, using the affiliations provided by the articles' authors.

[29] Parker et al., 2022.

[30] Stephen Chen, "China Building World's Biggest Quantum Research Facility," *South China Morning Post*, September 11, 2017.

[31] "China's 3rd-Gen Superconducting Quantum Computer Goes into Operation," Xinhua, January 6, 2024.

national laboratory there.[32] Overall, the PRC's research efforts in quantum technology are more centralized—both institutionally and geographically—than the United States' are.

Large Chinese technology companies, such as Alibaba, Baidu, Huawei, Tencent, and ZTE, have also invested in quantum technology R&D, but they appear to have recently pulled back from that field. For example, Alibaba and Baidu have both shut down their quantum computing research laboratories since November 2023.[33]

To my knowledge, none of these research entities have publicly announced that they have provided any operational quantum technology to the PLA.

Connections to Organizations Outside China

The global quantum science R&D ecosystem is highly interconnected. Like every other leading nation's scientists, Chinese scientists collaborate extensively with foreign researchers. I am not aware of any formal, institution-level partnerships for quantum science research between Chinese and foreign research institutions; most scientific collaboration occurs organically between individual researchers.

Applied quantum science is a relatively nascent technology, so much of the technical progress is published openly, and all nations study one another's progress. One of the biggest Chinese breakthroughs to date—a cutting-edge quantum computer announced in 2021—used a very similar design as a quantum computer that Google had developed and publicly described two years earlier.[34] To be clear, there is no public evidence that the Chinese researchers obtained any technical information from Google (or from any other foreign organization) through any illegal or inappropriate means.

The supply chain for quantum technology is particularly important, but there is very little public information about the Chinese supply chain. Several key hardware components, such as dilution refrigerators and high-quality lasers at relevant frequencies, are mostly or entirely manufactured by European or Japanese companies, some of which are quite small.[35] The United States does not have a self-sufficient supply chain, and I suspect that China does not either. Cutting-edge "traditional" semiconductor microprocessors—such as those fabricated in Taiwan—do not appear to be critical to the quantum supply chain, since quantum systems have very different performance requirements from standard electronics.

A final important source of international connections is financial investment. There is significant international financial investment in quantum technology firms between U.S. and allied nations,[36] but I do not know of any financial investment in quantum technology between

---

[32] Parker et al., 2022.

[33] "Baidu to Donate Quantum Computing Lab, Equipment to Beijing Institute," Reuters, January 3, 2024; Casey Hall, "Alibaba's Research Arm Shuts Quantum Computing Lab amid Restructuring," Reuters, November 27, 2023.

[34] Qingling Zhu, Sirui Cao, Fusheng Chen, Ming-Cheng Chen, Xiawei Chen, Tung-Hsun Chung, Hui Deng, Yajie Du, Daojin Fan, Ming Gong, et al., "Quantum Computational Advantage via 60-Qubit 24-Cycle Random Circuit Sampling," *Science Bulletin*, Vol. 67, No. 3, February 15, 2022.

[35] Parker et al., 2022.

[36] Parker et al., 2023.

the United States and China (in either direction). The closest connection that I am aware of is that Sequoia Capital China—which at the time was owned by the U.S. finance company Sequoia Capital but was based in China—previously invested in an Australian quantum technology company.[37] However, Sequoia Capital later instituted a screening policy for investments in quantum technology companies and then spun off its China branch entirely.[38] So that link appears to have been cut.

Last year, the Biden administration issued an executive order restricting U.S. outbound financial investment in Chinese quantum technology firms. Given the lack of known financial connections between U.S. investors and Chinese technology firms, as well as the generally small role that private firms play in the Chinese quantum industrial base, I believe that this executive order will have very little impact on China's R&D efforts over the short or medium term. Over the long term, the order may dissuade U.S. investors from *beginning* investment in the Chinese quantum commercial sector, if that commercial sector grows to become a larger part of the Chinese quantum industrial base. But because there is currently very little connection between the U.S. financial system and the Chinese quantum ecosystem, I do not think that any U.S. government actions regarding outbound financial investment would have a significant impact on Chinese quantum R&D efforts.

Recommendations

I believe that the United States has the good fortune to be at the forefront of almost all of the most important subfields of quantum technology. Moreover, it has a huge advantage that the PRC does not: a network of close alliances with many of the other leading nations in this field. For example, the United States has signed bilateral joint statements of cooperation in quantum science R&D with nine different allied nations.[39] Also, the most important applications of quantum technology are still probably at least five to ten years away, so I believe it is essential to take a long-term view toward maintaining the United States' advantages.

There are still significant scientific advances that need to be made before the full promise of quantum technology can be unlocked. If Congress determines that this technology should be a strategic priority, then the most important step toward that goal would be to continue to invest in scientific research in the field.[40] Another important step would be to strengthen the U.S. skilled workforce in this field—including both the domestic and the foreign pipelines of skilled talent—while ensuring that appropriate protections against intellectual property loss are in place.[41]

---

[37] Parker et al., 2023.

[38] Parker et al., 2023.

[39] Edward Parker, *Promoting Strong International Collaboration in Quantum Technology Research and Development*, RAND Corporation, PE-A1874-1, 2023, https://www.rand.org/pubs/perspectives/PEA1874-1.html.

[40] Parker et al., 2023.

[41] Subcommittee on Economic and Security Implications of Quantum Science, Committee on Homeland and National Security, National Science and Technology Council, *The Role of International Talent in Quantum Information Science*, October 2021; Subcommittee on Quantum Information Science, Committee on Science,

The financial stability of the U.S. commercial quantum industry is not guaranteed; no U.S. quantum technology company has yet reported any significant revenue or clear commercial application. Broad export controls on quantum technology would run the risk of slowing scientific progress and stifling a nascent commercial industry.[42] I believe that *narrowly targeted* export controls on specific Chinese (or other) organizations of concern are low-risk. But I believe that Congress should carefully consider the impacts on the U.S. commercial industry of any proposed broad export controls on quantum technology, unless those export controls are directly tied to a concrete military capability.

There are three other important aspects of the emerging quantum technology ecosystem that the U.S. government should consider understanding and monitoring:

1. the financial health of small, specialized quantum technology companies
2. the flows of skilled talent and intellectual property between the United States and competitor nations (including through intermediate allied nations)
3. the supply chain for critical components and materials.

I do not see any clear needs for immediate action regarding these topics, but all three of them represent potential risks to the long-term stability of the emerging quantum ecosystem.

National Science and Technology Council, *Quantum Information Science and Technology Workforce Development National Strategic Plan*, February 2022.

[42] Parker et al., 2022.

PANEL II QUESTION AND ANSWER

COMMISSIONER WESSEL: Thank you, each of you. And we'll begin with questions. And we're going in reverse alphabetical order, so I get to go first. Jacob, let me ask some questions, and I appreciate your testimony.

The first is -- and may be something that you have not looked at. But I've seen recent reporting, open source reporting about Ukraine's use of AI on battlefield in terms of target acquisition, et cetera. Number one, have you looked at that at all or are aware of it, and two, aware of any Chinese efforts to study what Ukraine has done and how it's being applied on the battlefield so that we have a better understanding?

MR. STOKES: Yeah, absolutely. The war in Ukraine has served as a sort of laboratory for a lot of these emerging technologies. And I think it's been watched around the world certainly including in China. Not just how Ukraine is doing it, but also how Russia is responding and the technological kind of tit-for -tat they have going on the battlefield there.

So it's certainly an area of key interest for China because they haven't fought a conflict in a long time and certainly not with these emerging cutting edge technologies. One particular area that I am concerned about is that Russia in the context of fighting that conflict is gathering a lot of data from its systems. In the course of fighting that conflict, that potentially could be useful in the China-Russia relationship.

That kind of data or insights in technology drawn from that might later be transferred to China. So I think that's something we'll have to watch closely as we go forward. And as it relates to AI in general, if you break it down, there's kind of four parts of it.

There's the chips for computing power. There's algorithms. There's data, and then there's the talent to make all those things come together. So if we think about China's progress, we can look at each of those component parts. And so certainly in the data and probably in the algorithm space, this is a place where China may be able to gain some advantage indirectly through Russia.

COMMISSIONER WESSEL: Also, how would you assess U.S. -- and I know some of this is in your testimony, utilization, for example, predictive maintenance and some other opportunities from AI. How would you judge U.S. capabilities in implementation? And again, you also talked about that it's still early for China. But what visibility or lessons might we gain?

MR. STOKES: Yeah, absolutely. I mean, I think that the U.S. has been very focused on this in a pretty bipartisan way with things like the development of the chief digital and artificial intelligence office. And the Department of Defense recently announced the DOD's Replicator Initiative, focused on uncrewed systems in particular and also its strategy on data analytics and AI adoption.

So there's certainly a recognition of what's at play here. I think that the challenge it's going to come up against is the challenge that many other areas of weapons procurement and other systems procurement meet which is often our procurement system was built in the 20th century. And so it's not always well-positioned to leverage technology in the 21st century.

And I think there's a lot of energy in DOD in trying to get ahead of that. But the obstacles are pretty big. And so that's going to be a place where as we move from experimentation to actually application at scale, we're really going to have to push forward to keep up with China.

But also thinking about how to do that in a way where the systems are safe, secure, and reliable. And what does testing and evaluation look like, in particular in systems that can change over time as they learn? And so you can basically assess a system when it's built. But then how

do you monitor it over time? So there's some unique challenges and testing evaluation for AI systems that we're still working to get our arms around, in DOD and then out in the services as well.

COMMISSIONER WESSEL: Thank you. Mr. Mustafaga, let me connect the last panel on this one and get your thoughts. The last panel, a lot of it was about data collection. One component was data collection. For generative AI and influence cognitive impact, et cetera, there's the broad application.

There's also the targeted application. And it would seem to me that the ability to target certain cohorts, whatever you will is significant. How do you view the last discussion about data acquisition platforms like TikTok which are able to gain large data sets and everything from the geolocation to particularized information? How does that fit with your comments about generative AI and its impact on elections, on potentially other disruptive approaches?

MR. BEAUCHAMP-MUSTAFAGA: Thank you. I think that's a great question. I would certainly say that fundamentally the PLA recognizes the importance of data. Talks a lot about data.

From an open source perspective, it's difficult to really look behind the curtain and see, as Jake was saying, what is the quality of their data? How well do they manage their data? How well do they actually leverage their data?

I think it's a really interesting question. It's hard to look at in depth from an open source perspective. But I think to your specific question on non-U.S. owned social media platforms, I think that's absolutely something that could come into play for this.

And looking at Chinese military writings, I haven't seen much specific discussion of TikTok or geolocation data, et cetera. But the theoretical risk is certainly there. And I think that's definitely something to consider.

I'll also note that beyond TikTok, Chinese government and affiliated organizations have been collecting vast troves of data from not just U.S. citizens but globally. And so, there's a question of how much -- for example, PLA researchers or PLA actors -- would have direct access to that data. Certainly, again, it's difficult to really make that assessment. But theoretically, that would absolutely support their efforts to improve their use of generative AI.

COMMISSIONER WESSEL: I'd just say that I think we've seen over the years, many years some of us have been on the Commission, that theoretical risk turns into real risk in a short period of time. So if we can think of it, they have thought of it. And they're probably putting it into practice. Commissioner Schriver.

COMMISSIONER SCHRIVER: Thank you, and thank you to all our witnesses. Yeah, I think this is a very key point. It strikes me that the stakes are very high.

You've actually described it as potentially shifting the military balance in China's favor. But some of this is going to be difficult to track from concept and R&D and development of particular capabilities to understand the progress that they're making in terms of application, seeing it in training for particular contingencies. Or knowing is this a disinformation point that is a result of generative AI or is this sort of classical what we always see.

I had a couple specific questions on recommendations and then a follow-up if I have time. Mr. Stokes, your recommendation number one was bold action to thwart the Chinese further development of artificial intelligence with military applications. I don't think I noted any specificity under that. Are there particular things you have in mind that would constitute bold action in this case?

MR. STOKES: Yeah, I think here we have to think about -- well, thank you, Commissioner Schriver, for your question. I think here we have to think about those categories I described earlier. So if we think back to the October 2022 semiconductor chip controls, I think broadly considered those were fairly bold and they were updated in 2023.

But there's still -- someone described them as leaky. I think that's a good way to think about them because they're still a black and gray market around them. It's still possible to access that kind of computing power through cloud computing. And also, China is making domestic advances in its manufacturing capabilities.

So that's kind of one node. We also have to think about how we handle things like open source algorithms where some of those advances might be accessible to China, the data, and then also the talent in question. So I think we have to -- I support the chip controls because I think they were the right level of boldness and kind of in many ways cutting the feet out from under China's domestic semiconductor manufacturing capability at the high end.

But they were limited in part because we needed to bring allies and partners on board, specifically Japan and the Netherlands where a lot of the most advanced chip making equipment is made. And so we're always going to have to, I think, strike a balance there as China responds and iterates on how it responds to those kinds of controls. So I think it's really about opening up the aperture.

So for example, on cloud computing, my understanding is the Commerce Department had put forward I think it's an interim rule that's requiring U.S. cloud computing companies to report who their customers are. And thinking about that, probably comparing that against the list of PRC military entities that was updated just yesterday. Those kinds of actions, we're going to have to think about across the full spectrum of the ingredients for AI.

COMMISSIONER SCHRIVER: Thank you. Mr. Beauchamp-Mustafaga, sorry, your recommendation about social media should be required to identify when content is the result of generative AI. Is that simple to do? I mean, no? Is it simple technologically to identify? I'm not asking is it easy to get such a law passed or something.

MR. BEAUCHAMP-MUSTAFAGA: No, I think that's a good question. I think there's two parts to this. One is social media regulation for Congress, the U.S. government.

That's certainly an ongoing conversation and it's challenging and somewhat fraught. But there's also as you mentioned the technological challenge of being able to identify content produced by generative AI models. Right now, it does seem that the offense in a sense has the advantage, right? That it's much easier to produce this than it is to identify it.

There are some ways you can get identification. But overall, especially at scale, right now it really seems that offense has the advantage. Part of my recommendations or policy options to consider was indeed for the U.S. government to support investing in probably long-term abilities to detect generative AI content.

And that doesn't have to be just U.S. government. Obviously, it'd be beneficial to find public-private partnerships. And I think social media companies are very well placed to support the development of that technology, one, because they have the data and really the first observer on these trends. And so it'd be an opportunity for U.S. government to potentially work with collaboratively social media platforms to help do that.

COMMISSIONER SCHRIVER: Thank you. It seems to me that could be low hanging fruit if we can actually do it from a technological standpoint just labeling and identifying. I'll have another question if there's a second round.

COMMISSIONER WESSEL: Commissioner, Vice Chair Price.

VICE CHAIR PRICE: Thank you. And thank you all for your important testimony today. I want to jump in right where Commissioner Schriver left off.

So when we're talking about this need to invest in understanding this and what the long-term need would be, what are we talking about? As we give recommendations to Congress, what are numbers? How big do you think this is? And then my second question following up on what we just said was how do we do this kind of media literacy training for citizens or for others in government?

MR. BEAUCHAMP-MUSTAFAGA: Sure. I think those are two great questions. Specifically on the cost of investment, I don't have specific numbers available to me. But I think in general, significant investment is worth it on this front.

Second, on supporting media literacy, other colleagues at RAND have done a lot of work on the broader crisis of truth decay. And specifically, one of the frequent recommendations from RAND colleagues is investing in civic engagement and media literacy. And so for example, DOD employees who have a security clearance have to go through an annual security clearance update process and do specific training.

So far to the best of my knowledge, that training doesn't include learning the basics of media literacy and identifying generated AI content. So I think there are opportunities for Congress and the broader U.S. government to support either by mandate or requirement or otherwise support broader U.S. government employee literacy awareness of these risks. And then I would certainly say it doesn't have to stop just at U.S. government employees, right?

This is really a whole of society challenge. Generative AI doesn't make a new problem on medial literacy. But I think it really emphasizes the risks and the shortcomings so far. So I think it's another opportunity for Congress to support outreach and really improve broader U.S. citizen awareness of these risks.

VICE CHAIR PRICE: Thank you. Mr. Parker, at the end of your statement, you talked about the three things that we should be monitoring and understanding better. I want to give you a minute to expand on it a little bit more and why particularly.

DR. PARKER: Thank you for the question, Commissioner. The three things that I listed at the end which I would describe as areas where the U.S. government has limited visibility are, first, financial health of quantum technology companies, second, flows of skilled talent and intellectual property, and third, the supply chain. Briefly, I'll touch on all three of them.

I think to the financial health of quantum technology companies, the technology is still very early stage. There are big questions as to realistic timelines for actual revenue generating applications. Most industry investment in quantum technologies and quantum computing which is arguably the most nascent technologically field within quantum technology.

There's a lot of venture capital investment. There's a lot of active private sector activity. But the companies that have reported revenues have reported fairly modest levels of actual revenue.

So there's a question as to the long-term financial stability of the -- I guess whether the technology readiness timelines are aligned with the current state of industry. What steps might be taken if there was, for example, a recession which made the investment environment less favorable for so-called deep tech, technologies? Secondly, regarding the flow of skilled talent and intellectual property, there's a lot of foreign talent in the U.S. research ecosystem.

Many graduate students are from foreign countries. I think on the whole that is a good thing for the U.S. research enterprise. But there are questions as to what are the appropriate

protections for an intellectual property, not only among students but also companies which may not have particular expertise in cybersecurity, for example, small start-up companies.

And third, the supply chain, the technology is still very nascent and there are many different approaches that are being pursued which have very different supply chains. I think there's a general lack of understanding as to where some of the most important components are coming from, which countries they're coming from, especially as we go several levels down into the supply chain, whether they're coming from competitor countries, how robust that supply is, whether it's sufficiently diversified across multiple vendors, and what a mature quantum technology supply chain will look like. So I think all three of those areas are areas of where just more information would be helpful for having a perspective on the ecosystem, even if immediate actions don't necessarily need to be taken. Thank you.

VICE CHAIR PRICE: Thank you.

COMMISSIONER WESSEL: Co-Chair Helberg.

COMMISSIONER HELBERG: Thank you, Co-Chair Wessel. I kindly ask our witnesses to keep their remarks as brief as possible in the interest of time. Mr. Mustafaga, does the PLA view cognitive warfare as a warfighting domain like land, air, space, and sea?

MR. BEAUCHAMP-MUSTAFAGA: Yes.

COMMISSIONER HELBERG: How much do you believe the PLA has invested in cognitive warfare? Are there public estimates available?

MR. BEAUCHAMP-MUSTAFAGA: I know of no public estimates available.

COMMISSIONER HELBERG: Do any of our other witnesses know of other public estimates?

Are you aware of -- do you believe the PLA is actively working to train models to enhance the way it targets Americans through information operations and its cognitive warfare efforts?

MR. BEAUCHAMP-MUSTAFAGA: It's a good question. I can't point to a specific publicly available PLA research directly discussing training generative AI models. Right now, the publicly available research that I surveyed for my testimony was more on I would describe kind of the theoretical side of understanding the value. But I would absolutely not be surprised if at least some of the PLA were beginning to experiment and work with these models, yes.

COMMISSIONER HELBERG: Mr. Stokes.

MR. STOKES: I agree with Nathan's assessment that I think it would be prudent to assume that they are. But I don't think we have good open source information on that topic right now.

COMMISSIONER HELBERG: Are either of you aware of ByteDance's efforts to build an OpenAI rival called LEGO? And doesn't ByteDance own TikTok, and do either of you believe there's a real plausible risk that ByteDance is using TikTok data to train its LEGO LLM?

MR. BEAUCHAMP-MUSTAFAGA: I don't have in-depth knowledge on ByteDance or LEGO. But I think in general, the possibility of any company is going to want to train its algorithms on the best available data. But I don't have specific information on that topic.

MR. STOKES: Yeah, I would just add. I mean, I think every big tech company in the world, certainly Chinese big tech companies, are working to build the types of LLMs because they see that as a market opportunity for themselves. And so I think, again, it stands to reason that they probably are, if they can access the data.

COMMISSIONER HELBERG: Okay. So just for the record, you believe there is a risk that ByteDance is using TikTok data to train its LEGO LLMs?

MR. STOKES: Yes.

COMMISSIONER HELBERG: Aren't LLMs inherently dual use and usable in military context as well? And wouldn't it be common sense for this country to bar Chinese social media company applications from harvesting and collecting vast amounts of American user data to train advanced AI models that can be repurposed to kill Americans?

MR. STOKES: Yes, I think it would be prudent to do that.

COMMISSIONER HELBERG: Is that your assessment as well, Mr. Mustafaga?

MR. BEAUCHAMP-MUSTAFAGA: I think social media regulation is a challenging topic. I think it's absolutely worth considering whether foreign-owned companies should be able to harvest the data of U.S. citizens.

COMMISSIONER HELBERG: And I mean, when we're talking about social media here, we're talking about social media companies under the control and influence of a foreign adversary government. And your response, Mr. Mustafaga, applies to those types of companies. Is that right?

MR. BEAUCHAMP-MUSTAFAGA: Yes.

COMMISSIONER HELBERG: Mr. Stokes, on a scale of one to ten, how high do you think the Chinese leadership ranks AI in their military modernization efforts? And would you say we're at an inflection point in the history of warfare and the character of war is poised to fundamentally change in the years ahead?

MR. STOKES: I believe they rank it pretty high. So by their standards, right, there's mechanization, informatization, and intelligentization. They say they've reached mechanization. So they're working on that next stage but increasingly trying to integrate informatization with intelligentization. So, the last revolution in military affairs with the coming one, so to speak. And I think whether they're able to actually do that is the question. But I think that's how they characterize and understand the environment.

COMMISSIONER HELBERG: And what do you see as being the most important implications for American national security? How should we respond to their embrace of AI in this intelligentization concept that you describe?

MR. STOKES: Yeah, I think we should think about it along three lines. One is improving our own capabilities and making sure we can keep pace. Two, how do we slow down their capabilities, especially where it applies or the most dangerous applications thereof. And then third, working domestically and internationally, including in some cases with China, to shape the rules and norms around controlling this technology. So it has to be a three-part strategy.

COMMISSIONER HELBERG: Can you expand a little bit more on the first one that you describe about enhancing our own capabilities?

MR. STOKES: Yeah, I think the initiatives that I described earlier are underway at DOD. I think our recognition that warfare is changing and that -- or it has the potential to change with these new technologies. And making sure that we're staying on the cutting edge, not just of the basic technologies themselves but also actually integrating them into our institutions, having the right personnel to train and operate them, and really across all the DOD enterprise. And so I think that's really how we should understand what we would need to do in that pillar.

COMMISSIONER HELBERG: And do you see the PLA's adoption of military AI as focused on a particular part of the kill chain, like, logistics or targeting? Or is it focused on all parts?

MR. STOKES: I would say it's probably focused on all parts. But there might be more emphasis on trying to have asymmetric approaches so we can not just have to kill the system, so

to speak, but to be able to disable their operation. And increasingly as we go towards a more integrated command and control architecture like, JADC2 for the U.S., China is thinking in those same terms.

Their term is multi-domain precision warfare. And so that's really -- it's kind of JADC2 versus multi-domain precision warfare. So it's really across the kill chain, I would say.

COMMISSIONER HELBERG: And my last question is for Mr. Parker. As Commissioner Wessel mentioned, we're still very much in learning mode when it comes to quantum technology. Can quantum sensing be used to conduct underground mapping?

DR. PARKER: Subsurface magnetometry is an area that the U.S. DOD has publicly acknowledged is an area of interest for quantum sensing. They have acknowledged that things like gravimeters could be used for, for example, underground tunnel detection, yes, in principle. The technology is not necessarily there yet, but it's certainly theoretically possible.

COMMISSIONER HELBERG: Thank you.

COMMISSIONER WESSEL: Commissioner Glas.

COMMISSIONER GLAS: Many thanks to you all. My first question is for Mr. Stokes. To what extent do you think we are gathering intelligence with some of our international allies around Chinese use of AI in the military space?

Is it adequate enough, that sort of collaboration? If not, what kind of risk assessment should we do? How much prioritization should we give this? What could Congress do in that regard? So that's my first question.

And to Nathan, sorry, I will mispronounce your last name, and my apologies. You mention about AI and the social media influence, the influence campaigns, especially with the upcoming election this year. What could Congress immediately do or the administration immediately do to help safeguard some of the concerns that you raise in your testimony?

MR. STOKES: Thank you for your question, Commissioner. I think we have to draw from our -- especially our closest allies but really across the world because everyone is probably going to have a little bit of a different -- they've got a different hand on the elephant to use the metaphor on what's going on with China in this particular space. I think broadly speaking, we do need to make it a priority given its importance in terms of our intelligence collection.

I'm not an expert on exactly all of the ways you might gather that intelligence. But I think broadly speaking, you've seen U.S. intelligence leaders talk about the need to change the U.S. intelligence enterprise to catch up with some of these emerging technologies. And that the way we gather intelligence and synthesize it, analyze it might have to change. And I think I can't imagine a more important topic for the security of the United States to make sure that we get our understanding of where China is, especially in military AI, that we get that right.

MR. BEAUCHAMP-MUSTAFAGA: I think it's a key question this year. I'll give you four pillars to think about. First is, as I was talking about with the other Commissioners before, considering social media regulation or at least engagement, it could be positive and collaborative to make sure social media companies are well positioned to do what they can on their platforms to identify, and if appropriate, remove inauthentic content and generative AI content.

Second is to support -- really empower as much as possible U.S. government transparency on these topics. Social medial companies can only provide so much information. They have so much information.

Sometimes U.S. government has additional information as seen in the declassified NIC assessment on 2022 elections. But I think transparency is really important for supporting U.S.

public faith in elections and election integrity. Third is, as mentioned before, civic engagement, media literacy.

I think Congress has a role to play both in supporting those efforts and investing in those efforts. And then just in terms of constituent engagement and constituent services, that's really something that Congress could also play on as a key touchpoint for the U.S. government with the broader American public. And then lastly, I do think it's worth at least having some engagement with Beijing on the topics.

I saw a CNN report I believe yesterday morning that Xi Jinping has promised President Biden I believe now twice that he will not interfere in this year's elections. FBI Director Wray testified to the Select Committee yesterday and was asked about it and said basically I'll believe it when I see it. I'm old enough to remember when Xi Jinping promised President Biden he wouldn't militarize the South China Sea.

So I'm heartened by the promise. I think it's very good that the Biden administration is at a high level engaging with Beijing on the topic. But as an analyst, I look at capability and intent equals risk or threat.

And I think both are there, and so I'm concerned. I think even this kind of Xi Jinping promised, is Xi Jinping going to follow through, question one. Is the rest of the Chinese Communist Party state going to follow through, right?

He doesn't actually manage day-to-day everything that's going on. As we sit here, one year on from Balloon-gate, right? Third, how do we define election interference?
It might mean something in a CCP lexicon than it does for the U.S. So I think there are a lot of challenges to that. I think it's good to see the Biden administration engaging.

Last point I'll make is that as Jake mentioned briefly, the Chinese government put out a white paper ahead of the U.K. Summit in October last year on AI global governance. One of those tenets actually said, no one should be doing AI driven social media manipulation. I believe that's low-lying fruit for the Biden administration to say, great, we agree. Let's not do it.

So far, I haven't seen the Biden administration actually seize on that as an opportunity. Again, we can discuss whether we should trust a Chinese government pledge on that topic. But I think it's an opportunity for positive engagement.

COMMISSIONER GLAS: Thank you.

COMMISSIONER WESSEL: Commissioner Friedberg.

COMMISSIONER FRIEDBERG: Mr. Beauchamp-Mustafaga, if I could continue with you. You said in your testimony written and you said it again this morning that the CCP fears that the United States and the West would use generative AI to undermine it. Could you say more about what exactly they're afraid of, how do they imagine that taking place? And do you think that this is an expression of a genuine concern, or is it a kind of projection of the things that they might like to be able to do?

MR. BEAUCHAMP-MUSTAFAGA: Thank you. I think this is an underappreciated aspect of CCP thinking. So, when I'm reading these PLA writings, they do talk a lot about the foreign threat. Sometimes they discuss it as a Western threat.

Sometimes they specifically address U.S. intent. This is part of a longstanding broader CCP concern of U.S. information operations. Nearly every single Chinese domestic crisis at some point in time has been blamed on the United States.

Tiananmen, Hong Kong protests, we can go on and on and on. The Chinese Ministry of Foreign Affairs has very kindly put out several white papers over the last couple years that very

neatly in very long form lists their view of U.S. government activity. So I think it's important to understand this CCP and PLA view.

Doesn't mean we have to agree with it. But it's understanding their perspective. As an analyst, I think it's important. What really drew my concern was that some of these writings described it as a tit for tat as retaliation and response.

DOD's report to Congress last year said the same thing, right? And I quoted my written testimony from a PLA perspective other countries who are engaging in cyber-enabled influence operations basically justify a response. And so I think it's this perceived tit-for-tat that's really important to understand.

COMMISSIONER FRIEDBERG: Thank you. Dr. Parker, you referred in your testimony to the supply chain for quantum computing or quantum devices. Could you say a little bit more about what's involved? Am I correct in understanding that, for example, quantum computing devices would be made out of entirely different kinds of components?

They're not the typical semiconductors that go into all the other computers we're talking about. And who makes these things at this point? What are they and where do they come from?

DR. PARKER: Thank you for that question. It's correct to say that the supply chain for quantum computers and other quantum devices is very, very different from traditional computing technology. They do require a lot of traditional computers in them for control.

But the true heart of it often revolves around extreme low temperatures. So a surprising amount of quantum supply chain revolves around extremely powerful refrigerators to get things down to 1,000th of a degree of absolute zero in some cases. These refrigeration and cryogenics technologies are unusual, very boutique.

Different ones work in different ways. Some of them revolve around lasers. Others revolve around things called dilution refrigerators, and there's no one supply chain.

By and large, most of the devices come from allied nations I would say. Relatively little comes from China or Russia. But the United States does not have domestic production capacity either.

One example, in dilution refrigerators, the large majority of the market is controlled by a single Finnish company called Bluefors. On the laser side, certain companies in Japan and Germany make very high powered, high quality lasers of very specific frequencies which are difficult to source in other places. So it's a difficult supply chain to categorize globally other than to say there are many distinct types of technologies that are sourced all over the world by and large from allied nations.

The one other thing I would say is because there are these multiple non-overlapping supply chains that correspond to very different technology approaches, many of them may not be important in the long run. It may be the case that one of these particular technical approaches, quote-unquote, wins. And then that supply chain becomes extremely important strategically whereas the other six or seven technical approaches may become irrelevant. But it's difficult to know which one will win. So we need to sort of track all these different supply chain simultaneously.

COMMISSIONER FRIEDBERG: Thank you very much. Mr. Stokes, you made the case or your asserted that it was important to -- if there were going to be limitations and controls imposed on artificial intelligence that focused on military applications. How is it possible to do that with the technology which is often described as being equivalent to electricity, having sort of general application and which is in very early stages of development. Is it really possible to target controls on narrowly military applications?

MR. STOKES: I think it's more about targeting -- building controls in a way where we control what we can without undermining the commercial viability of some of our domestic industries that enable our AI progress. So I agree with you that it's very hard, if not impossible, to control military AIs or commercial sector AI applications for military, especially in the PRC context. It's more about trying to understand the market dynamics in any given sector where U.S. advantages are, where U.S. and allied advantages are, where China's are and account for that.

So I think sometimes our instinct is just to shut everything off. And I think there's a good -- that's often -- there are good reasons to feel that way. But to be effective over time, I think we have to consider the particulars of the given market that we're operating in, including what drives the dynamism of American companies.

COMMISSIONER FRIEDBERG: Thank you.

COMMISSIONER WESSEL: Acting Chair Cleveland.

ACTING CHAIRMAN CLEVELAND: Please emphasize that, the acting part. Dr. Parker, I had actually a very similar question to Dr. Friedberg's in that I'm interested in the supply chain. And you say in your testimony that you talk about refrigeration and lasers.

And you just said that there are six or seven technologies that may be relevant. And you don't know which one's the likely winner. So investment in all right now makes sense. Are any of those technologies controlled by any export regime or arms control? Are they subject to any kind of restriction in terms of transfer to China?

DR. PARKER: There are no broad export controls that apply to quantum technology specifically. Now there are a couple caveats there. One is certain specific Chinese organizations have been placed on the Commerce Department's entity list.

So several of the leading Chinese research organizations do not have legal access to U.S. exports in those. The second caveat is that there are some export controls that apply to certain classes of sensors broadly which are not specifically tailored to quantum sensors but would plausibly apply to quantum sensors. Just for example, export controls on magnetometers, some of them might apply to quantum magnetometers.

I think that if the United States decides to impose export controls on some of the more mature technologies, it would be useful to update those export controls which may or may not apply. But it's a bit of a gray area because they were crafted before the current technologies became more mature. So it could well be an area that could just use a little updating and clarifying.

ACTING CHAIRMAN CLEVELAND: Appreciate that. And I think you also said in your testimony that much of this technology is made in Japan and Europe. And so it would require collaboration if it's to be effective I would assume.

DR. PARKER: Yes.

ACTING CHAIRMAN CLEVELAND: I wonder if you could supply for the record, since None of us really understand quantum, kind of your assessment of what these technologies, the ones that need to be updated might be just so we have a very primary understanding of what we're talking about here. I would appreciate that. You also said in your testimony that Alibaba, Huawei, Tencent, ZTE, and Baidu have invested in quantum.

And I assume that there's some leader that it was designated to undertake this effort as the government usually designates a leader. But you say that they appear to have pulled back from that field and shut down quantum computing research labs in November. Could you talk a little bit more about what may be behind that, if not trend series of actions?

DR. PARKER: So that's correct. The Chinese quantum ecosystem looks very different from the U.S. one. The U.S. ecosystem is by and large led by private industry at this point. The Chinese quantum industry is much more heavily funded -- focused in government funded national labs. So already this sort of weight of R&D effort is significantly heavier in national labs in China than in commercial industry. Several of the large Chinese players you mentioned, Baidu, Tencent, et cetera, did have quantum computing efforts.

They have -- several of them if not all of them have shut down just in the past six months. Baidu announced it was selling all of its quantum computing hardware to a national lab. So that concentration to national labs appears to be consolidating even more just in the past six months. I don't have great visibility as to why Baidu made that decision. My guess would be that they assessed that they were not particularly technically competitive in that space. They were far behind U.S. companies, did not seem to be catching up, and did not see it as a revenue generator. So the extent that we can talk about Chinese thinking as a whole, they seem to be further doubling down on national laboratories. None of the Chinese quantum technology companies seem particularly competitive globally ever.

ACTING CHAIRMAN CLEVELAND: So you would characterize it as increased risk, that the government is consolidating under government control these capabilities or along with an assessment by these companies that it's not profitable?

DR. PARKER: I don't know if I would necessarily characterize it as an increased risk. I think -- frankly, I don't think it really matters too much from a U.S. national security perspective, whether it's the Chinese government or Chinese industry that's controlling the technology. I think in China, they're more or less the same thing.

I would maybe interpret it as cautious good news that the Chinese -- at least one aspect of the Chinese ecosystem does not appear to be self-assessed. It's not at the very top of the global competitive landscape there. But I don't think it's a particularly major increase or decrease in risk either way.

ACTING CHAIRMAN CLEVELAND: Thank you. Are we going to go to a second round?

COMMISSIONER WESSEL: We'll try and keep this round shorter so that everyone has a chance. I'm going to pull a Star Trek issue here because it has baffled me. But while we were talking, I looked at it again.

China is rumored to have successfully engaged in teleportation which was seven years ago. You're nodding your head yes, so I assume you're aware of this. And I believe Science magazine and others talked about the profound nature of that.

That's seven years ago. Has -- number one, has that been peer reviewed and in fact is it true? Number two, what are the implications? I can't wrap my head around that.

DR. PARKER: Thank you for the question. It is a difficult question to answer briefly, but I will try. Quantum teleportation as a scientific phenomenon actually goes back to 1995, I believe.

So it is -- I think it was first demonstrated in the United States or maybe it was in Europe. So it's not a completely new scientific phenomenon. It is -- in the long term, it could be useful for things like networking together quantum computers.

I think in the near term, there are no immediately concrete applications that will prove transformative. But I think it speaks to a larger part of the Chinese focus and prioritization in quantum which is that they are focused on communications technologies and the use of quantum

technology to secure their communications. There's some disagreement among experts as to how significant that is operationally, whether it's actually a useful capability.

But the Chinese do appear to have chosen that to be an area which they want to excel globally. And one aspect of that is China has launched two different satellites that are capable of quantum communications from outer space, which includes quantum teleportation of individual particles mediated by satellite communication. No other country is known to have launched quantum communication satellites.

Again, the U.S. National Security Agency actually publicly said that specific application is not a high priority, not something that they intend to pursue themselves. So there's definitely disagreement as to how seriously we should take this. But it is one area that the Chinese do appear to be leading globally. And just one last technical note, the teleportation certainly does not allow teleportation of humans or significant quantities, material. It's individual particles.

COMMISSIONER WESSEL: No, I read about it in terms of quantum internet and how it might enhance command, control, survivability, et cetera, in terms of military facilitation. So I'm not expecting that Spock is beaming up somewhere. Let me say that for the record. Commissioner Schriver.

COMMISSIONER SCHRIVER: Dr. Parker, I think you forgot to end your sentence with yet. Thank you. Both Mr. Stokes and Mr. Beauchamp-Mustafaga mentioned the need for dialogue and direct engagement with the Chinese and the PLA on these matters.

I think, Nathan, you already had a chance to expand on that a little bit. So Mr. Stokes, I'm wondering how you see that as a useful engagement and what topics you would prioritize, et cetera, noting that this is an interlocutor that still claims that the spy balloon was a weather balloon that went off course. And they know we shot it down and collected it. So what would our expectations be in such a dialogue?

MR. STOKES: Sure. Thank you for the question, Commissioner. I think it's important to note about kind of the timing of this that it comes after major steps in the U.S. to put in place a regulatory framework for our own AI but then also to work internationally through moves like the political declaration on responsible use of military artificial intelligence and autonomy, excuse me, that one's a mouthful, which has been endorsed by about 50 countries.

So before engaging China and try to set a framework for what we think normatively the rules and institutions ought to look like in AI and then engage China from that perspective. I think it's worth stepping back and saying one of our grand strategic objectives is to support a rules-based international order. The rules are being written in real time here.

And so we need to think from that context. And it makes sense to build China in if we can get China to accommodate and agree to a certain set of rules that we put in place and are leading a coalition in defense of. As it relates to the specific talks, National Security Advisor Sullivan talked earlier this week that the talks are probably going to happen sometime in the spring.

It would likely be very, very basic about exchanging views on what we see as the actual risks from AI technology, understanding more about how China understands the risks. Maybe in certain areas sharing information about how we test and evaluate our weapons or what parts of particularly the nuclear command and control complex would or would not have artificial intelligence. Those types of very basic topics are where you would have to start here.

You would be miles, perhaps even decades away from an agreement that looks like an arms control agreement where there's verification and those kinds of things, both for the political

reasons you raised but also underlying technical challenges around verification with AI. So I think it's a good thing in that right context and with the right low basic expectations. Thank you.

COMMISSIONER WESSEL: Vice Chair Price.

VICE CHAIR PRICE: I just -- thank you. I just have one quick question for Mr. Stokes on your recommendations for policymakers. Your last one, you say we should prioritize intelligence gathering and analysis. Are you just flagging something, or are you suggesting that Congress ask for something in particular?

MR. STOKES: I think it would be beneficial, especially for the open source analytical community that I work in to have more open source information about this. One potential way of doing that that Congress could do is to mandate an additional section in the China Military Power Report related to some of these topics as they've done with other topics in the past. You could also probably mandate that the DOD or the intelligence community provide briefings on this particular topic to members of Congress and relevant committees and even commissions.

Those kinds of actions because I think we're at a place in the policymaking process where we're still getting up to speed on what the technologies are, what they do, and then trying to get past that to what should we do about them. And having an accurate understanding to the extent possible of where China is relative to the U.S. in a robust way would be really helpful. So that would be where I would start as a recommendation within the China Military Power Report.

VICE CHAIR PRICE: Thank you for clarifying. That's it.

COMMISSIONER WESSEL: Co-Chair Helberg.

COMMISSIONER HELBERG: No additional questions on my end.

COMMISSIONER WESSEL: Commissioner Glas. Friedberg?

COMMISSIONER FRIEDBERG: Nathan, you mentioned a translation I think of a phrase, something like controlling the brain. The Chinese have several categories of things that they talk about. Is that simply a figure of speech, I want to influence your thinking? Or is there more to that?

MR. BEAUCHAMP-MUSTAFAGA: Yeah, thank you for asking the question. I'm happy to clarify. So, that was in reference to one of the popular kind of overarching conceptions of some of the technologies that underline or are often associated with cognitive domain operations, right?

Cognitive domain operations is the most popular operational concept, per se. When the Chinese military researchers discuss -- are able to influence operations more broadly. So there is some discussion about controlling the brain, "zhinao."

That is -- it really has a longstanding history in Chinese military, kind of influence operations, psychological warfare, information operations discussions. Some of the conversations you can find in Chinese military writings are, I will say, futuristic. That is certainly not unique to the Chinese military when you look globally about what some in global militaries write about future potential breakthroughs in brain science or other things.

But one of the more concrete examples I provided, it is actually something that Chinese military researchers look to the U.S. for which is laser weapons and also acoustic weapons. And so the ability to use that to degrade somebody's not quite cognitive function. Make them uncomfortable so ideally they would lay down their arms, right? Surrender on the battlefield.

I believe the U.S. developed -- perhaps deployed but developed something the area - denial weapon which I said it in my testimony. So there is some conversations in PLA writings that are futuristic. And there are some that are more concrete and not totally distant from what U.S. DOD has considered sometimes.

COMMISSIONER FRIEDBERG: Thank you.

COMMISSIONER WESSEL: Futuristic and we just talked about teleportation. Okay. Acting Chairman Cleveland.

ACTING CHAIRMAN CLEVELAND: Yeah, yeah, yeah. So, Mr. Stokes and Mr. Beauchamp-Mustafaga, for decades, part of U.S. military policy calculations have been that Chinese military doctrine is very hierarchical and that part of our strategy has always calculated or presumed that decisions will be made by the top leadership in Beijing. And I think, if anything, over the last decade that idea that Xi is in charge and in control and is the ultimate decision-maker on everything has -- this Commission certainly has reinforced that idea.

I'm wondering -- Mr. Stokes, you say in your written testimony that there are some military leaders who might not trust applications of AI because it loosens that control. I'm wondering how AI is changing the idea that decisions may not be made in real time in Beijing. Does that question make sense? I'm sort of wondering if there's been a shift in thinking that more control will be yielded to field commanders or regional commanders. Or how is AI changing military -- our military thinking about their military doctrine?

MR. STOKES: Well, thank you, Acting Chair Cleveland for that question. I think it can -- my sense is it can kind of work in one of two ways. On the one hand, you could -- as I wrote in my testimony, you could see a reluctance from especially mid-level commanders who are going to be held accountable for what these systems do to employ them because one of the characteristics of AI systems is sometimes they're brittle.

Sometimes they fail in unexpected ways. Sometimes you just don't know exactly what it's going to do. And when you are responsible for both operational effects but also the political implications of that, in other words, if you're in the PLA and you've got your political commissar sitting right next to you, do you want to take -- do you want to role the dice on whether the system is politically correct in addition to being operationally correct?

So I think that's one thing that might hamper a deployment of PLA or military AI systems in the PLA. I think on the other hand, you see a lack of trust from the top leadership all the way down that they could implement decisions well. I'm sure you are familiar with this concept of the "five incapables."

And I think if you had too much faith in military AI systems or AI generally that the machine will make the right decision and the machine is reliable, you might be able to have the notion that you could make all the decisions from the top and let the machine push it down through the system. And I don't know where that nets out. I think we're probably still too early to tell. Thank you.

MR. BEAUCHAMP-MUSTAFAGA: Can I add to that? I agree with Jake. I think it's very early to tell. I think it's absolutely something that's very important to watch from what we can observe open source, not just in the writings but as they're doing their exercises and training.

It's absolutely something, as Jake already mentioned, vital to engage with China and specifically Chinese military on how do they assess trust, how do they -- the quality of their AI systems. Is there an opportunity for at least making sure that they don't trust the wrong system in the wrong way? And I think as Jake said and as this Commission has heard before, right, Xi Jinping has publicly denigrated his senior officer corps for their inability to do their job, right, command troops in war, which is an amazing thing to say publicly.

And so one of my concerns is indeed that Xi Jinping decides after some amount of time these guys -- and they're mostly all guys -- can't do their job. And then someone else offers him a magical AI system. And he says, great, can't be worse than these guys.

I think that's absolutely a concern. I think it's something to watch. And I think again, there's hopefully some value in dialogue on this topic. We can't solve the problem for them. But it's just something that's really important.

ACTING CHAIRMAN CLEVELAND: What would we be looking for? I mean, if you were to say -- define some metrics for us to say if we see a consolidation of leadership -- military leadership or an elimination of a whole layer of leadership, how might we think about what would be a measure of Xi saying, okay, AI has got to be better than what I've got?

MR. STOKES: I think that's an analytical question we're still grappling with. I mean, Nathan and I have been in some sessions together where we've got a wall full of possible metrics that we can measure to try to understand exactly analytical questions like these. I think if we understand more -- one of the ways you might look at it is just by understanding more about what systems we know are out there and being applied in the PLA.

And then we can probably infer from there about what level the control and orders are coming from and then how they're executed from there. But we're still at that early stage where we don't really know specific systems that are being fielded by the PLA. So I think I would start there and then you can look at things like training materials, the way grades and specialties for specific personnel are named. Those kinds of subtle indicators might tell us something about the way the PLA bureaucracy and command structure is working.

COMMISSIONER WESSEL: Co-Chair Helberg.

COMMISSIONER HELBERG: I have one quick questions for Mr. Parker and then a quick question for the witnesses writ large. You mentioned earlier, Mr. Parker that a quantum sensor could potentially be capable of doing subterranean mapping. If you hypothetically attached a quantum sensor to a giant helium balloon that you flew over -- in a guided way over our nuclear silos, wouldn't that allow revealing sensitive national security information about our nuclear silos?

DR. PARKER: I haven't looked into that question with enough technical detail to comment.

COMMISSIONER HELBERG: My question for the witnesses in general are if you look at the overall pattern of behavior that you described today. And if you add facts about China that we know the military drills, the cognitive warfare, the adoption of AI, the statements about wanting to reunify with Taiwan, et cetera, et cetera. Is China preparing for war? Is this the behavior of a peaceful -- of a peace seeking country? Mr. Stokes, maybe we'll start with you and work our way down.

MR. STOKES: I think China is preparing to have the capability to fight a war, right? We know that -- our the U.S. intelligence assessment is that Xi Jinping has ordered the PLA to have the capability to invade Taiwan by 2027. Now an order doesn't mean that they'll have it because it's a dynamic military balance between China, Taiwan, the U.S., other potential partners and that type of contingency.

But it's clear that Xi Jinping wants China to be in a place to do that, to have that as an option. I don't think that necessarily means he will do it. I think he can still be deterred with the right set of actions. And it's really incumbent upon us and our allies and partners to determine what those actions need to be and then to undertake them to prevent any such war from taking place. Thank you.

MR. BEAUCHAMP-MUSTAFAGA: I agree with Jake's comments and specifically on the topic of cognitive domain operations. I think we're really at the beginning of our understanding of this idea and there's still a lot of research to be able to support answering that

question. I think it's really an important topic to understand how does the Chinese military conceive of activities that are acceptable or prioritized in steady state versus crisis versus wartime.

We have some information on that. There's always more to do. But I think fundamentally in terms of Xi Jinping and Chinese leadership decision calculus, I defer to the U.S. government on those assessments. I think Jake has summarized them well. I absolutely think deterrence is still a viable option. It's important for the U.S. DOD and broader U.S. government and allied partners to support efforts for deterrence so we don't get to that point.

DR. PARKER: I can't comment whether China as a whole is preparing for war. But I can say I would not necessarily interpret their efforts in quantum specifically as an attempt to increase their warfighting capacity in the near term. I think the timelines are still fairly large, fairly long.

I think they see certain areas of quantum technology as a big economic opportunity. So a lot of it might be oriented around generally growing their economy. The third slightly more specific comment I'll say is a lot of their efforts in quantum communication have the goal of shoring up the security of their communications against external access.

And I think the provocation of a lot of that was the alleged Snowden leaks about a decade ago. They publicly said that those alleged leaks reoriented their thinking about the wisdom of relying on Western communication systems for their own internal communications. So I think that may have been a motivation for their attempt to reinvent their communication system which is not directly related to any near term plans for warfare.

COMMISSIONER HELBERG: Well, a few people on the China Select Committee seem to believe that there might be plans for military -- for the use of military force in the not too distant future. But I thank you for your responses.

COMMISSIONER WESSEL: Commissioner Friedberg for a quick follow-up.

COMMISSIONER FRIEDBERG: Just a factual question. Is there a discussion in the open source Chinese literature, military writings, on the potential risks or dangers of autonomous weapons?

MR. STOKES: I think both in the literature and having spoken to some Chinese experts on these issues, I think there is an understanding that there are risks involved, both kind of what are often talked about as catastrophic risk for AI technology generally but also the specific risks that, for example, highly autonomous uncrewed vehicle could take an action that would precipitate a crisis that was unintended. And so I think there is a recognition. And that relates to the control question we were talking about earlier of my sense is still that's something -- China wants to -- there are times when it probably wants to start crises.

But it wants to do so at a time and place of their choosing. And so they want a system that might start an unintended crisis. It's not something that they're seeking. So I think they are aware of that risk and probably see it as in their interest to be able to avoid those kinds of outcomes. Thank you.

COMMISSIONER WESSEL: Thank you to the panelists. We will take a break until 1:50 and look forward to being back at that time. Thank you.

(Whereupon, the above-entitled matter went off the record at 12:50 p.m. and resumed at 1:52 p.m.)

PANEL III INTRODUCTION BY COMMISSIONER MICHAEL R. WESSEL

COMMISSIONER WESSEL: Our third panel will examine several case studies of other technology areas which United States and China are competing for strategic advantage, namely the commercial applications of AI, biotechnology and battery technology.

These commercial technologies are being used to, or eventually will, boost Chinese economic competition against U.S. firms, dominate global supply chains and defer to the military and surveillance objectives of the CCP.

We will start with Ms. Ngor Luong, Senior Research Analyst at the Center for Security and Emerging Technology. Her research focuses on China's science and technology ecosystem, AI investment trends, and AI diplomacy in the Indo-Pacific region.

Ms. Luong will discuss the trends in China's commercial AI industry as well as the key institutions driving China's AI development. She is a new voice here before the Commission. And thank you.

Next we will hear from Dr. Michelle Rozo, Vice Chair of the National Security Commission on Emerging Biotechnology. Dr. Rozo was previously Director of Technology and National Security at the National Security Council. She will testify on China's progress in various subfields of China's biotechnology industry, including agriculture, pharmaceuticals, and more. This is her first time appearing here. Thank you.

Lastly, we will hear from Dr. Jeb Nadaner, Senior Vice President of Government Relations at Govini. Dr. Nadaner previously served as former Deputy Assistant Secretary of Defense for Industrial Policy in the Trump administration.

He will address China's battery development, including industrial and EV batteries and the risks associated with their presence in U.S. military and critical infrastructure systems. This is his first time appearing before us as well, and I appreciate all of the new voices and views we are getting today.

Thank you all very much for your testimony. I will ask all of our witnesses to please keep their remarks to seven minutes to preserve time for questions and answers.

Ms. Luong, we will begin with you.

OPENING STATEMENT OF NGOR LUONG, SENIOR RESEARCH ANALYST, CENTER FOR SECURITY AND EMERGING TECHNOLOGY

MS. LUONG: Good afternoon, Co-Chair Wessel and Co-Chair Helberg and members of the Commission. Thank you for the opportunity to testify today on China's progress in commercial applications of emerging technologies.

I have been asked to focus my testimony on China's investment landscape as well as key institutions driving its commercial development of artificial intelligence.

I will begin my statement with China's AI investment landscape and trends followed by internal and external factors impacting China's AI ability to innovate and conclude with recommendations for U.S. policymakers on U.S. and China competition for artificial intelligence.

The PRC has emphasized AI essential to its ambition to become a technology superpower. And it has called on both government and private sector actors to support this goal. China's ambition to leapfrog the United States can pose economic and security challenges to the United States. For instance, under its military-civil fusion policy, China's progress in commercial AI applications can also support its military modernization goals in a way that can threaten U.S. national security.

In my written testimony, I discuss in-depth multiple financing mechanisms that the PRC has used to increase capital support for AI. This includes R&D funding, subsidies, public, and private equity investment.

Today I want to focus on government guidance funds. The Chinese government uses these funds to mobilize both public and private capital in order to achieve two goals; one, generous financial returns and two, to further its industrial policy goals.

Guidance funds can take on the form of a limited partnership structure, pretty common in equity finance. This has allowed government to direct investments into strategically important industries.

My research shows that the government is involved across multiple funding stages, investment in early stage companies, especially in emerging technologies, can be really risky. And so the Chinese government sets up guidance funds in order to contribute the first 20 to 30 percent of capital.

In theory, this initial investment can attract private investors who may not have the appetite to fund high risk/high reward sectors like AI. But in practice, these investments are often state-owned enterprises and state-run banks. And once deployed, these guidance funds are operated under the hands of management institutions that are established by government agencies or state-owned investment firms.

Guidance funds are one of the government's tools to maintain close ties between public and private sectors. When the Chinese government takes up shares in a non-state AI company, it can exercise and manage their control over that company.

However, there are serious limitations to this financing mechanism. Chinese government guidance funds are plagued with corruption, waste, inefficiencies, and lack of coordination. For example, they often raise much money down plan. And when they do raise the money, much of it is actually not deployed into productive projects.

And the Chinese economic slowdown has also been exacerbating this problem. For instance, fundraising amounts in 2022 saw a 35 percent reduction from the previous year.

Guidance funds and other financing tools are not going to go away despite their uneven impact on China's AI development.

The PRC has put a lot of stock in its capacity to fund innovation, even tolerating waste and inefficiencies.

And there are other internal factors impacting China's ability to innovate in AI and other emerging technologies. These include demographic changes, talent shortages and the evolving regulatory environment.

Of these three factors, I am going to focus on China's AI governance efforts. These efforts are led by the cyberspace administration of China. And in recent years, it has launched three main AI regulation policies, one focusing on recommendation algorithms and the other two on generative AI.

These regulations could offer AI companies priority on what is and what is not permitted when they develop their models for commercial uses in a fast-paced AI market.

However, excessive regulation can stifle innovation. We have seen some indications that Chinese companies are concerned about compliance costs associated with expanding regulations. But it is too early to judge the full impact of China's AI regulations on a country's ability to innovate and to follow its technology ecosystem.

Beyond that, there are also other external factors that impact China's AI innovation. For one, U.S. export controls on advanced computing chips and related semiconductor manufacturing equipment may hinder China's ability to train large language models that often demand high computing power.

Another is the U.S. 2023 outbound investment restrictions on venture capital and private equity investment in China. Although the EO narrowly scopes the restriction to companies that are mainly doing -- mainly are engaged in AI systems that are for military purposes, the impact can extend beyond that.

It is possible that with more limited access to U.S. experts and expertise and networks, these companies may have difficulty finding investors to fund their visions.

Such measures are intended to restrict Chinese access to U.S. technologies and know-how, capital and markets. But to really ensure policy effectiveness, I recommend the following three actions, which I also discuss in detail in my written testimony.

First, U.S. policymakers need accurate, evidence-based assessments of China's technological power to regularly track and update China's AI capabilities and their impact on U.S. competitiveness. For instance, creating an open-source intelligence center can help enhance our understanding of China's S&T capabilities.

Second, to restrict U.S. capital and intangible benefits from aiding the development of China's AI use for military purposes, the U.S. should carefully scope the outbound investment programs to be headed by the Department of Treasury. And this mean revising the scope of the end use prohibited transactions as well as implementing an entity-based approach as well for the restriction.

Third, the United States cannot do this alone. There have been government efforts to align with allies at the strategic level, but further specific actions are needed.

For instance, information sharing with key U.S. allies such as on transactions of concern can really make coordination efforts more effective. This could also avoid overextending U.S. jurisdiction and also help countries learn from each other's experiences as they are trying to establish their own outbound investment authority.

Thank you again for the opportunity to testify today, and I look forward to your questions.

COMMISSIONER WESSEL: Thank you. I appreciate it. Dr. Rozo?

PREPARED STATEMENT OF NGOR LUONG, SENIOR RESEARCH ANALYST, CENTER FOR SECURITY AND EMERGING TECHNOLOGY

Testimony before the U.S.-China Economic and Security Review Commission on "Current and Emerging Technologies in U.S.-China Economic and National Security Competition"

Panel III: China's Progress in Commercial Applications of Selected Emerging Technologies

Ngor Luong
Senior Research Analyst, Center for Security and Emerging Technology (CSET)

February 1, 2024

Co-Chairs Wessel and Helberg, distinguished Commissioners and staff, thank you for the opportunity to testify on China's current and emerging technologies and their implications for U.S.-China Economic and National Security Competition. It is an honor to be here alongside esteemed experts on this panel. My testimony reviews China's domestic and international efforts to ramp up the development of artificial development (AI), focusing on investment trends and key institutions driving the country's commercial development of the technology. It also assesses China's current AI governance and internal and external factors impacting the country's AI growth, including the Biden administration's 2023 executive order restricting U.S. private equity and venture capital investments in China's technologies. Finally, it concludes with recommendations based on the economic and national security implications these factors hold for the United States. These recommendations include:

- U.S. policymakers need accurate, evidence-based assessments of China's technological power.
- To restrict U.S. capital and intangible benefits from aiding the development of China's AI used for military purposes, the United States should carefully scope the outbound investment program spearheaded by the Department of Treasury.
- The United States should coordinate with its allies and partners to track the flow of venture capital and private equity investments into Chinese AI companies.

1. Domestic Support for AI

The Chinese government has consistently emphasized AI as central to China's aim to become a technology superpower. In particular, the 2017 New Generation Artificial Intelligence Development Plan (AIDP) calls for both relevant state and non-state actors to support the central government in pursuing global leadership in AI and using the technology to achieve the next phase of economic growth.[1]

[1] "Notice of the State Council on Issuing the New Generation Artificial Intelligence Development Plan" [国务院关于发音《新一代人工智能发展规划》的通知], PRC State Council, 2017, https://perma.cc/B9ZR5LQL; English translation is available at https://www.newamerica.org/cybersecurityinitiative/digichina/blog/full-translation-chinas-new-generation-artificial-intelligence-development-plan2017/.

1.2. State Support for Public AI R&D

The Chinese government views basic science as key to winning the global competition for leadership in AI, and to this end is responsible for funding the bulk of basic research and development (R&D) in AI. The 2016 Innovation-Driven Development Strategy aims to reclaim control over key emerging technologies previously dominated by advanced nations like the United States.[2] China's 14th Five-Year Plan (covering 2021-2025) further specifies the need to boost spending on basic research to reduce chokepoints in areas such as AI, biotechnology, robotics, and quantum computing.[3] In 2022, the Chinese National Bureau of Statistics reported that China's R&D investment exceeded $421 billion (3 trillion RMB), a 10 percent increase from 2021.[4] This meets China's goal of increasing R&D expenditure by more than 7 percent annually, as addressed in the 14th FYP.[5]

The Chinese Academies of Science (CAS) and The National Natural Science Foundation of China (NSFC) are China's largest funders of basic research, dedicating $23.8 billion (170 billion RMB) and $6 billion (42.8 billion RMB), respectively, to basic research programs in 2023.[6] Some of the NSFC's research funding objectives for AI in 2023 included deep learning, brain-inspired AI, AI methods in biomedicine and computing.[7] In December 2023, NSFC also announced plans to fund 6 generative AI basic research projects to "enhance [China's] international competitiveness."[8]

One way the Chinese government can channel capital to AI research is through state funding mechanisms such as the National Key R&D Programs (NKPs). After the 2014 reform of the national S&T funding system, the NKPs absorbed both the 973 Program for basic research and

[2] "Outline of the National Innovation-Driven Development Strategy Issued by the CPC Central Committee and the State Council [中共中央 国务院印发《国家创新驱动发展战略纲要》]," *Xinhua*, May 19, 2016, http://www.xinhuanet.com/politics/2016-05/19/c_1118898033.htm; English translation is available at: https://cset.georgetown.edu/wp-content/uploads/t0076_innovation_driven_development_strategy_EN.pdf.
[3] "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035."
[4] "China R&D investment will exceed 3 trillion yuan in 2022," [2022 年我国研发经费投入突破 3 万亿元], *Xinhua*, September 18, 2023, https://www.gov.cn/lianbo/bumen/202309/content_6904781.htm.
[5] "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035" [中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要], *Xinhua*, March 12, 2021, 8 https://perma.cc/73AK-BUW2; English translation is available at https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf.
[6] "Department Budget of the Chinese Academy of Sciences 2023" [中国科学院 2023 年部门预算], CAS, https://www.cas.cn/tz/202303/P020230328780041440473.pdf; "National Natural Science Foundation of China 2023 Department Budget" [国家自然科学基金委员会 2023 年度部门预算], NSFC, https://www.nsfc.gov.cn/Portals/0/fj/fj20230330_01.pdf.
[7] Notice on the Release of the "Guide to the 2023 Annual Projects for the Major Research Program on Explainable and Generalizable Next-Generation Artificial Intelligence Methods" [关于发布可解释、可通用的下一代人工智能方法 重大研究计划 2023 年度项目指南的通告], NSFC, March 31, 2023, https://perma.cc/9C45-MK52; English translation is available at https://cset.georgetown.edu/wp-content/uploads/t0552_explainable_AI_plan_EN.pdf.
[8] "Application Guideline for the Special Project 'Basic Research on Generative Artificial Intelligence'" ["生成式人工智能基础研究"专项项目申请指南], NSFC, December 13, 2023, https://www.nsfc.gov.cn/publish/portal0/tab434/info91118.htm.

the 863 Program for high-tech development.[9] This integration of different R&D programs serves as a means to link basic research to the development of applied technology.[10] Another way is through the "2030 Science and Technology Innovation—'New Generation Artificial Intelligence' Megaproject" (科技创新 2030—'新一代人工智能'重大项目), which was launched in 2018 to ramp up AI development among a wide array of Chinese universities, companies, and research labs.

On the receiving end of some of these funds are State Key Labs (SKLs). These labs secure a steady stream of funding from the government to drive China's strategic basic research in S&T in the military and commercial spaces. In 2019, for instance, SKLs received a total of $925 million from China's Ministry of Education, Ministry of Science and Technology, and CAS.[11]

SKLs also sit at the intersection of public- and private-operated labs. The Chinese government establishes enterprise-based SKLs hosted within firms to link basic research to advanced technology applications. As of July 2022, nearly 40 percent of the 469 known SKLs were managed by government-designated AI national champions such as iFlytek and other conglomerates like Huawei and ZTE.[12]

1.3 State Support for China's Commercial AI Development

In the commercial sector, the government also plays a role in aligning public and private interests around strategic technologies like AI. As stipulated in the 14th Five-Year Plan, the Chinese government aims to "deepen the reform of investment and financing systems, exploit the leveraging role of government investment, stimulate private investment activity, and form endogenous growth mechanisms based on market-led investment."[13] To identify key commercial actors in China's AI innovation system, it is important to examine different means by which the state finances AI development in the commercial sector.

1.3.1. State financing for commercial AI

One of China's traditional industrial policy mechanisms to boost strategic industries is subsidies. In recent years, the state has identified and supported the "Little Giants," which are small and medium-sized companies with significant responsibilities for China's economic growth. Launched by the Ministry of Industry and Information Technology (MIIT) in 2018, the nationwide Little Giant initiative seeks to promote innovation while insulating the country from

[9] "Press Conference on the 'Launch and Implementation of the National Key R&D Program': Summary Transcript [国家重点研发计划启动实施"新闻发布会：文字摘要]," PRC Ministry of Science and Technology, February 16, 2016, https://perma.cc/XFZ3-3AMX; English translation is available at: https://cset.georgetown.edu/publication/press-conference-on-the-launch-and-implementation-of-the-national-key-rd-program-summary-transcript.
[10] Ibid, 2-3.
[11] Emily S. Weinstein, et al., "China's State Key Laboratory System: A View into China's Innovation System," Center for Security and Emerging Technology, June 2022, https://cset.georgetown.edu/publication/chinas-state-key-laboratory-system/.
[12] Author's calculation of the numbers provided in Ibid.
[13] "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035 [中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要]," Xinhua, March 12, 2021, https://perma.cc/73AK-BUW2; English translation is available at: https://cset.georgetown.edu/wp-content/uploads/t0284_14th_Five_Year_Plan_EN.pdf.

supply-chain vulnerabilities and other external shocks by supporting companies in strategically important sectors such as manufacturing, hardware, and software.

As of July 2023, there are 12,756 Little Giant companies, although it is difficult to tell exactly whether all of them have received public and private funding.[14] In 2021, the MOF and MIIT issued a notice to support the first three batches (out of five total) of the Little Giants, offering more than $1.4 billion (10 billion RMB) in grants and subsidies between 2021 and 2025.[15] From 2020-2022 more than 1,500 Little Giants also received other forms of funding by winning major national S&T projects.[16] Given the government's interests in these companies, they are also popular among venture capital (VC) firms, having received nearly $224 billion (1,597 billion RMB) in funding since 2018.[17]

In the public equity investment realm, the Chinese state has emphasized the importance of tech-focused stock exchanges such as the Shanghai-based STAR Market and Shenzhen-based ChiNext board on China's tech industry. Tech companies listed on the STAR Market align closely with China's industrial policy goals. According to the 14th Five-Year Plan, China "will open up domestic IPO financing channels for S&T enterprises, enhance the 'key and core technology' characteristics of the STAR Market…to serve growing innovative and entrepreneurial enterprises."[18] The exchange market aims to fast-track IPOs for Chinese tech firms in key sectors like AI, semiconductors, and biotechnology by relaxing regulations and restrictions on IPO pricing.

Meanwhile, in China's private equity market, the government uses a public-private funding mechanism, known as government guidance funds (GGF), to steer capital into strategic industries like AI.[19] The government is involved across the different stages of the funding process, from fundraising to investment to operation. A 2021 CSET report found that the government sets up the fund's target size and allocates 20–30 percent of the total funding target to attract private investors who may have too little appetite for the risk of investing in high-risk, high-reward sectors like emerging technologies.[20] Often, these private investors are state-owned enterprises and state-run banks. Finally, government-affiliated entities, such as management

[14] "2023 National "Specialized, Specialized, New" Little Giant Research Report" released: These companies may become the stars of tomorrow" [《2023 全国"专精特新"小巨人研究报告》发布：这些企业或成为明日之星], *21st Century Business Herald*, December 06, 2023, https://www.stcn.com/article/detail/1056972.html.
[15] "The central government's financial incentives and subsidies support the development of 'specialized, special and innovative' small and medium-sized enterprises - 10 billion yuan in red envelopes invested in 'little giant' firms" [中央财政奖补资金支持"专精特新"中小企业发展——100 亿元红包投向"小巨人"企业], *People's Daily*, February 6, 2021, https://perma.cc/RPY3-9ZLT.
[16] "The Report on the Development of Specialized, New Small and Medium Enterprises was Released [《专精特新中小企业发展报告》发布]," Zhongguancun Hi-Tech Technology Enterprise Association, September 19, 2022, http://www.cecc.org.cn/news/202209/569205.html.
[17] https://www.stcn.com/article/detail/1056972.html
[18] "Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035."
[19] Ngor Luong, Zachary Arnold, and Ben Murphy, "Understanding Chinese Government Guidance Funds," Center for Security and Emerging Technology, March 2021, https://cset.georgetown.edu/publication/understanding-chinese-government-guidance-funds/.
[20] Luong et al.,, "Understanding Chinese Government Guidance Funds."

institutions established by government agencies or state-owned investment firms, can also be found among the general partners who handle the day-to-day operations of the GGFs.

1.3.2. State Control and Influence over Non-state Firms

Within China's tech ecosystem, the state maintains close linkages between different military, public, and private actors, including under its military-civil fusion (MCF) policy. The Chinese government can assert control in and influence non-state firms by acquiring controlling stakes, directly subsidizing AI companies, establishing contract relationships with firms, and guiding private action by signaling its interests in specific industries of strategic importance.

The state can appear in Chinese non-state AI firms' ownership structure via investment common in the equity finance world. One way the state can take up shares in a non-state AI company is through its GGF investments. For instance, Chinese AI and facial recognition company iFlytek received a $2.9 million (18.5 million RMB) investment from Hefei Venture Capital Guidance Fund (合肥市创业投资引导基金), which accounted for nearly 8 percent of the company's equity shares in 2021.[21] Another way is through its state-owned companies. According to the financial database Refinitiv, AI and facial recognition company Hikvision, is 36 percent owned by CETHIK Group Co., Ltd., a subsidiary of SOE China Electronics Technology.

Beyond direct funding, the state can maintain close ties with non-state firms through contract relationships. China's MCF strategy has increasingly muddled the distinction between technologies developed in the military and civilian realm, or public sectors and private ones. In the implementation of MCF, the Chinese government's emphasis on developing AI systems for both military and civilian applications aligns with the dual-use nature of AI. Most AI systems are designed to have flexible models and customizable uses where users can fine-tune the model to their needs. There is evidence that AI systems developed by commercial entities can be adapted for military purposes to meet the needs of a government client. For instance, the People's Liberation Army (PLA) awarded 4Paradigm, a Chinese AI company, a contract to deliver decision-making and human-machine-teaming software in 2020.[22] According to its website, 4Paradigm offers products and services such as generative AI and decision-making AI that can be used in both civilian and military settings.[23]

To a lesser extent, the Chinese government sometimes relies on signaling to influence private capital flows in the commercial sector to serve the state's interests. The China Banking and Insurance Regulatory Commission plans to set up a "traffic light" system meant to guide private capital toward what the government deems as productive sectors, making clear the areas in which private investors can invest, while urging "firms to obey the Party's leadership."[24] For

[21] "关于科大讯飞股份有限公司非公开发行股票申请文件反馈意见回复报告" (About 'Report on Feedback of Application Documents for Non-Public Offering of iFlytek Co., Ltd.'), April 1, 2021, https://q.stock.sohu.com/cn,gg,002230,7014689930.shtml.
[22] Ryan Fedasiuk, Jennifer Melot, and Ben Murphy "Harnessed Lightning" (Center for Security and Emerging Technology, October 2021), https://cset.georgetown.edu/publication/harnessed-lightning/.
[23] "4Paradigm," 4Paradigm, https://www.4paradigm.com/.
[24] "Correctly Understand and Grasp the Characteristics of the Rules of Capital (People's Viewpoint) [正确认识和把握资本的特性和行为规律（人民观点）]," *People's Daily*, February 8, 2022, http://qh.people.com.cn/n2/2022/0208/c401598-35125876.html; Ella Cao And Kevin Yao, "China to increase

many Chinese VC or PE investors, following government signals when making investment decisions is likely their best bet. This is especially true as the Chinese government pushes for greater control of what it has referred to as a "disorderly expansion of capital."[25]

1.3.3. Funding Limitations

The Chinese government's efforts to control, influence, and support the development of AI in the commercial sector through the aforementioned range of funding mechanisms face a number of limitations. First, traditional industrial policy mechanisms like subsidies and emerging ones like GGFs are often plagued with corruption, inefficiencies, waste, and lack of coordination.[26] For example, one independent market research firm reporting on the implementation of GGFs found that "many regions have jumped on the bandwagon of establishing AI industry development funds, even though there are few local companies in the AI field."[27]

Second, there is tension between Beijing's expectations and market realities concerning public equity flows into Chinese companies. Despite financial incentives for localization, as of 2023, there were 252 Chinese companies listed on the New York Stock Exchange (NYSE), Nasdaq, and NYSE American, which are the three largest US stock exchanges.[28] A number of these companies have also opted for dual listing, which allows US investors to convert their shares into securities listed in Hong Kong to hedge against the uncertainty caused by heightened tensions between the United States and China.

2. Chinese AI Companies and the World

Over the past decades, the Chinese leadership has amassed the country's resources to improve its technology innovation system to compete globally. It has emphasized the ability to build indigenous capacity at home to gain a first-mover advantage and according to the AIDP, become the global center for AI by 2030.[29] Although it is difficult to compare the innovativeness of Chinese non-state AI firms to that of U.S. firms, it is clear that China has become a leader in AI research, based on metrics such as the number of research publications, citation counts, and participation in top AI conferences.[30] China also tops the list of global AI-related patent producers, which can be a useful (albeit imperfect) indicator of technological advancement and a linkage between science, technology, and commercial activity. As Chinese firms are ramping up their ability to compete globally, further monitoring of their activities and indicators of success can help improve our understanding of China's innovativeness.

support for private firms to bolster recovery," *Reuters*, July 19, 2023, https://www.reuters.com/markets/asia/china-increase-support-private-companies-bolster-economy-2023-07-19/.

[25] "Correctly Understand and Grasp the Characteristics of the Rules of Capital (People's Viewpoint)."

[26] Luong et al., "Understanding Government Guidance Funds."

[27] Luong et al., "Understanding Government Guidance Funds."

[28] "Chinese Companies Listed on Major U.S. Stock Exchanges," USCC, January 9, 2023, https://www.uscc.gov/research/chinese-companies-listed-major-us-stock-exchanges.

[29] Hannas, William, and Huey-Meei Chang. Chinese Power and Artificial Intelligence. 1st ed. Taylor and Francis, 2022; "Notice of the State Council on Issuing the New Generation Artificial Intelligence Development Plan."

[30] Such indicators and measures can be found on CSET's Emerging Technology Observatory (ETO)'s Country Activity Tracker (CAT): Artificial Intelligence, https://cat.eto.tech/?countries=China+%28mainland%29%2CHong+Kong&countryGroups=.

2.1. Chinese AI Firms' Investment and Research Ties to Other Countries

In addition to supporting Chinese non-state AI companies at home, the Chinese government also encourages them to seek opportunities abroad. The New Generation AI Development plan frames AI as "a new focus of international competition" and urges Chinese firms to "go out" into the global economy—namely, to invest and expand overseas.

In the investment world, Chinese AI companies, like others, often make strategic investments to benefit themselves, including gaining insights into the portfolio company's technology, establishing partnerships, or locking out a competitor. In the past 5 years, a number of leading Chinese AI companies, including tech giants like Baidu, Alibaba, and Tencent (BAT) as well as AI unicorns such as SenseTime, have been "going out" to invest in companies based in other countries (Appendix, Figure 1). For these companies, the top investment destinations include the United States and, to a lesser extent, the United Kingdom and Singapore. Tencent is slightly more active outside the Chinese border. It's important to note that investment is a two-way street. China, deeply connected to the global economy, sees companies like Tencent expanding their global financial footprints to fund and reap the benefits of technologies in other countries. At the same time, companies on the receiving end are also benefiting from Chinese AI companies' investments, especially when they can develop, scale, and commercialize their products.

Another way in which Chinese AI companies are establishing and deepening ties with the broader, global AI community is through collaborative research. For instance, according to CSET's merged corpus of scholarly articles, over the past five years, about half the English-language research papers published by some of China's leading tech companies, including BAT, SenseTime, ByteDance, and Yitu, were co-authored with foreign researchers (Appendix, Figure 2).[31] Such extensive collaboration between top Chinese AI firms and foreign researchers shows how much progress China has made in becoming a vital part of and a leader in the global research community.

2.2. China's Reliance on Foreign Tech

A 2022 CSET report by Ben Murphy on 35 Chinese tech chokepoints, namely, China's strategic technology import dependencies, found that the Chinese tech market, particularly in strategic areas such as photolithography machines and aviation design software heavily relies on foreign products. Take for example the aviation design software area. A Chinese scholar notes that "if foreign companies stop providing China with the software, the PRC aviation industry will be 'paralyzed.'"[32]

One of the explanations behind China's dependency, as the report points out, is that Chinese universities and labs struggle to link basic research with commercial applications.[33] While

[31] The AI papers analyzed here exclude a very high proportion of Chinese-language-only publications, so we are likely overestimating the percentages of collaborations. However, analysis of papers published in English-language publications, indicating prestige and a certain level of paper quality, still offers meaningful results.
[32] Ben Murphy, "Chokepoints: China's Self-Identified Strategic Technology Import Dependencies" (Center for Security and Emerging Technology, May 2022), https://cset.georgetown.edu/publication/chokepoints/.
[33] Murphy, "Chokepoints: China's Self-Identified Strategic Technology Import Dependencies."

Chinese universities and research institutes are not solely responsible for commercializing products, the Chinese government emphasizes the importance of translating AI research into practical applications. In 2021, Xi Jinping said, "Our capacity to convert S&T achievements [into practical applications] is weak" and declared that the country must accelerate the "application of independent innovation achievements."[34]

To address this dependence on foreign technologies and materials, the Chinese government has focused on policies aimed at achieving self-sufficiency such as the investment efforts discussed above. Through such investments and other political and financial support mechanisms, the Chinese government is consolidating its influence in both the domestic market and across the overseas markets where it has encouraged Chinese firms to "go out." Taken together, this combination of public, private, and public-private investment vehicles is meant to advance China's goal of becoming a self-sufficient technological power within the next decade.

3. China's AI Regulatory Environment

In recent years, the Chinese government has put forth a number of regulatory frameworks to govern the development and deployment of AI. These regulations focus on recommendation algorithms, synthetically generated content, and generative AI. These regulations highlight the Chinese state's focus on steering AI development to align with its interests and priorities, particularly in areas of information control for political, economic, and social stability. In doing so, Beijing is grappling with challenges in balancing between state control and state support for AI development.

Several of the Chinese government's policy documents since the launch of the AIDP in 2017 discuss general guidance for AI regulations and the layout of relevant issues.[35] However, three policy documents are key drivers behind the country's attempt at shaping the regulatory environment for AI development.

In 2021, four Chinese ministries jointly related the "Provisions on the Management of Algorithmic Recommendations in Internet Information Services."[36] This document emphasizes the role of the state in planning and coordinating the governance of algorithmic recommendation services. It prohibits algorithm recommendation companies from engaging in services that "endanger national security or the societal public interest, disrupt economic and social order, or harm the lawful rights and interests of others."[37] One provision is worth highlighting; article 13

[34] "Xi Jinping: Strive to Become the World's Primary Center for Science and High Ground for Innovation," translated by Ben Murphy, Rogier Creemers, Elsa Kania, Paul Triolo, and Kevin Neville, DigiChina, March 18, 2021, https://digichina.stanford.edu/work/xi-jinping-strive-to-become-the-worlds-primary-center-for-scienceand-high-ground-for-innovation/.
[35] Matt Sheehan, "China's AI Regulations and How They Get Made," Carnegie Endowment for International Peace, July 10, 2023, https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117.
[36] "Provisions on the Management of Algorithmic Recommendations in Internet Information Services," [国家互联网信息办公室、中华人民共和国工业和信息化部、中华人民共和国公安部、国家市场监督管理总局], CAC, December 31, 2021, http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm; English translation is available at https://www.chinalawtranslate.com/en/algorithms/.
[37] "Provisions on the Management of Algorithmic Recommendations in Internet Information Services."

restricts synthetically generated fake news information, underscoring the state's interest in controlling online news content.

Given the Chinese government's concern over artificially generated content, the Cyber Administration of China (CAC) released the "Provisions on the Administration of Deep Synthesis Internet Information Services" in 2022.[38] Through this document, the state articulated that deep synthesis (or deepfake) technology threatens China's information security, and therefore, activities that "endanger the national security and interests, harm the image of the nation, harm the societal public interest, disturb economic or social order, or harm the lawful rights and interests of others" are prohibited.[39] This regulation tracks with Beijing's efforts to prevent what it considers political and social disruption and enforce censorship and content regulations more broadly.

In 2023, CAC, the National Development and Reform Commission (NDRC), the Ministry of Education (MOE), the Ministry of Science and Technology (MST), the MIIT, and the Ministry of Public Security (MPS) issued "Interim Measures for the Management of Generative Artificial Intelligence Services."[40] These measures focus on text, image, audio, and video generated by large language models (LLMs) like OpenAI's ChatGPT, as well as on training data. Previously discussed documents on recommendation algorithms and deepfakes had laid the groundwork for content generation regulation. What's new in this document is the inclusion of measures to govern the data used to train generative AI systems. The quality and quantity of data is an important component that makes training deep learning models possible.[41]

As such, the Chinese National Information Security Standardization Technical Committee put together a draft for feedback, "Basic Safety Requirements for Generative Artificial Intelligence Services," addressing specific requirements for Chinese AI companies.[42] With respect to training data, the draft notes the use of a blacklist; data that contains over 5 percent of what is referred to as "illegal and unhealthy information" is deemed unsafe for training. From the compliance perspective, companies that build AI software will likely opt in for state-approved content, for instance from state-run media sources, to meet the threshold.

Based on the three AI regulatory frameworks, it is clear that the Chinese government aims to shape the development of AI to serve its interests, especially in the realm of information control

[38] "Provisions on the Administration of Deep Synthesis Internet Information Services" [国家互联网信息办公室 工业和信息化部 公安部], CAC, November 25, 2022, http://www.cac.gov.cn/2022-12/11/c_1672221949354811.htm; English translation is available at https://www.chinalawtranslate.com/en/deep-synthesis/.
[39] "Provisions on the Administration of Deep Synthesis Internet Information Services."
[40] "Interim Measures for the Management of Generative Artificial Intelligence Services" [国家互联网信息办公室 国家发展和改革委员会 教育部等], CAC, July 10, 2023, http://www.cac.gov.cn/2023-07/13/c_1690898327029107.htm; English translation is available at https://www.chinalawtranslate.com/en/generative-ai-interim/.
[41] Ben Buchanan, "The AI Triad and What It Means for National Security Strategy" (Center for Security and Emerging Technology, August 2020), https://cset.georgetown.edu/publication/the-ai-triad-and-what-it-means-for-national-security-strategy./
[42] "Basic Safety Requirements for Generative Artificial Intelligence Services (Draft for Feedback)" [生成式人工智能服务安全基本要求（征求意见稿）], Chinese National Information Security Standardization Technical Committee, October 11, 2023, https://cset.georgetown.edu/wp-content/uploads/t0574_generative_AI_safety_EN.pdf.

for political, economic, and social stability. The proposed regulations largely deal with the current and potential social, ethical, and economic impacts of AI on Chinese citizens, and the decision to focus early regulatory efforts on these areas reflects the state's desire to solidify its political legitimacy amid rapid technological changes. Finally, China wants the world to see itself as a leader in AI governance and is creating a regulatory environment domestically to shape an international one. Shan Zhiguang (单志广), director of the State Information Center of China's Information and Industrial Development Department, takes pride in China leading the release of measures to regulate generative AI and suggests inserting China's practices into the international framework.[43]

3.1. Domestic Factors Impacting China's AI Growth

China's efforts to regulate AI can provide firms with some degree of predictability and articulate government expectations in rapidly evolving and dynamic AI markets. As Carnegie Endowment's Matt Sheehan pointed out, China's AI regulatory frameworks will help shape the parameters for the future development of AI in the country.[44] For companies, regulations offer some assurance that the systems they develop will have a receptive market if they abide by the rules. Indeed, there is already some evidence that Chinese AI companies are developing technologies to adapt to the new rules. For instance, SenseTime is developing a "deepfake detection + digital watermark" ("深伪检测+数字水印") technology to prevent AI models from generating false content.[45]

At the same time, excessive regulation can stifle innovation and impose prohibitive compliance costs, especially on new and small companies. It is still too early to assess the actual impact of China's AI regulations on innovation in the country, but there is some evidence that Chinese AI companies are concerned about the costs of complying with expanding regulations. For instance, at a Chinese AI forum hosted by the Institute of Law of the Chinese Academy of Social Sciences and attended by key industry leaders, participants expressed concerns that AI companies will require not only technical teams for developing large models but also risk assessment teams to ensure compliance with the rules. They are also concerned that the overlapping rules and unclear bureaucratic authorities will add more pressure on companies developing and deploying AI across China.[46]

Other internal factors including economic slowdown and demographic changes are also impacting China's AI ecosystem. China's economy is expected to see an annual growth average of just 4.5 percent, with no signs of potential recovery to the 10 percent growth rate numbers that turned China into an economic powerhouse more than a decade ago.[47] The continuation of slow

[43] "Promoting the safe development of AI" [推动人工智能安全发展], *Xinhua*, January 3, 2024, http://www.news.cn/tech/20240103/da71ac3a00a34af588b9b515084d6739/c.html.
[44] Sheehan, "China's AI Regulations and How They Get Made."
[45] "Promoting the safe development of AI."
[46] "How can risk governance take into account innovation and safety when artificial intelligence legislation is being carried out?" [人工智能立法进行时 风险治理如何兼顾创新与安全？], *21st Century Business Herald,* December 19, 2023, https://www.21jingji.com/article/20231219/herald/70fc4a20d58e447ac91a6a590d10bff9.html.
[47] Greg IP, "Why Xi Can No Longer Brag About the Chinese Economy," *Wall Street Journal*, November 14, 2023, https://archive.is/L6bBJ.

and stagnant growth may impact the country's ability to finance major investments in emerging technologies. Local governments, which are important players in setting up and contributing initial capital to government guidance funds, are also facing financial pressures. With more local debt burdens, these guidance funds often struggle to meet their fundraising goals. Fundraising amounts saw a 35 percent drop in 2022 from the previous year.[48]

China's ability to innovate and its population problems are intertwined. Innovation needs talent. The current supply of AI workers is estimated to only meet 10 percent of the demand in the workforce.[49] The geographic distribution of available opportunities in the AI sector is another question. A 2023 CSET report assessing China's AI workforce found that in some provinces such as Shangdong and Henan, AI professionals who graduated from AI programs locally may struggle to find employment given the relatively low level of AI job demand in the area.[50]

Despite these challenges, the Chinese government continues to view technology as crucial for China's economic development, societal well-being, and geostrategic and military goals. Xi Jinping in 2018 said that "key technologies are the most important weapons of the country to promote high-quality economic development and guarantee our national security."[51] This political declaration is not a new phenomenon. Xi's predecessors have also stressed the idea of self-sufficiency to better guard against both domestic and global volatility. The high-level ambitions are clear but how the Chinese leadership will cope with these domestic challenges remains to be seen.

3.2. External Factors Impacting China's AI Growth

There are a number of external factors impacting China's ability to meet its AI goals, including U.S. export controls on advanced computing chips and related semiconductor manufacturing equipment. Access to advanced chips is critical in researching and developing advanced AI systems like LLMs, which often demand extensive computing power, and some evidence suggests that Chinese companies developing LLMs use Nvidia's chips more often than Chinese-made chips.[52] At least in the short term, U.S. export controls on advanced semiconductors will likely undercut China's AI advancement, including by forcing Chinese companies to use stockpiles of less advanced Chinese-made chips, which are not optimal for training LLMs.[53]

[48] Author's calculation from "Zero2IPO 2022 annual review: 120 new government guidance funds were established, and integration and optimization became the norm" [清科 2022 年度盘点：新设立政府引导基金 120 支，整合优化成常态], Zero2IPO, https://pdf.dfcfw.com/pdf/H3_AP202302151583167286_1.pdf?1676457061000.pdf.
[49] TAKASHI KAWAKAMI, "China's shortfall in AI tech talent estimated in the millions," *Nikkei Asia*, September 14, 2023, https://asia.nikkei.com/Business/China-tech/China-s-shortfall-in-AI-tech-talent-estimated-in-the-millions.
[50] Dahlia Peterson, Ngor Luong, and Jacob Feldgoise, "Assessing China's AI Workforce: Regional, Military, and Surveillance Geographic Job Clusters" (Center for Security and Emerging Technology, November 2023), https://cset.georgetown.edu/wp-content/uploads/CSET-Assessing-Chinas-AI-Workforce.pdf.
[51] "Xi Jinping: Core Technology is the Most Important Weapon of the Country [习近平：关键核心技术是国之重器]," Xinhua, July 15, 2018, https://perma.cc/3XVT-U6C2.
[52] Helen Toner, Jenny Xiao, and Jeffrey Ding, "The Illusion of China's AI Prowess," *Foreign Affairs, June 2, 2023,* https://archive.is/hfgV8.
[53] Hanna Dohmen Jacob Feldgoise, "A Bigger Yard, A Higher Fence: Understanding BIS's Expanded Controls on Advanced Computing Exports," CSET, December 4, 2023, https://cset.georgetown.edu/article/bis-2023-update-explainer/.

Second, the U.S.'s 2023 outbound investment executive order (EO) restricting venture capital and private equity (VC/PE) investment in China could also impact the country's AI development. Although the EO narrowly scopes the restriction to companies working on military applications of AI, its impact may extend beyond that. In recent years, the Chinese VC/PE market has been maturing thanks to government support and foreign capital and networks, including those from the United States.[54] If U.S. VC firms become reluctant to continue investing in China, they will also be denying the investment expertise and networks that benefit the Chinese VC players. Investments from big VC firms, especially those in the United States, may convey a credible signal of a firm's quality to other parties. For example, Intel Capital's investment in Chinese Easy Tech raised the profile of this AI chip company, resulting in more investment from state-backed Zhuhai S&T VC firm.[55] It is possible that with more limited access to U.S. expertise and networks, Chinese AI companies may face challenges in finding investors to fund their prototypes and products.

U.S. restrictions on tech export and investment could also add to the pessimism about the economic and technological outlook in China. In response to these restrictive measures, Chinese AI companies and investors may look to grow their financial and technology footprint in regions like Southeast Asia with its growing tech base, potentially at the expense of investment in the domestic AI ecosystem.[56] There is evidence that Chinese entrepreneurs and wealthy individuals who could be funders are leaving China, especially for Singapore.[57] That said, external factors such as restrictive U.S. measures on semiconductor exports and AI investment screening are also adding more pressure on Beijing to push forward with its self-sufficiency policies in order to guard against these external changes.

4. Economic and national security implications for the United States

China's rapid advancement in AI, fueled by significant state support, can pose economic and security challenges to the United States. In particular, China's progress in commercial AI applications can also support its military modernization efforts in a way that threatens U.S. national security. The United States has implemented measures to restrict Chinese access to U.S. technologies and know-how, capital, and markets. To ensure current and future U.S. policies toward China meet their goals, it is crucial to regularly assess China's AI capabilities and their impact on U.S. competitiveness. I recommend the following actions for U.S. policy:

1) **U.S. policymakers need accurate, evidence-based assessments of China's technological power.** Open-source intelligence (OSINT) collection and analysis, for instance, can help augment our understanding of China's science and technology capabilities, including in emerging technology areas such as AI. CSET experts have recommended establishing a center, outside of the intelligence community, to collect

[54] Emily S. Weinstein and Ngor Luong, "U.S. Outbound Investment into Chinese AI Companies" (Center for Security and Emerging Technology, February 2023), https://cset.georgetown.edu/wp-content/uploads/CSET-U.S.-Outbound-Investment-into-Chinese-AI-Companies.pdf.
[55] Weinstein and Luong, "U.S. Outbound Investment into Chinese AI Companies."
[56] Ngor Luong Margarita Konaev, "In & Out of China: Financial Support for AI Development," CSET, August 10, 2023, https://cset.georgetown.edu/article/in-out-of-china-financial-support-for-ai-development/.
[57] Jason Douglas , Keith Zhai and Stella Yifan Xie, "As China Reopens, Flight of Wealthy Chinese to Singapore Set to Accelerate," *Wall Street Journal,* February 27, 2023, https://archive.is/6lGIp.

open-source intelligence, monitor, analyze, and share information with allies and partners on China's S&T capabilities.[58]

2) **To restrict U.S. capital and intangible benefits from aiding the development of China's AI used for military purposes, the United States should carefully scope the outbound investment program spearheaded by the Department of Treasury.** According to the Treasury's accompanying advanced notice of proposed rulemaking (ANPRM), prohibited transactions currently cover investments in companies that are engaged "in the development of software that incorporates an AI system and is designed to be exclusively used for military, government intelligence, or mass-surveillance end uses." In a public comment in response to the Treasury's ANPRM, CSET, the Center for New American Security (CNAS), and the Atlantic Council recommend a revision to the scope of end use-based prohibited transactions to reflect the dual-use nature of AI systems, replacing "exclusively used" with "intended, entirely or in part, for use in military, government intelligence, or mass-surveillance end uses."[59] While there are AI systems designed specifically for military purposes, most are designed to have flexible models and customizable uses where users can fine-tune the model to their needs. There is evidence that Chinese military entities have acquired AI systems that are not exclusively designed for military uses. For instance, in 2020, 4Paradigm secured a contract to provide intelligent algorithm models, metadata classification software, and knowledge discovery software.[60] 4Paradigm is not exclusively a military AI company, but its products are nonetheless being sold to the Chinese military.

   I also recommend an entity-based approach to prohibit U.S. investments in AI for military purposes. This approach would prevent the U.S. government from having to determine which AI systems are designed for military purposes. It accounts for the fact that AI systems are made more harmful based on the entity developing or using such systems. An entity-based approach can also offer a tool that is similar to the Bureau of Industry and Security (BIS)'s "know your customer" guidance.[61] A list of problematic entities may also make compliance easier for the industry since it would not be left up to interpretation on a company-by-company basis. Without such guidance, one firm could decide that a transaction should be prohibited on the basis of end use restrictions, while another may disagree and choose to pursue the transaction, which could put the companies that conduct extensive due diligence at a competitive disadvantage.

[58] Owen J. Daniels, "CSET Analyses of China's Technology Policies and Ecosystem: The PRC's Efforts Abroad" (Center for Security and Emerging Technology, September 2023), https://cset.georgetown.edu/wp-content/uploads/20230036_The-PRCs-Efforts-Abroad_FINAL9.20.2023.pdf; Dewey Murdick, Ph.D., "Testimony before the Senate Select Committee on Intelligence: Countering the People's Republic of China's Economic and Technological Plan for Dominance," Center for Security and Emerging Technology, May 11, 2022, https://cset.georgetown.edu/wp-content/uploads/2022.05.11-Testimony-before-theSenate-Select-Committee-on-Intelligence.pdf.

[59] Emily Kilcrease, Tim Fist, Sarah Bauerle Danzman, Ngor Luong, and Emily Weinstein, Comments on Provisions Pertaining to U.S. Investments in Certain National Security Technologies and Products in Countries of Concern (September 29, 2023), https://www.regulations.gov/comment/TREAS-DO-2023-0009- 0049.

[60] Fedasiuk et al., "Harnessed Lightning."

[61] "Supplement No. 3 to Part 732—BIS's "Know Your Customer" Guidance and Red Flags," Code of Federal Regulations, accessed on November 25, 2023, https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-732/appendix-Supplement%20No.%203%20to%20Part%20732.

3) **The United States should coordinate with its allies and partners to track the flow of venture capital and private equity investments into Chinese AI companies.** To increase the effectiveness of U.S. outbound investment restrictions on certain technologies in China, there is a need to coordinate with allies and partners that also have investments in China's AI ecosystem. CSET research found that Chinese AI companies also attract investment from foreign investors other than the United States. Any unilateral U.S. action will be weaker without the help of U.S. allies and partners.

   Since the launch of the 2023 EO restricting U.S. capital into China's technologies, the United States has made some progress with U.S. allies and partners at the strategic level, but specific coordinated actions on how to develop and implement this outbound investment screening are further needed. We see the Group of Seven (G7) releasing a statement noting the importance of forming appropriate measures to address outbound investment concerns related to emerging technologies.[62] In a joint declaration, the United States and the United Kingdom also agreed to address their concerns over capital flow into China's technologies.[63] But additional information sharing between key U.S. allies, such as on transactions of concern, can make coordination efforts more effective, avoid overextending U.S. jurisdiction, and help countries learn from each other's experiences.[64]

I would like to thank Daniel Chou, Danny Hague, Rebecca Gelles, Margarita Konaev, and Igor Mikolic-Torreira for their assistance in preparing for this testimony. All errors are mine.

[62] "G7 Leaders' Statement," White House, December 6, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/12/06/g7-leaders-statement-6/#:~:text=We%20recognize%20that%20appropriate%20measures,that%20threaten%20international%20peace%20and.

[63] "Addressing the national security risks posed by certain types of outbound investment," United Kingdom Government, June 21, 2023, https://www.gov.uk/government/publications/the-atlantic-declaration/addressing-the-national-security-risks-posed-by-certain-types-of-outbound-investmen.

[64] Ngor Luong Emily S. Weinstein, "A Guide to the Proposed Outbound Investment Regulations," CSET, October 6, 2023, https://cset.georgetown.edu/article/a-guide-to-the-proposed-outbound-investment-regulations/.

5. Appendix

Figure 1: Select Chinese AI companies' investments outside of China (2019-2023)

AI company	Investment transactions outside of China	All investment transactions	Percentage of investment transactions outside of China
Tencent	222	407	54.6%
Alibaba	37	98	37.8%
ByteDance	8	52	15.4%
Baidu	4	24	16.7%
SenseTime	1	12	8.3%

Source: CSET analysis of Crunchbase

Figure 2: Select Chinese AI companies' AI collaboration with foreign researchers (2019-2023)

AI company	AI papers in collabation with foreign researchers	All AI papers	Percentage of AI papers in collaboration with foreign researchers
Alibaba	2,379	2,732	87%
Tencent	1,287	3,083	42%
Baidu	631	1,460	43%
ByteDance	208	349	60%
Sensetime	117	256	46%
iFlytek	52	167	31%
MEGVII	40	168	24%
Yitu Technology	28	45	62%
Horizon Robotics	17	44	39%
CloudWalk Technology	4	11	36%

Source: CSET's Merged Academic Corpus

OPENING STATEMENT OF MICHELLE ROZO, VICE CHAIR, NATIONAL SECURITY COMMISSION ON EMERGING BIOTECHNOLOGY

DR. ROZO: Thank you so much. Thank you to Co-Chair Wessel and Co-Chair Helberg, and members of the U.S.-China Economic and Security Review Commission.

Thank you for inviting me to testify about U.S.-China competitiveness and biotechnology. And I am delighted to be here to share the work that we are currently undertaking at the National Security Commission on emerging biotech.

We just released our interim report. I encourage everyone to check that out at biotech.senate.gov.

I come to my role as vice chair of the commission as a molecular biologist by training. I studied stem cells in my graduate work and then infectious diseases before serving in government.

And I, along with my 11 fellow commissioners, spanning members of Congress, industry executives, academics, and former government officials are currently examining the opportunities and challenges facing the United States at the critical intersection of national security and emerging biotechnology.

One of the challenges we are finding is the risk of being overmatched by China. With recent advances in biotechnology, we are beginning to be able to program cells like we program computers. And the applications here go far beyond the pharmaceutical domain. These technologies can be applied across our economy to agriculture, to energy, to industrial production, manufacturing and, of course, defense and military applications.

The CCP is keenly aware of the potential here and are investing heavily across these domains. Losing ground risks ceding an enormous geopolitical advantage. But we still have time. We haven't yet hit the ChatGPT moment for this technology. We can see it coming though. And this race is on.

Continued U.S. leadership in biotechnology is not guaranteed. And we are seeing indicators that China is catching up and in some critical subfields may be surpassing us. So the time to act really is now.

Our Commission is modeled after the National Security Commission on Artificial Intelligence, which was created well before the recent advances in large language models. This was by design. Congress intended that the AI Commission provide context and policy options to legislators before it was too late.

And similarly, Congress has recognized that we are almost to an inflection point with biotechnology and informed our Commission accordingly.

So as I mentioned, we have just completed our first year of work and delivered our interim reports after engaging with hundreds of stakeholders. And this report lays out our plan for the year ahead.

So of some of what we found so far. There are significant roadblocks in the United States that could harm our ability to reach that ChatGPT moment, if you will. It still takes too long and costs far more than it should to move a biotech product from lab to market.

There is a lack of both physical infrastructure here and the workforce required to operate it and regulatory improvements are necessary alongside advances in technologies.

In contrast, the CCP is making serious investments and true policy decisions that could put it on the track to outpace us. China's last three five-year plans have prioritized biotechnology, and

their governments have invested billions of dollars in the sector, by some accounts over $100 billion.

They are employing a familiar playbook, the Huawei playbook if you will. R&D spending, talent recruitment program, state supported enterprises, licit and illicit acquisition of intellectual property. And this top down approach may serve China well in the biotech race where high risk tolerant investing and state support for enabling capabilities and infrastructure could allow them to confront -- to overcome the barriers confronting progress in the United States.

So one example where this Chinese strategy may be already paying dividends is at the critical intersection of AI and biotechnology.

AI is revolutionizing biotechnology, and it is likely that this future ChatGPT moment for the field will be because of this convergence between these two technologies.
And I will say that the Chinese system may be better oriented towards this AI and bionexus than ours. For example, Chinese policies have co-located AI and bio researchers to foster collaboration. They have established biomedical clusters, which contain AI and bio researchers and companies.

They recognize that AI models depend on good quality and large scale data sets and accordingly have established large scale biological databases, including the Chinese National GeneBank, which is a biorepository hosting tens of millions of biological samples along with their genetic information.

And their biodata programs have also benefitted from talent coming back from U.S. universities and the U.S. National Institutes of Health. And both AI and biotech have been major priorities for China's foreign talent programs.

These policies are paying off. There are leading edge Chinese players in industry. For example, BioMap, co-founded by the owner of Baidu, has developed the first bio in AI foundation model to hit 100 billion parameters according to their online marketing. They call this the largest of its kind.

China is building domestic capabilities in AI and bio that could provide a long-term strategic and geopolitical advantage. And in contrast, we have not yet prioritized this intersection at a national level.

Another example of CCP policy is for biotech in action is the support of BGI or Beijing Genome Institute, or the Huawei of DNA sequencing. This may provide China with advantages in this critical subfield and, of course, the associated biological data because for biotech, data truly is the new oil.

The CCP supports BGI. For example, a $1.5 billion, 10 year loan in 2010 led to its growth as a national company. And today BGI operates in the U.S. and partners with hospitals, universities and other research organizations.

U.S. researchers often look for low cost genomic sequencing services. It makes sense. And BGI can provide this, thanks in part to large state subsidies.

These unfair economic practices could position BGI to drive competitors out of the market. And with data security laws that require Chinese companies like BGI to share data with the government and a publicized partnership with the Chinese military, U.S. biological data may be fueling China's economic and national security priorities.

So I have to share two examples that demonstrate that China is using familiar tactics to try and win out in biotech. However, unlike the sectors that came before, 5G, we have time to act before we may be surpassed.

And as we led in our interim report, there are policy options that we are considering to address challenges to biotech progress that exist in the United States, including how to prepare the U.S. government for the age of biology, how to accelerate domestic innovation as well as how to protect against the technologies misuse.

We will provide our formal recommendations in our final report in December 2024, and I look forward to the discussion today and answering your questions.

COMMISSIONER WESSEL: Mr. Nadaner?

PREPARED STATEMENT OF MICHELLE ROZO, VICE CHAIR, NATIONAL SECURITY COMMISSION ON EMERGING BIOTECHNOLOGY

U.S.-China Economic and Security Review Commission hearing on “Current and Emerging Technologies in U.S.-China Economic and National Security Competition”

Prepared statement by

Michelle Rozo, Vice Chair
National Security Commission on Emerging Biotechnology

Co-chair Wessel, Co-chair Helberg, and members of the U.S.-China Economic and Security Review Commission, thank you for inviting me to testify before the Commission about U.S.-China competitiveness in biotechnology, biomanufacturing, and related technologies. The National Security Commission on Emerging Biotechnology (NSCEB) is exploring the opportunities and challenges facing the United States at the intersection of national security and emerging biotechnology. Our interim report, released earlier this month, discusses our findings thus far and the research plan that will inform our comprehensive policy recommendations to be issued in 2024.[1]

Like the introduction of computers, biotechnology is a tool with the potential to revolutionize multiple economic sectors. Biotechnology—the application of living organisms in science or engineering—already solves problems today, like improved cancer treatment, agricultural sustainability, and novel types of materials. The United States can do more to integrate biotechnology across the domestic economy so that Americans are reaping the economic and security benefits that biotechnology can offer. Failing to meet this moment will have far-reaching consequences, especially because we have a strategic competitor that seeks to control critical supply chains and dominate key elements of the biotechnology industry.

Based on what we are seeing, China recognizes that advancements in biotechnology—such as DNA synthesis, gene editing, and precision fermentation—are essential to meeting the needs of their population and to competing globally. These same technologies could be used for nefarious purposes: China has expressly invested in biotechnologies that create military advantages. While any country can target technology areas for investment, we have seen a more nefarious side of China’s use of biotechnology. They have used biotechnology related advancements to support military purposes, acquire personal data, and surveil and control their own populations.[2]

China’s last three Five-Year Plans have prioritized biotechnology, and China has invested billions of dollars in the sector. Some estimate that China’s central, provincial, and local governments have collectively invested over $100 billion into the life science sector.[3] Most recently, China’s ‘14th Five-Year Plan for Bioeconomy Development’

describes China's intentions to use biotechnology and other life sciences to strengthen its economy, especially biomanufacturing.[4] The plan describes the importance that China sees in merging artificial intelligence (AI) and biotechnology, as well as the need for both political and financial support, stating "[w]e will promote the integration and innovation of biotechnology and information technology, accelerate the development of biomedicine, bioengineered breeding, biomaterials, bioenergy, and other industries and increase the size and strength of the bio-economy." In this plan, China sets a goal of increasing the scale and usage of biotechnology in multiple sectors by 2025. China aims for its bioeconomy to "be at the forefront globally" by 2035.[5]

China's Methods to Pursue Dominance

The United States is a global leader in biotechnology, but that status is increasingly threatened by China's strategic actions. China is positioning itself as a leader in biotechnology in order to increase their self-sufficiency and take advantage of associated economic and military benefits. China views biotechnology as the next industrial revolution and key to future economic development and comprehensive national power. This state support goes far beyond the traditional industrial policies implemented in Europe and other parts of Asia. China's strategy is comprehensive and represents an alternative blueprint for the development of emerging technologies and industries. China's all-embracing approach plays a key role in fostering technology areas that rely on longer timelines, multidisciplinary coalitions, or big science facilities—such as advanced computing, high-end gene sequencing, and colonies of non-human primates.

Over the last two decades, China has put in place policies to support the Chinese biotechnology industry, including: relatively high research and development (R&D) spending, talent recruitment programs, expansion of state-owned and state-supported enterprise, licit and illicit acquisition of intellectual property (IP), central government strategy and coordination, preferential tax treatment, subsidies, and government procurement initiatives. China is on the path to becoming a biotechnology superpower thanks to its long-term commitment to building an innovation base that includes industrial clusters and interdisciplinary research labs which collect and analyze extraordinary amounts of genomic and other "omic" data, and leverage its collaborations with foreign entities—much like its strategy to develop 5G.

Research Funding

The Chinese government heavily supports later stage R&D and translational research, often using basic research conducted in the United States as its starting point. In contrast, the U.S. Government funds basic research, and has historically taken a relatively hands-off approach to translational research. A system that funds translational research is better poised to realize applications in certain biotechnology sectors, including agriculture, industrial, and defense. In a way, China is taking advantage of American basic R&D by heavily funding translational research, while the United States relies on the market (mature pharma/biotechnology companies and VC-backed startups) to conduct translational work.

According to the Center for Strategic and International Studies, China's R&D spending on basic and applied research lags behind other major powers.[6] China's basic and applied research investment was $77 billion in 2018, compared to $200 billion in the United States. Chinese basic research averaged 5% of total R&D expenditure in 2000 to 2018, while the share of applied research dropped from 17% to 11%. Over the same time frame, U.S. R&D funding included 17% for basic research and 20% for applied research. China consistently spends most of its R&D resources on experimental development, using existing knowledge to improve products and processes. China's experimental development averaged 80% of R&D from 2000 to 2019, compared to 62% for the United States.

Talent Recruitment Programs

To achieve its goal of becoming a world leader in science and technology by 2050, China has orchestrated a coordinated campaign of hundreds of party- and state-sponsored talent programs. These talent programs are meant to bring back Western trained experts to drive China's research and cultivate China's domestic talent pool in support of civilian and military goals outlined in central government strategic plans. A recent study highlights how China's technology-transfer professionals, the so-called science and technology diplomats, broker technology-transfer deals and coordinate with overseas experts to fulfill technology wish lists for Chinese entities. More than half of the 642 projects examined in the study were biotechnology or AI projects.[7]

The most prominent program is the Thousand Talents Plan, which incentivizes individuals engaged in science and technology to work overseas to bring their expertise to China in exchange for Western level salaries, research funding, lab space, and more. According to a 2019 staff report from the Senate Committee on Homeland Security and Governmental Affairs' Permanent Subcommittee on Investigations, members of the Thousand Talents Plan misappropriated U.S. Government funding, provided research ideas to their Chinese employers, stole intellectual capital from U.S research before it was published and engaged in IP theft.[8] The Thousand Talents Plan is an example of one of China's premier talent programs; other programs operate at provincial, local, and academic levels.

China's talent programs take advantage of the United States' openness and target U.S. pre-competitive basic research, critically impacting the U.S. economy and competitiveness. Talent programs have been enormously successful as one of the primary means of misappropriating IP. China's IP theft machine steals an estimated $600 billion in IP every year, including from U.S. companies active in the national security field. Participants in talent programs are obligated to recruit new members. Normal, seemingly innocuous activities, such as contacting a researcher to provide a lecture in exchange for an honorarium can lead unsuspecting researchers to innocently participate in activities that benefit China and are designed to recruit them for talent programs. At present, there are no existing U.S. laws that makes it illegal for researchers to participate in a talent program. Tackling this scale of IP theft requires a whole-of-government effort and cooperation with universities and industry.

State-Owned and State-Supported Enterprise

Chinese state-owned enterprises have broad freedom to operate in the United States and can own land, sell products (e.g., seeds and software) directly to U.S. consumers and farmers, and access tax incentives, grants, and loans. At the same time, China prohibits foreign investment in biotechnology, mergers and acquisitions by foreign companies, foreign seed sales, technology licensing, and land ownership.[9] State-owned enterprises regularly interact with U.S. officials and influence policy matters without restriction as members and leaders of international trade associations.

The U.S. Department of Defense has identified multiple major Chinese biotechnology companies as Chinese military companies, including BGI Group (BGI), ChemChina, and SinoChem, which we discuss below. In addition, the Department of Commerce added BGI to the Export Administration Regulation's Entity List, noting that "their collection and analysis of genetic data poses a significant risk of contributing to monitoring and surveillance by the government of China, which has been utilized in the repression of ethnic minorities in China. Information also indicates that the actions of these entities concerning the collection and analysis of genetic data present a significant risk of diversion to China's military programs."[10] Both Syngenta and BGI subsidiary, MGI, have taken steps to conceal their connections to the Chinese government.[11,12]

Acquisition of Intellectual Property and Data

While China has made great strides in its domestic biotechnology capabilities and development strategies, they invariably incorporate technology transfer as a key component of dominating the field. China is working to access critical IP and data through a variety of legal and illegal means. Acquiring trade secrets through espionage has contributed to China's biotechnology advancement, and in some cases, Chinese scientists have stolen IP rather than conduct the research themselves. In other cases, Chinese companies have simply purchased U.S. companies with the goal of acquiring IP or data.[13,14]

Key Biotechnology Domains for China

Below, we describe China's methods to pursue dominance and key domains that are particularly important for biotechnology, including: sequencing technology, AI, agricultural biotechnology, and military applications.

Sequencing Technology

DNA sequencing technology is critical for the future of biotechnology. DNA sequencing is the process of determining the order of individual bases in a sample of DNA. Determining this genetic sequence can help identify an organism or understand some of its properties. This technology is indispensable for applied fields such as biotechnology, virology, and medical diagnosis, and is used in routine biotechnology research to help understand what genes do. As such, DNA sequencing technologies and services are foundational for emerging biotechnologies and could be considered a chokepoint or bottleneck. Especially important is that the future of DNA sequencing is evolving, for

example, new technologies that are proficient at reading longer stretches of DNA (e.g. nanopore-based sequencing) are changing the landscape.

DNA sequencing costs have fallen dramatically, to less than $600, to sequence a human genome. The increased accessibility has led to a proliferation of genomic data and biotechnology innovation. The global DNA sequencing market was estimated to be about $8.91 billion in 2022 and is expected to grow by 20% through 2030.[15] Academic research accounted for over half of revenue, and North America accounted for about half of the market.

There are two major aspects of the sequencing market – selling the instruments for genome sequencing (U.S.-dominated) and then selling genomic sequencing services (major U.S. companies do not provide this type of service, but some Chinese companies do). A critical differentiation in the sequencing market is that companies that provide sequencing services potentially have access to the genetic information provided by the customer, while users of sequencing instruments can potentially keep the genetic information that is produced in-house. Major players in the space include U.S.-based Illumina, Thermo Fisher Scientific, and Agilent Technologies, along with China-based BGI and its global network of over one hundred subsidiaries, including MGI (referred to collectively in this document as BGI). Illumina represents 80% of the DNA sequencing market globally, and primarily sells instruments for genome sequencing.

Similar to Illumina, BGI manufactures instruments for genome sequencing. In addition, they provide sequencing as a service, with sequencing facilities in China, Hong Kong, and Europe. By providing sequencing services in facilities in China, BGI has access to customer genomic data that could be directed towards the interests of the Chinese Communist Party (CCP).[16] The growth and success of BGI demonstrates not only the holistic nature of China's science and technology industry, combining the private and public sectors and the military, but also how sustained support can affect a key emerging industry.[2] These collaborations give BGI—and China—access to genomic data worldwide.

State-Owned and State-Supported Enterprise

China has been taking steps to boost Chinese companies and to acquire biotechnology companies both in the United States and elsewhere. In the sequencing space, BGI has publicly stated that "none of BGI Group is state-owned or state controlled, and all of BGI Group's services and research are provided for civilian and scientific purposes."[11] However, BGI has published at least twelve joint studies with the People's Liberation Army since 2010.[2] BGI has always been well connected and favored by the CCP, starting as state-backed lab at the Chinese Academy of Sciences before it was spun off to participate in the Human Genome Project in 1999. BGI leverages its ties to the government to develop products for the global market. For example, the Non-Invasive Fetal Trisomy Test (NIFTY) for prenatal testing of Down syndrome was developed by scientists from BGI, with hospitals and universities contributing to the project.[17] BGI has also been involved in more controversial activities for the Chinese government, such as the collection of genomic data from China's ethnic minorities in Xinjiang and Tibet.[18]

Several Chinese laws have favored BGI. For example, the Chinese government is required to only purchase from domestic corporations, which has been beneficial to BGI. BGI has received considerable Chinese state funds and support, including the Chinese government entrusting BGI to build and operate the China National GeneBank, the Chinese government's national genetic database. This partnership leverages the sequencing capability of BGI to form a biorepository hosting tens of millions of samples from humans, plants, animals, and microorganisms; banking DNA to "support science and technology development".[19] A $1.5 billion 10-year loan from the China Development Bank in 2010 allowed BGI to gain the world's largest sequencing capacity through purchase of 128 high-end Illumina-brand sequencers.[20] With Chinese state support, BGI expanded its operations through the acquisition of U.S.-based Complete Genomics in 2013, after review by the Committee on Foreign Investment in the United States (CFIUS). This provided BGI with the equipment and capabilities to compete with Illumina internationally.[21] In 2021, BGI received over $30 million in subsidies from Chinese state funds.[22] Government loans have been critical for BGI's growth.

Acquisition of Data

China views genetic data as a national resource and uses variety of means to ensure access. Through extensive partnerships with U.S. healthcare providers and researchers, BGI has provided large-scale genetic sequencing services for medical research efforts. U.S. researchers often look for low-cost providers of these services, which BGI can provide, thanks in large part to state subsidies; in February 2020, BGI said it could sequence a human genome for just $100.[23] These partnerships provide BGI with more genetic data on more diverse sets of people that they can use for more products and services, further intrenching their market position. Further, while it is unclear if clinical data is obscured, genetic information can be used to identify an individual.

While these partnerships give BGI access to genetic information, more nefarious means are also employed to gain access to data. In 2015, 78.8 million personal records were stolen from Anthem, a U.S. health insurer. The U.S. Department of Justice indicted two individuals in China, and an intelligence assessment showed that the Chinese government has directed actions to acquire genetic data from around the world.[24]

Internationally, Chinese institutions used the COVID-19 pandemic as an opportunity to create partnerships and donated or sold BGI equipment to eighty countries.[25] These capabilities may boost countries' diagnostics and research, but they also provide a means to collect genomic data that China otherwise would not have access to. BGI has also partnered with the Bill and Melinda Gates Foundation through a memorandum of understanding to work on genetics studies for human health and agriculture.[26]

Acquisition of Intellectual Property

While BGI is the largest Chinese sequencing company, multiple Chinese startups are using technology that can be traced back to the United States and other countries such as Canada and the United Kingdom, with little restriction. For example, Fapon Biotech acquired U.S.-based SequLite, and GeneMind has licensed IP from U.S.-based Helicos.

WuXi PharmaTech acquired the US firm NextCODE Health in 2015, which allowed integration of NextCODE's genome sequence analysis platform with WuXi's next-generation sequencing capabilities, and increased WuXi access to U.S. doctors and patients.[27]

As mentioned above, in 2013, BGI acquired U.S. sequencing company Complete Genomics, gaining proprietary sequencing technology and a U.S. base of operations. Illumina had made a competing bid for Complete Genomics, but the Federal Trade Commission (FTC) had antitrust concerns as Illumina was becoming a dominant presence in the market. Though some national security concerns were raised, CFIUS cleared the acquisition.[28]

Biotechnology-Artificial Intelligence Nexus

The use of AI and machine learning (AI/ML) to enhance research and encourage breakthrough discoveries through the combination of AI and biotechnology (AIxBio) has advanced over the last several decades.[29] Nearly every area of biology has advanced through the use of AI/ML tools, and will continue to do so as the data and models improve. AI has the potential to revolutionize biotechnology across all sectors. These tools help researchers and developers understand and interpret the genetic code, analyze images for farming and medical diagnostics, and run autonomous experimentation to increase the speed of cutting-edge research. These tools are important because they will increasingly impact every area of biotechnology research—from driving discovery, to automating experimentation, to streamlining scale-up manufacturing. Often it is the investments we make today, as well as the data that we acquire, that will have the biggest impacts in the future.

It is difficult to fully assess where we are vis-à-vis China in AI or biotechnology but there are elements that suggest that this is a close race. There are numerous AIxBio companies that are looking to leverage AI for biotech applications and products and there are leading-edge Chinese players in the field. For example, Insilico Medicine, with dual headquarters in Hong Kong and New York City, has become one of the biggest global players in AIxBio. The company claims that its use of AI in pharmaceutical development reduced a multiyear, hundreds of millions of dollars discovery process to 18 months at a fraction of the cost of traditional drug development[30]. Additionally, BioMap, co-founded by the owner of Baidu, has developed the first life science AI Foundation Model to hit 100+ billion parameters, which they call they "largest of its kind". As described by BioMap, "model training is enabled by our world-leading super-computing center and enhanced by our AI-centric, 100,000 sq ft, high-throughput wet labs."[31]

It appears that the Chinese system is better oriented towards convergent AIxBio research. The Chinese government has been prioritizing this intersection at a national level for years, while the U.S. Government has yet to do so at the same scale. China's actions in the AIxBio sector demonstrate how China leverages its own research funding, talent programs, and market access to both acquire technology in the short term and develop its domestic capabilities, which could provide a longterm strategic and geopolitical advantage.

Talent Recruitment Programs

AI models depend on good quality and large-scale data sets. China's National Genomics Data Center, founded in 2019, benefits from returned talent that have direct experience in leading U.S. universities and the U.S. National Institutes of Health (NIH). The center acts as a clearinghouse for China's genetic data, with a genome sequencing archive and branches with portfolios in precision medicine and agriculture. Many of its leading scientists have trained abroad and are members of China's various talent programs, often while still employed by their Western university. One of its leading scientists was selected for the Chinese Academy of Sciences 100 Talents Program while still working at the NIH.

Acquisition of Intellectual Property

Chinese investors are supporting AIxBio firms, many with ties to talent programs that could enable IP transfer. For example, ZhenFund is an early-stage investor, whose leadership partners with Chinese state-sponsored talent programs and start-up contests. ZhenFund has invested in numerous AI companies, some of which are in the biotechnology space. These include SYNYI-AI, a smart hospital solutions provider; Deep Intelligent Pharma, a firm pursuing pharmaceutical discovery and development through AI; and CareAI, a bioinformatics technology and high-performance computing company. AI-biotechnology firm XtalPi Technology, based in China with a Boston branch, also received investments from Zhenfund after winning a cash prize at the Harvard College China Forum Pitch Competition.[32] XtalPi provides drug R&D services for pharmaceutical firms using computational physics, quantum chemistry, AI, and cloud computing; all three of its co-founders were MIT postdoctoral researchers, recruited through China's talent programs.[33]

Agricultural Biotechnology

Agricultural biotechnology is another key area of interest, as it can be used to increase yields and improve sustainability; increase food quality and nutrition; protect against pests and diseases; and cultivate alternative food sources. China has been a net importer of agricultural products since 2004, and today imports more agricultural products—including soybeans, corn, wheat, rice, and dairy—than any other country. Accordingly, China considers food security an integral part of national security.[34] China aims to increase self-sufficiency by increasing domestic production through use of biotechnology and other methods, reducing dependance on imports, and increasing influence on agricultural production in other countries. Increased corn and soybean production within China would reduce China's dependency on U.S. products, potentially resulting in more challenging market conditions for U.S. farmers.

In recent years, China has become the largest funder of agricultural R&D in the world, surpassing the United States and the European Union.[35] In 2019, China applied for 22% of all international patents, surpassing the United States as the global leader. In particular, China applied for agricultural patents that use the genome editing tool, CRISPR.[36] While the number of patents does not necessarily indicate tangible advancements, it does indicate China's increasing interest in agricultural biotechnology.

To date, low yields, poor soil, water scarcity, low adoption of modern farming practices, and other problems are holding China back from meeting its goals.[37]

The potential weaponization of animal and plant disease to harm agriculture is a longtime concern. With advances in biotechnology, combined with access to U.S. agricultural data and IP, an adversary could develop a disease that selectively targets U.S. crops or livestock. The U.S. Government has established interagency approaches to prepare for, respond to, and recover from biological incidents, including those that target U.S. agriculture.[38]

State-Owned and State-Supported Enterprise

China is strategically positioning its companies to control more and more market share in the agriculture sector. During 2015 to 2020, consolidation in the agriculture sector reduced the number of major global companies from six to four and major U.S.-based companies from three to one. Today, just four companies control agricultural biotechnology and other agricultural inputs: U.S.-based Corteva, German-based Bayer and BASF, and China-owned Syngenta.

In 2017, state-owned ChemChina purchased then Swiss-based seed-producing giant Syngenta. CFIUS cleared the acquisition in 2016. At the time, agricultural stakeholders outlined many concerns with the merger, including that Chinese state-ownership of Syngenta would create a unique conflict of interest in which the Chinese government would be both approving and marketing genetically engineered (GE) crops and agrochemicals. Others warned that a Chinese state-owned Syngenta could withhold ongoing biofuel advancements from the U.S. military, and that many Syngenta facilities are near U.S. military facilities. Bipartisan members of the Senate Committee on Agriculture, Nutrition, and Forestry noted: “It is not unreasonable to suggest that shifts in company governance; operational strategy; or financial health…could have consequences for food security, food safety, biosecurity, and the highly competitive U.S. farm sector as a whole.”[39]

In 2020, China began combining agricultural assets of ChemChina and another state-owned company, Sinochem, under the Syngenta name. The resulting state-owned Syngenta will be the world’s largest seed and agrochemicals conglomerate, with $27 billion of annual sales and unprecedented global influence.[40] Syngenta is also planning a $10 billion initial public offering (IPO) to facilitate Chinese government-directed acquisition of global agricultural technology companies.[41]

Uneven Biotechnology Regulation

China’s ownership of Syngenta allows the Chinese government to both develop and approve seeds and agrochemicals, while disadvantaging and delaying approvals of U.S. and other foreign-developed products. China has taken steps to facilitate approvals of GE crops for domestic cultivation, and published their first regulations on gene-edited crops, providing a clear path to domestic cultivation and marketing. Simultaneously, China is working to improve Chinese public opinion of agricultural biotechnology, in

advance of more wide-scale plantings of Chinese-developed GE crops. China is also advancing regulations for biotechnology in animal agriculture.

While expanding its own ability to develop, produce, and potentially export GE crops, China delays or declines import approval for foreign-developed GE crops. Biotechnology developers will not market a GE crop in the United States prior to approval by major U.S. export markets, due to concerns about rejection of grain at the ports. This means that China effectively controls what technologies U.S. farmers can use in their fields. In January 2023, the Chinese government approved imports of eight GE crops after a decade-long wait, allowing U.S.-based Corteva to market a now-outdated GE canola variety to U.S. farmers.[42]

China's power over U.S. farmer access to GE crops is largely due to litigation that found then-Swiss-based Syngenta responsible for marketing to U.S. farmers GE seed that was approved in the U.S. but not yet approved by Chinese regulators. From 2013 to 2014, China's rejections of U.S. GE corn shipments contributed to a steep drop in grain prices. Syngenta ultimately settled with farmers and grain companies for $1.51 billion in 2017.[43]

Acquisition of Data and Intellectual Property

U.S. farmers' use of Chinese-made drones and apps allows the Chinese government access to farmers' data, including agricultural productivity data and high-resolution images of U.S. critical infrastructure. China leverages its scientists and businesspeople to acquire technology and technological knowledge. For example, Chinese operatives have stolen IP and sensitive agricultural trade secrets from U.S. firms, including by gaining access through education and employment in the United States and by physically digging up research seeds from U.S. fields.[44] China also requires large physical samples of viable GE seed when a company seeks import approval, far more than would be needed for routine testing. Using U.S. data and seeds, China can develop its own versions of American seed varieties in a fraction of the time.

Military Biotechnology

Advancing biotechnology is a stated goal of the U.S. Department of Defense as it provides opportunities for new methods of producing products in the military supply chain, as well as for creating new or improved products with enhanced capabilities. Biological systems can be used for biomanufacturing of products in the defense supply chain, for example in the critical chemicals that the Department of Defense uses to make lubricants, fuels, or energetics, on which it now relies on foreign or sole sources. Biological systems can also produce novel products, such as materials that trap and prevent toxic chemicals from affecting soldiers. Biomanufacturing on-demand could enable logistics in contested environments, for example through engineered microbes that can transform waste streams like plastics into critical supply chain components like fuels. Biotechnology can be used to generate novel materials, for example fabric resembling spider silk could make lighter, stronger, and more flexible body armor, allowing warfighters to operate under reduced physical strain. Biological sensors could

recognize a chemical or biological agent in real time and engineered human enzymes could deactivate nerve agents in the body.

However, biotechnology can also be applied for military usage in ways that run counter to the policies and goals of the United States, for example to produce a biological weapon. Additional potential future military capabilities enabled by biotechnology include augmented solider performance, brain-computer interfaces, as well as advanced biological weapons.

As the U.S.-China Economic and Security Review Commission has previously noted, China is prioritizing advancement in critical and emerging technologies because these technologies could lead to substantial scientific breakthroughs, economic disruption, enduring economic benefits, and rapid changes in military capabilities and tactics. Under the national policy of “military-civil fusion,” Chinese officials state that information and technology that are obtained in civilian sectors will be used to benefit the military and military applications. China’s pursuit of biotechnology could enable a range of military capabilities.

Specific Recommendations

The National Security Commission for Emerging Biotechnology is identifying policy options to address some of these concerns. The Commission will provide a full range of recommendations in our comprehensive report, to be provided to Congress in December 2024 and continuing through the duration of the Commission, which ends in June 2026. Our January 2024 report described our scope of research, which spans a wide range of topics related to biotechnology. We are considering how to better prepare the U.S. government for the age of biology, including by: leveraging international partners and allies, growing bioliteracy of the U.S. Government workforce, improving U.S. Federal interagency coordination, and harmonizing the U.S. system for biotechnology product oversight. We are looking at policy options to accelerate innovation and embrace biotechnology, including by: scanning the horizon for new and emerging technologies, leveraging biological data for future innovation, building an ecosystem conducive to innovation, increasing American bioliteracy, and bolstering the U.S. biotechnology workforce. Finally, we are identifying ways to protect against misuse of biotechnology, including by: promoting reasonable and responsible governance and preventing, detecting, and responding to misuse.

We also provided a policy proposal to strengthen ties between national security agencies and the U.S. Department of Agriculture. Amid rising concerns about China’s investment in U.S. agricultural companies and land, and both licit and illicit acquisition of intellectual property, particularly in agricultural biotechnology, U.S. agricultural groups have argued that food security should be considered part of national security. While the United States has some means in which to prevent or mitigate acquisitions by Chinese companies, these acquisitions continue to occur for biotechnology companies, including for sequencing technology. The United States cannot only rely on broad export controls to protect technologies due to the complexity of Chinese subsidiaries and the speed in which they can shift their business to avoid consequences from sanctions.

In the course of our research to date, the Commission identified that the United States lacks understanding of China's capabilities in biotechnology as a whole. We have some understanding of China's capabilities in the pharmaceutical sector, such as their recent move from "fast follower" to leader in CAR-T immuno-oncology therapies. CAR-T therapies now represent 10% of new drugs developed by Chinese companies, compared to 2% of drugs developed by U.S. companies.[45] We know less about China's work in industrial, agricultural, and other areas of biotechnology. Overall, it appears that the United States is not tracking China's advances in biotechnology the same way that it is tracking other technologies, such as AI and hypersonics. Additional intelligence in this sector will improve our ability to implement policies that respond to threats. For example, information that determines how much the U.S. Federal Government relies on Chinese-owned products and services is important to craft policies that could limit critical dependencies.

In addition to potential economic and food security risks, there is an ongoing contest to determine who will shape global norms and values around research, development, and deployment of biotechnology. Ultimately, there is a risk that adversaries may develop and weaponize biotechnology against the United States. Military applications could pose threats to American forces in the not-too-distant future. As with other technologies that have the potential for weaponization, preventing misinterpretation of each other's actions and intent is essential for the safe development of biotechnologies. For example, with the increased reliance on digital systems, nations have created normative and legal structures for optimizing the opportunities of the digital era while deterring cyberattacks. Though biotechnology is significantly different from cybertechnology, there are commonalities with cybersecurity in that both technologies can be used for civilian and defense purposes, and agreement upon and understanding of state actors' use of biotechnologies for civilian purposes can help prevent misinterpretation that could lead to escalation.

1 National Security Commission on Emerging Biotechnology. (2023). Interim Report. https://www.biotech.senate.gov/press-releases/interim-report/
2 Needham, K. & Baldwin, C. (2021). Special Report: China's gene giant harvests data from millions of women. Reuters. https://www.reuters.com/investigates/special-report/health-china-bgi-dna/
3 Moore, S. (2020). China's role in the global biotechnology sector and implications for U.S. policy. Brookings Institution. https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_china_biotechnology_moore.pdf
4 Zhang, X., Zhao, C., Shao, M., Chen, Y., Liu, P., & Chen, G. (2022). The roadmap of bioeconomy in China. Engineering Biology, 6(4), 71–81. https://doi.org/10.1049/enb2.12026
5 China Daily. (2022) Bioeconomy prominent on growth agenda. State Council, People's Republic of China. https://english.www.gov.cn/policies/policywatch/202205/11/content_WS627b169ec6d02e533532a879.html
6 China Power Project. (2021). Is China a Global Leader in Research and Development? Center for Strategic and International Studies. https://chinapower.csis.org/china-research-and-development-rnd/
7 Fedasiuk, R., Weinstein, E. & Puglisi, A. (2021). China's Foreign Technology Wish List," CSET, Georgetown University. https://cset.georgetown.edu/publication/chinas-foreign-technology-wish-list/
8 Senate Committee on Homeland Security and Governmental Affairs' Permanent Subcommittee on Investigations. (2019). Threats to the U.S. Research Enterprise: China's Talent Recruitment Plans.

https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/2019-11-18%20PSI%20Staff%20Report%20-%20China's%20Talent%20Recruitment%20Plans%20Updated2.pdf
9 Congressional Research Service. (2021). China's Recent Trade Measures and Countermeasures: Issues for Congress. https://crsreports.congress.gov/product/pdf/R/R46915
10 Bureau of Industry and Security, Department of Commerce. (2023). Additions and Revisions of Entities to the Entity List. https://public-inspection.federalregister.gov/2023-04558.pdf
11 Worldecr. (2023). China genetics company – 'not state owned or controlled' – challenges Entity List inclusion. https://www.worldecr.com/news/china-genetics-company-not-state-owned-or-controlled-challenges-entity-list-inclusion/
12 Earley, N. (2023). State orders a Chinese-state owned Syngenta Seeds to divest ownership of Arkansas farmland: China-state owned is reason. Arkansas Democrat Gazette. https://www.arkansasonline.com/news/2023/oct/18/state-orders-a-chinese-state-owned-company-to/
13 Chafetz, G. (2023). How China's Political System Discourages Innovation and Encourages IP Theft. SAIS Review of International Affairs. https://saisreview.sais.jhu.edu/how-chinas-political-system-discourages-innovation-and-encourages-ip-theft/
14 Bhattacharjee, Y. (2023). The Daring Ruse That Exposed China's Campaign to Steal American Secrets: How the downfall of one intelligence agent revealed the astonishing depth of Chinese industrial espionage. New York Times. https://www.nytimes.com/2023/03/07/magazine/china-spying-intellectual-property.html
15 Grand View Research. DNA Sequencing Market Size, Share & Trends Analysis Report By Product & Services (Consumables, Instruments), By Application (Oncology, HLA Typing), By Technology, By Workflow, By End-use, By Region, And Segment Forecasts, 2023 – 2030. https://www.grandviewresearch.com/industry-analysis/dna-sequencing-market
16 Baker, G. (2020). The Chinese Communist Party Targets the Private Sector. Center for Strategic and International Studies. https://www.csis.org/analysis/chinese-communist-party-targets-private-sector
17 Jiang, F., Ren, J., Chen, F. et al. (2012). Noninvasive Fetal Trisomy (NIFTY) test: an advanced noninvasive prenatal diagnosis methodology for fetal autosomal and sex chromosomal aneuploidies. BMC Med Genomics 5, 57. https://doi.org/10.1186/1755-8794-5-57
18 Warrick, J. & Brown, C. (2023). China's quest for human genetic data spurs fears of a DNA arms race. Washington Post. https://www.washingtonpost.com/world/interactive/2023/china-dna-sequencing-bgi-covid/
19 Wang B, et al. (2019). The China National GeneBank—owned by all, completed by all and shared by all. Yi Chuan. 41(8):761-772. https://pubmed.ncbi.nlm.nih.gov/31447427/
20 Illumnia. (2010). BGI Purchases 128 Illumina HiSeq(TM) 2000 Sequencing Systems. https://emea.illumina.com/company/news-center/press-releases/2010/1374343.html
21 Bouley, J. (2012). Complete Genomics Inc. to be acquired by Chinese firm BGI-Shenzhen for $117.6 million. Drug Discovery News. https://www.drugdiscoverynews.com/complete-genomics-inc-to-be-acquired-by-chinese-firm-bgi-shenzhen-for-117-6-million-6603
22 Needham, K. (2021). Chinese state fund invests in gene firm BGI. Reuters. https://www.reuters.com/article/us-china-genomics-state/chinese-state-fund-invests-in-gene-firm-bgi-idUSKBN2AM0AT/
23 Regalado, A. (2020). China's BGI says it can sequence a genome for just $100. MIT Technology Review. https://www.technologyreview.com/2020/02/26/905658/china-bgi-100-dollar-genome/
24 National Counterintelligence and Security Center. (2021). China's collection of genomic and other healthcare data from America: risks to privacy and U.S. economic and national security. https://www.dni.gov/files/NCSC/documents/SafeguardingOurFuture/NCSC_China_Genomics_Fact_Sheet_2021revision20210203.pdf
25 BGI. (2020). BGI Group Helping Over 80 Countries for Timely COVID-19 Detection and Intervention. https://www.bgi.com/us/news/video/bgi-group-helping-over-80-countries-for-timely-covid-19-detection-and-intervention
26 BGI. (2012). BGI and the Bill & Melinda Gates Foundation Sign Memorandum of Understanding on Collaboration for Global Health and Agricultural Development. PR Newswire. https://www.prnewswire.com/news-releases/bgi-and-the-bill--melinda-gates-foundation-sign-

memorandum-of-understanding-on-collaboration-for-global-health-and-agricultural-development-171139691.html
27 Brennan, Z. (2015). WuXi jumps into genomic analysis, bioinformatics with $65m acquisition. Outsourcing Pharma. https://www.outsourcing-pharma.com/Article/2015/01/12/WuXi-jumps-into-genomic-analysis-bioinformatics-with-65m-acquisition
28 Genome Web. (2012). National Security Concerns over BGI Bid for Complete Genomics. https://www.genomeweb.com/blog/national-security-concerns-over-bgi-bid-complete-genomics
29 National Security Commission on Emerging Biotechnology. (2023). AIxBio White Paper 1: Introduction to AI and Biotech. https://www.biotech.senate.gov/press-releases/aixbio-white-paper-1-introduction-to-ai-and-biotech/
30 Betuel, E. (2021). AI drug discovery platform Insilico Medicine announces $255 million in Series C funding. TechCrunch. https://techcrunch.com/2021/06/22/a-i-drug-discovery-platform-insilico-medicine-announces-255-million-in-series-c-funding/
31 BioMap. The Foundation Model. https://www.biomap.com/
32 Harvard College China Forum. Pitch Competition. https://www.harvardchina.org/pitch
33 XtalPi. About XtalPi. https://www.xtalpi.com/en/about
34 Branson, A. (2023). Top Ag Policy Document Outlines Key Agricultural and Rural Development Priorities. U.S. Department of Agriculture. https://apps.fas.usda.gov/newgainapi/api/Report/DownloadReportByFileName?fileName=Top%20Ag%20Policy%20Document%20Outlines%20Key%20Agricultural%20and%20Rural%20Development%20Priorities_Beijing_China%20-%20People%27s%20Republic%20of_CH2023-0026
35 Nelson, K. & Fuglie, K. (2022). Investment in U.S. Public Agricultural Research and Development Has Fallen by a Third Over Past Two Decades, Lags Major Trade Competitors. U.S. Department of Agriculture. https://www.ers.usda.gov/amber-waves/2022/june/investment-in-u-s-public-agricultural-research-and-development-has-fallen-by-a-third-over-past-two-decades-lags-major-trade-competitors/
36 Cohen, J. & Desai, N. (2019). With its CRISPR revolution, China becomes a world leader in genome editing. Science News. https://www.science.org/content/article/its-crispr-revolution-china-becomes-world-leader-genome-editing
37 Liu, Z. (2023). China Increasingly Relies on Imported Food: That's a Problem. Council on Foreign Relations.https://www.cfr.org/article/china-increasingly-relies-imported-food-thats-problem
38 White House. (2022). National Biodefense Strategy and Implementation Plan. https://www.whitehouse.gov/wp-content/uploads/2022/10/National-Biodefense-Strategy-and-Implementation-Plan-Final.pdf
39 U.S. Senate Committee on Agriculture, Nutrition, and Forestry. (2016). Senators Call On Treasury Department To Review ChemChina's Acquisition of Syngenta. https://www.agriculture.senate.gov/newsroom/dem/press/release/senators-call-on-treasury-department-to-review-chemchinas-acquisition-of-syngenta-
40 Jia, H. (2020). ChemChina and Sinochem will combine their agriculture assets. Chemical and Engineering News. https://cen.acs.org/food/agriculture/ChemChina-Sinochem-combine-agriculture-assets/98/i2
41 Ellis, J. (2021). This year's biggest agrifoodtech IPO will probably involve a company you've definitely heard of. AgFunderNews. https://agfundernews.com/syngenta-aims-to-raise-10bn-in-shanghai-ipo-at-60bn-valuation-report
42 Patton, D. & Polansek, T. (2023). Cautious China approves GMO alfalfa import after decade-long wait. Reuters. https://www.reuters.com/markets/commodities/china-approves-import-bayers-gmo-alfalfa-corteva-canola-after-decade-2023-01-13/
43 Begemann, S. (2018). Syngenta Settles MIR162 Case for $1.51 Billion. Farm Journal. https://www.agweb.com/news/crops/corn/syngenta-settles-mir162-case-151-billion
44 Bennett, C. (2021). While America Slept, China Stole the Farm. Farm Journal. https://www.agweb.com/news/business/technology/while-america-slept-china-stole-farm
45 Pharmaceutical Technology. (2022). Tracking the rise of CAR-Ts in China: the dawn of an immunotherapy superpower? https://www.pharmaceutical-technology.com/features/tracking-the-rise-of-car-ts-in-china-the-dawn-of-an-immunotherapy-superpower/

OPENING STATEMENT OF JEFFREY NADANER, SENIOR VICE PRESIDENT OF GOVERNMENT RELATIONS, GOVINI

DR. NADANER: Co-Chairs Helberg and Wessel, Honorable Commissioners, I appreciate this opportunity to speak about building Chinese resistant battery supply chains in the United States.

In March 2021, I returned to the private sector after serving as Deputy Assistant Secretary of Defense for Industrial Based Policy.

I saw significant, indeed alarming, vulnerabilities of the United States, vis-a-vis China, in several industrial sectors crucial to the readiness and capability of the U.S. military and America's overall economic and national security.

These, of course, included semiconductors and microelectronics, critical minerals, and closely-related advanced batteries. Here we are talking about the most technically advanced mid-size batteries needed to operate not just automobiles but those also required for distributed military weapon systems such as satellites, directed energy, UAVs and I could go on, and also critical infrastructure for our civilian economy, transportation to wastewater.

Some three years later, the U.S. government over two administrations through the executive and legislative branches has acted to remediate some of these U.S. vulnerabilities concerning battery technologies, components and materials.

Now one might quibble about the particulars, but collectively, they constitute a series of steps in the right direction. Nonetheless, fundamental American weaknesses remain and will continue for advanced batteries. And that is our dependence, in some cases directly and in most cases indirectly, on China for crucial phases of the battery supply chain. And that starts with mineral extraction, moves to processing -- I can't stress processing enough -- and then ends after numerous stages with a fully integrated battery.

I bring your attention to the data that I brought here today, Figures 1 to 6, from Govini's RKI, showing intensely rising U.S. imports from China of lithium and nickel cadmium batteries, battery parts, and primary battery cells.

The one partially positive trends is the emergence of Korea as a hefty exporter in addition to China of battery parts. However, I say that the Korean factor is only partially positive because Korea in turn has large dependencies on Chinese suppliers.

The situation is the same or worse for allies Japan, Germany, and Taiwan, all of whom supply us with battery components.

Finally, many of the battery supply chains from which the federal government draws have huge underlying Chinese dependencies. Even when the known supplier, the company that is being contracted with seems fine and is headquartered in the U.S. or an ally like Japan or France, still the underlying dependency is China.

Batteries represent a prime example of how China's manufacturing competitiveness has evolved over the past decade. China, having bought or pilfered Western technology in years past is now at the forefront of development and innovation. This stems from its many cycles of experience and expertise in complex manufacturing, which has no substitute.

Several U.S. firms with promising battery technologies existed around a decade and a half ago, however, federal incentives dried up. Permitting obstacles, which I will speak about more later, remain unabated. We failed to counter predatory Chinese trade practices and subsidies. And the nascent EV market was too small.

In recent years, bipartisan concern has grown. And I think it is useful to break the battery supply chain from an upstream through midstream through downstream for our purposes.

Most U.S. public attention on batteries aims to re-slice slices of the midstream and the downstream phases of battery manufacturing. The midstream includes the production of -- you take Chinese source anodes and turn them into cells, and Chinese source cathodes and turn them into modules. The downstream includes fabricating the cells and modules in the packs and then integrating the packs into a finished battery.

Now with a boost in state and federal incentives over the last few years, we have seen a number of battery cell and pack plants open up around the United States. However, the impression of a growing domestic battery manufacturing industry is partially misleading. In reality, essential parts of the battery of subcomponents and materials originate in China.

Recognizing that realistically we cannot do everything at once to secure this entire vital supply chain, the place to start is the point of maximum Chinese control, and that is maximum Western vulnerability.

And this is the critical but often neglected upstream mineral extraction and mineral processing and then the early stage of the midstream, fabricating refined materials into positive and negative electrodes, electrolytes, and separators.

Today at the upstream, China is the world's dominant processor of copper, nickel, manganese, cobalt, and lithium, and I could go on. And that is despite the fact that they have limited geological deposits within their borders.

In the midstream, Chinese entities dominate not only the production of anodes, cathodes, electrolytes, and separators, but also the invertors, foils, binders and cooling equipment that are essential to turning these cathodes, anodes, electrodes, and separators into cells.

The number of companies in the world that have mastered these processes are relatively few, most are Chinese, all involve intricate manufacturing, all are capital intensive.

Nonetheless, these manufacturing steps are considered low value in the United States under the business paradigm that came to dominate us over the last few decades. Yet, there are no lithium batteries without owning those phases of the process.

As the U.S. has learned in other crucial industrial sectors, just because a particular item or material is cheaply produced or extracted elsewhere does not mean that we do not need some level of domestic capacity. We certainly don't think about energy that way.

The U.S. Department of Defense faces the same battery supply chain challenges and vulnerabilities as the private sector but with vastly added complications and concerns.

The U.S. military shift toward distributed operations, stealthier vehicles, long duration uncrewed systems, above air, on the ground, water, electronic warfare, and large constellations of small satellites have swelled the demand for advanced batteries.

Yet, as with microelectronics, the military's relatively tiny share of domestic battery demand limits the military's market power to shape supply chains. The DOD is far from being even a 1 percent consumer of the battery market of the United States. It is just a tad more than zero percent.

Addressing the national battery problem, commercial defense requires speed and above all scale. We need a sense of wartime urgency like we did with the Apollo Space Program and Operation Warp Speed for the COVID vaccine. And trying to focus on export investment controls will not suffice.

Today it is astonishingly difficult in the U.S. and some of our allies to break the all-important processing sector. And it is impossible to compete solely on course. Mineral

processing is energy intensive and involves strong chemicals and potentially produces hazardous waste.

Building a new environmentally clean processing facility is possible today. But it will cost several hundred millions dollars and, in some cases, more than a billion. And that is if the construction is even allowed.

The permitting regulations associated with the National Environmental Policy Act, NEPA, which governs the building of just about anything of any size in this country, effectively serve as an automatic break, if not a barrier, to building a complete domestic supply chain for advanced batteries.

I commend the work of Noah Smith, a non-partisan economist analyst who has written extensively on NEPA. And he describes our predicament because of NEPA in particular as a build nothing country.

What are my recommendations? Well, one set takes the form of tax incentives. That is a well-constructed tariff, tax credits for capital expenditures, and channeling unrealized capital gains into the battery sector.

A sine qua non is imposing a much stiffer tariff on Chinese batteries and all components of Chinese origin. And we need to impose that tariff even on friendly trading countries so they will not be pass-throughs.

If they adopt the same tariff we do, then we can waive the tariff. The goal is not here to create a tariff block against our allies but rather against China.

COMMISSIONER WESSEL: If you could finish up --

DR. NADANER: Yes, sir.

COMMISSIONER WESSEL: -- then we will get back to the recommendations and questions and answers as well.

DR. NADANER: In addition, there are trillions of unrealized capital gains siting on the sidelines that ought to be freed up for the domestic mineral processing industry.
Unlike direct incentives, and I want to stress this, tax incentives keep the pivotal decisions in the hands of entrepreneurs and ordinary Americans rather than government officials. And there needs to be serious reform of NEPA.

Finally, I want to state that the many assumptions about pollution are based on dated assumptions of five decades ago. What was a dirty process could be a very clean one today. And the Department of Defense needs -- if it wants specific military batteries, it is going to have to put real dollars behind contracts.

So in short, we have outsourced whole industries, including the battery industry. It will take years to unwind these vulnerabilities. But there are things that we could do very quickly that could reverse this situation.

Thank you, sir.

COMMISSIONER WESSEL: Thank you.

PREPARED STATEMENT OF JEFFREY NADANER, SENIOR VICE PRESIDENT OF GOVERNMENT RELATIONS, GOVINI

Jeffrey Jeb Nadaner, Ph.D.
Senior Vice President, Government Affairs, Govini

Testimony on Current and Emerging Technologies in
U.S.-China Economic and National Security Competition
before the
U.S.-China Economic and Security Review Commission

Building Chinese-Resistant Battery Supply Chains
February 1, 2024, Statement as Prepared (1-31-2024)

Co-Chairs Helberg and Wessel and honorable Commissioners:

In March 2021, I returned to the private sector after serving as Deputy Assistant Secretary of Defense for Industrial Base Policy. In that post, I saw the significant, indeed alarming, vulnerabilities of the United States relative to the People's Republic of China in several crucial industrial sectors crucial to the readiness and capability of the U.S. military and to America's overall economic and national security. Those included microelectronics (semiconductors), critical minerals and, closely related, advanced batteries, which will be the focus of my testimony today. Here we are talking about the most technically advanced mid-sized batteries needed to operate not just automobiles, but also those required for distributed military weapons systems (satellites and UAVs) and critical infrastructure (from transportation to wastewater).

Some three years later, the U.S. government over the last two administrations – via policy and funding, through the executive and legislative branches – has acted to remediate U.S. vulnerabilities concerning battery technologies, components, and materials. One might quibble with the particulars, but collectively, they constitute a series of steps in the right direction. Nonetheless, the fundamental American weakness remains and will continue for advanced batteries. That is, our dependence – in some

cases directly, in most cases indirectly – on China at crucial phases of the supply chain that starts with mineral extraction, moves to processing, then to making components, and ends, after numerous stages, with battery assembly.

Here is telling data from Govini's Ark.ai, the software platform that uses leading-edge artificial intelligence and machine learning to solve supply chain challenges in acquisitions, production, and sustainment.

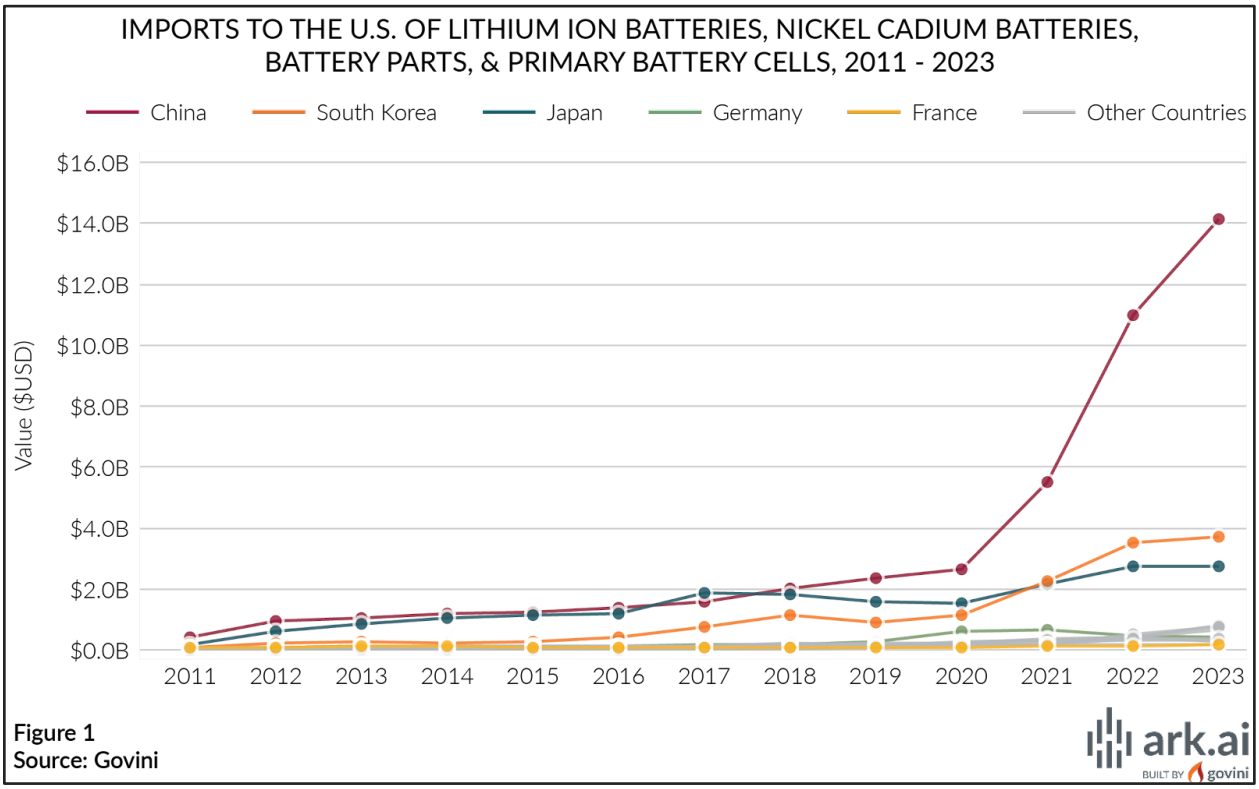


Figure 1
Source: Govini

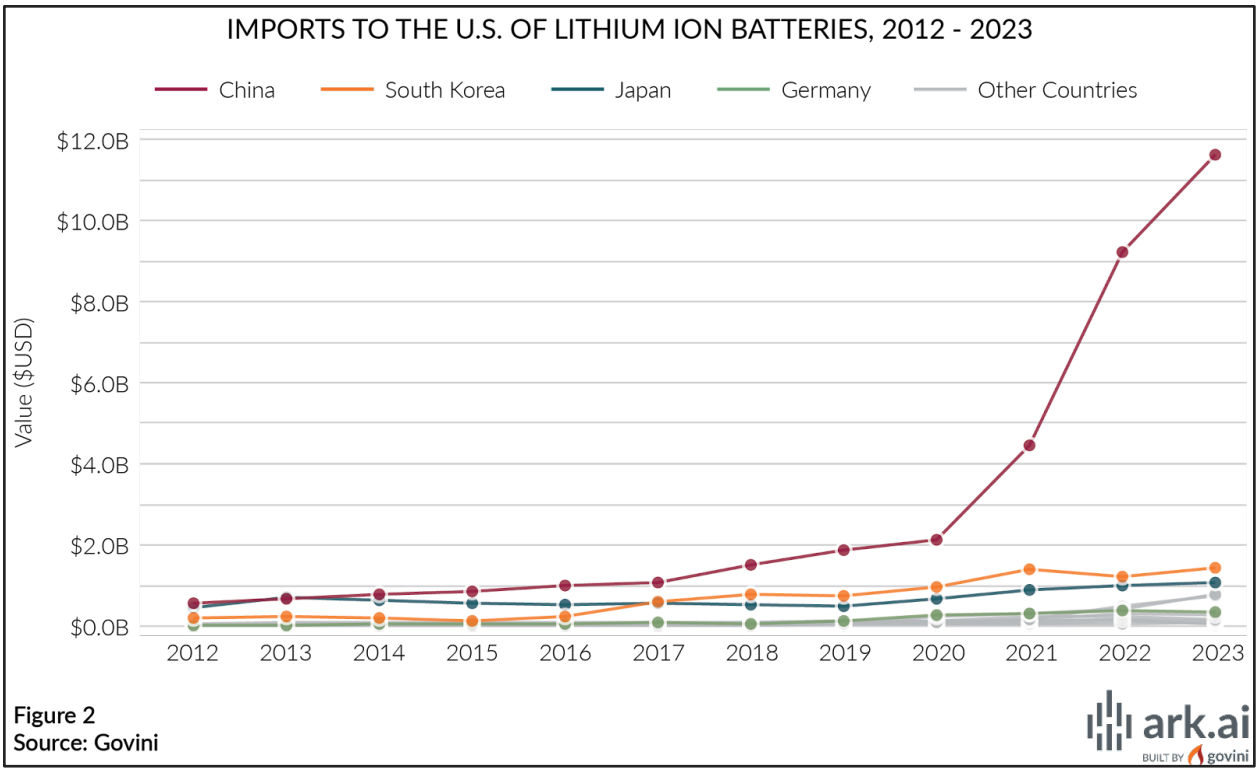


Figure 2
Source: Govini

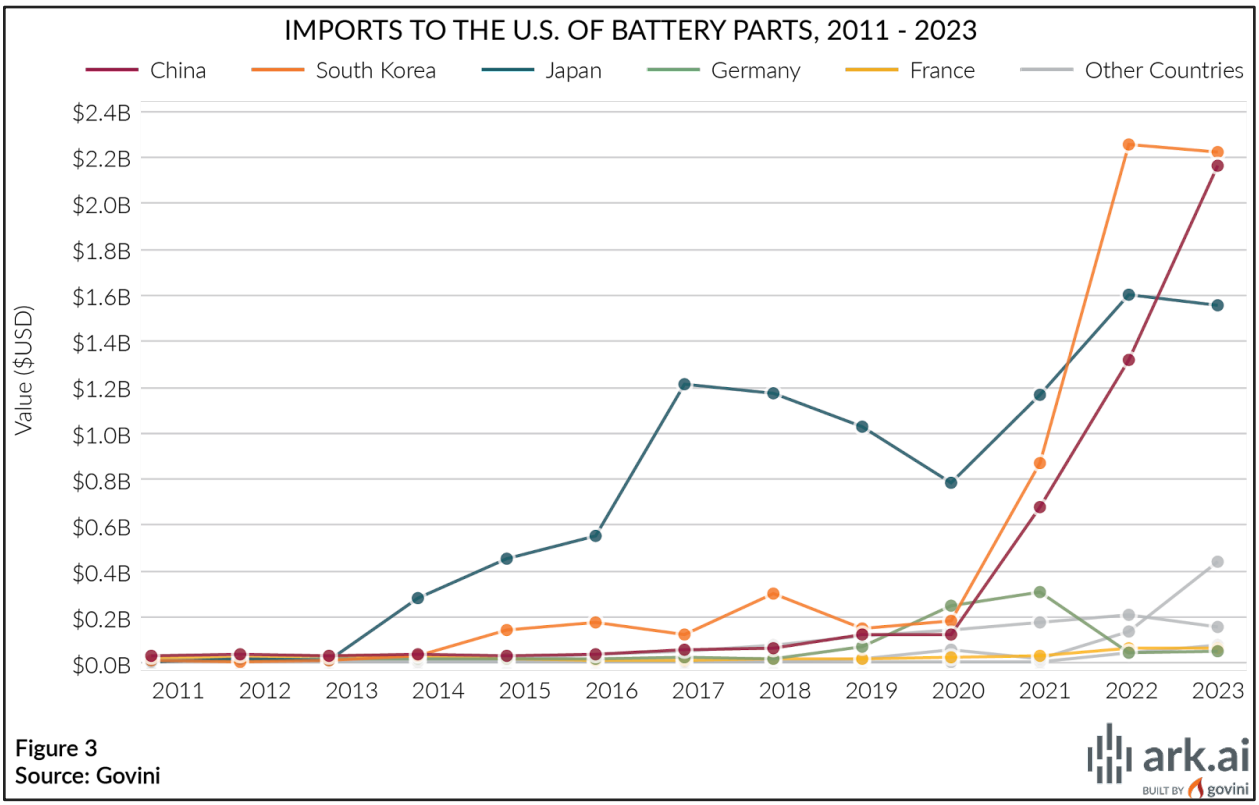


Figure 3
Source: Govini

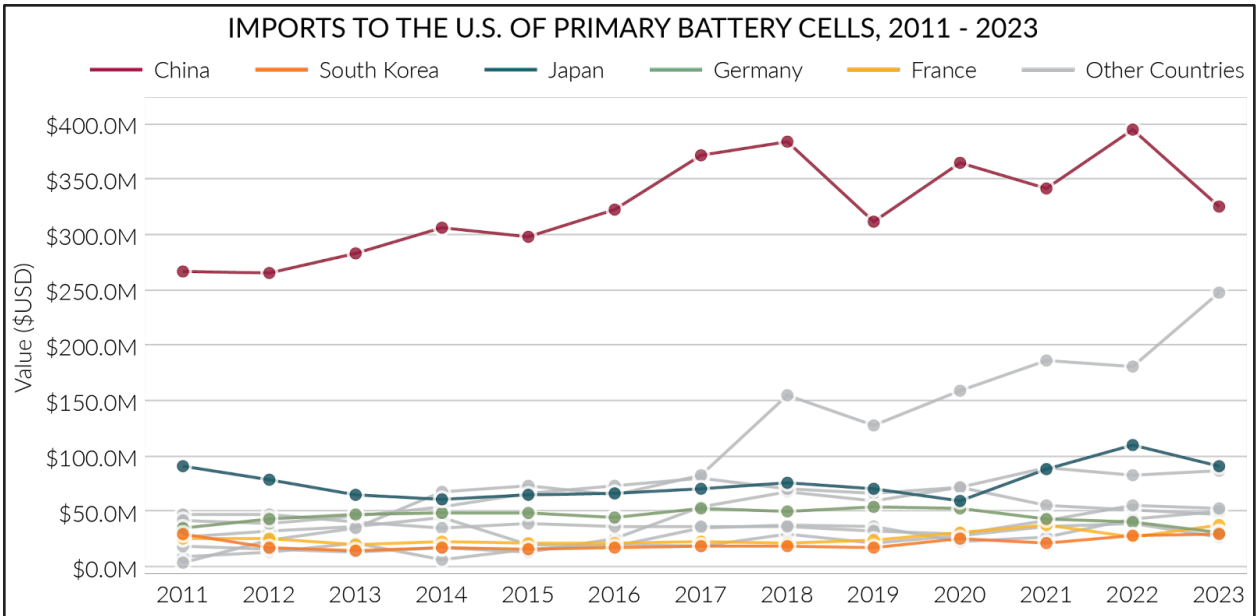


Figure 4
Source: Govini

IMPORT CONNECTIONS OF COMPANIES BY ORIGIN COUNTRY TO THE USG, 2018 - 2023

1st Highest Connection Count | 2nd Highest | 3rd Highest

ORIGIN COUNTRY	LITHIUM-ION	NICKEL CADIUM	PRIMARY CELLS	BATTERY PARTS	TOTAL
China / Hong Kong	801	68	537	97	1,503
Japan	238	28	140	56	462
Germany	194	41	97	60	392
South Korea	171	4	47	15	237
Taiwan	107	6	51	17	181
Singapore	58	1	82	5	146
Great Britain	35	2	38	37	112
France	26	24	18	38	106
Indonesia	3	0	97	3	103

Figure 5
Source: Govini

TOP USG-LINKED U.S.-BASED IMPORTERS BY ORIGIN COUNTRY, 2018-2023

CONSIGNEE	CORPORATE HQ LOCATION	% CN/HK IMPORT CONNECTIONS	% OTHER FOREIGN IMPORT CONNECTIONS
Panasonic Corp. of North America	Japan	41.0%	59.0%
Saft America Inc.	France	8.0%	92.0%
Retail Acquisition & Development Inc.	U.S.	83.0%	17.0%
Energizer Manufacturing Inc.	U.S.	33.0%	67.0%
Tenergy Corp.	U.S.	100.0%	0.0%
Ascent Battery Supply LLC	U.S.	96.0%	4.0%

Figure 6
Source: Govini

ark.ai BUILT BY govini

Batteries represent a prime example of how China's manufacturing competitiveness has evolved over the past decade. Since its opening to the West in the 1970s, Chinese manufacturing success has been mainly driven by low labor costs and loose environmental regulations in service of foreign export markets – the "Old China," if you will. But as the Roland Berger firm has noted, there is a "New China" of manufacturing characterized by (a) industrial modernization, (b) low carbon emission development, and (c) rising demand from domestic consumption. Over time, China has demonstrated how repeated practice with large-scale manufacturing – of products initially conceived and designed abroad – turns into proficiency and home-grown innovation in related areas, including precision engineering.

In the case of advanced batteries, China, having bought or pilfered Western technology in years past, is now at the forefront of development and innovation, mainly stemming from its cycles of experience and expertise in complex manufacturing. It is sustained by a massive domestic market for EVs, which blunts the impact of U.S. trade and technology restrictions.

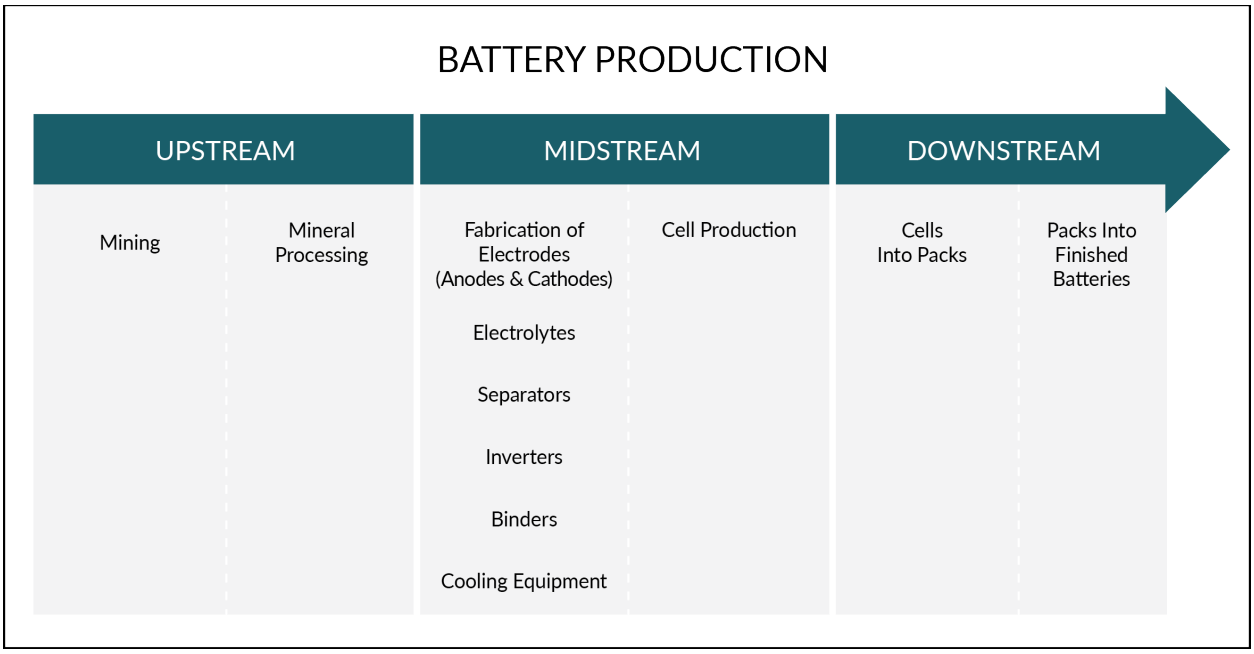
Several U.S. firms with promising battery technologies existed 10 to 15 years ago. However, Federal incentives for these industries tailed off; permitting obstacles remained unabated; we failed to counter predatory Chinese trade practices and subsidies; and the nascent EV market stood too small to sustain these kinds of battery companies. In many cases, Chinese firms were all too happy to scoop up what was left with the permission of all-too-willing U.S. CFIUS regulators.

Roughly the same thing happened with solar panels and wind turbines; though important to advocates of a "green" energy transition, these products are of significantly lesser strategic consequence than batteries.

The demand for advanced batteries – combining lower weight and greater endurance – will only grow across American industry, commerce, and national defense. The two most strategically consequential sectors are automobile manufacturing and the production and operation of military weapons systems. Each is at significant risk in case of a battery supply chain interruption instigated by China or any other natural or man-made cause.

The Challenge Now

In recent years, bipartisan concern has grown over China's rising dominance over key parts of the battery manufacturing supply chain. Worrisome reports have been written, and legislation has been introduced. Irrespective of one's view of the Inflation Reduction Act as a whole, it was helpful that Senator Joe Manchin insisted on provisions expanding domestic sourcing and phased-in reduction of "foreign entities of concern." The Manchin provision has pushed automobile and battery companies to rethink where they operate and how.



Most U.S. public attention and policy action on batteries aims to re-shore slices of the "midstream" and "downstream" phases of battery manufacturing. The midstream includes the production of Chinese-sourced anodes into cells and cathodes into modules. The downstream includes fabricating the cells and modules into packs, and then integrating them into finished batteries.

The focus in the United States on this more visible, higher-value, closing stage of battery manufacturing is understandable given that it is the most visible and politically appealing – the stuff of job fairs and ribbon cuttings. It may produce a "Made in America" label, which is better than the alternative. With a boost from state and federal financial incentives, several battery cell and pack plants have opened in recent years around the United States, providing good jobs for American workers and a more secure source of finished batteries. However, the impression of a growing domestic battery manufacturing strength is partially misleading. In reality, essential parts of the battery are subcomponents and materials originating elsewhere, notably China.

Battery cell facilities within the U.S. are principally driven by Korean and Japanese companies – sometimes owned outright or as joint ventures or partnerships. They bring in the latest battery manufacturing capabilities that the U.S. simply does not have. Acquiring this technical and engineering proficiency is a good thing, especially from countries that are strong U.S. allies. But it also reflects America's near total surrender of manufacturing know-how and technology leadership in this crucial sector. Consider that of the world's most important battery companies, few are American. By contrast, the majority are Chinese.

Low Value, High Stakes

Recognizing that, realistically, we can't do everything all at once to secure the entire battery supply chain, the place to start is the point of maximum Chinese control and, thus, maximum Western vulnerability. And this is the critical but often neglected "upstream" – mineral extraction and mineral processing, and the early stage of the "midstream" – fabricating the refined minerals into positive and negative electrodes (anodes and cathodes), electrolytes, and separators.

Today, at the upstream, China is the world's dominant processor of copper, nickel, manganese, cobalt, and lithium despite having limited domestic geological deposits of these resources. In the midstream, Chinese-entities dominate not only the production of anodes, cathodes, electrolytes, and separators, but also the inverters, foils, binders, and cooling equipment integral to transforming the cathodes, anodes, electrolytes, and separators into cells.

To grasp the scale of the manufacturing challenge, I find it illustrative to dip into some of the workflows. These include:

- Front stage electrode production: mixing, coating, drying, compression, and slitting.
- Battery cell fabrication: winding, stacking, welding, canning, injection, and sealing.
- Charging, storing, testing, and shipping to another site for integration.

The number of companies in the world that have mastered these multifarious processes is relatively few: Wuxi Lead Intelligent, Yinghe, Kanhoo, MAURA, Pitutaila, and some others. Few are known outside energy storage circles, yet they form a linchpin – and choke point – in the battery supply chain. Most are Chinese. All involve intricate manufacturing. All are capital-intensive.

Nevertheless, many of these manufacturing steps are considered "low value" in the business paradigm that came to dominate the American economy in the contemporary era. Yet, lithium batteries simply cannot come into existence without them.

As the U.S. has learned in other crucial industrial sectors, just because a particular item or material is more cheaply produced or extracted elsewhere, the necessity to have some level of domestic capacity is not eliminated.

Most Americans, for example, take this position on energy supplies. Aided by fracking innovation, we have robust oil and natural gas production in the United States. A similar mindset – followed by a comparable level of freedom, action, incentives, and investment – is required for battery materials and components.

In the upstream, we should boost responsible domestic mining of lithium, nickel, and other critical minerals. Countries such as Canada and Norway – with environmental standards as good, if not higher, than our own – do not confront the mining deadlock we have in the United States. In addition, more mining will be of little strategic avail if the capacity to turn those raw ores into usable battery material resides across the Pacific Ocean within the borders of America's principal competitor.

Today, the battery cells that go into most of the batteries we use come from a supply chain that starts with the Chinese refining of minerals – a capacity that is virtually non-existent within the U.S. and among our closest allies. No substitution of Chinese battery

materials and components is possible unless the U.S. and our allies lift the self-imposed barriers to refining and adopt incentives that make American production economically viable against unfair Chinese trade practices.

Defense Requirements

The U.S. Department of Defense faces the same battery supply chain challenges and vulnerabilities as the private sector, but with added complications and concerns. Weapons have used batteries since the invention of stored electricity, but newer military systems and modes of operation have increased their significance to national defense.

In particular, the U.S. military's shift toward distributed operations, stealthier vehicles, survivable long-duration uncrewed systems, electronic warfare, and large constellations of small satellites have swelled the demand for advanced batteries. Yet, as with microelectronics, the U.S. military represents a small portion of the total battery market. The unique requirements of many military systems translate into low volume and thus high per-unit production costs, which disincentivize U.S. and allied commercial entrants into the defense battery segment.

The Way Ahead

Addressing the national battery problem, commercial and defense, requires speed and, above all, scale. Our situation calls for a wartime sense of urgency to fuel a do-what-it-takes approach seen in the Apollo space program and in Operation Warp Speed for the COVID-19 vaccine.

Congress has taken valuable first steps to reduce the benefits Chinese State-Owned and State-Influenced Enterprises might get indirectly from U.S. taxpayer dollars. Stricter export controls are in place, and today's CFIUS, due to Congressional action, now

regards Chinese-linked investments and mergers in key sectors like batteries with much greater skepticism than in the past.

The problem is that China has always found a way to co-opt, copy, buy, or steal the latest technology from the West despite sanctions and restrictions. Trying to block and protect will not suffice. It is a national imperative that we steadily shift production for the most important energy, transportation, and computing products away from China – or sources vulnerable to China – towards either the United States, our allies, or some other assured sources.

Today, it is astoundingly difficult for the United States and similar countries to break into the mineral processing sector – and even more difficult, nee impossible, to compete solely on cost. Mineral processing is energy-intensive, uses strong chemicals and reagents, and potentially produces hazardous waste, even if contemporary production technologies are vastly cleaner than was possible in the past. Building a new environmentally clean processing facility from scratch costs several hundred million dollars and, in some cases, more than a billion dollars.

And that is if the construction is allowed to proceed at all. Tens, if not hundreds of billions, of appropriated dollars for alternative energy projects – wind and solar electricity generation and transmission, for instance – have stimulated substantially less new construction than expected despite strong environmentalist support for low-carbon energy. The challenges are even stiffer for projects connected to advanced batteries, mining and processing activities, which prompt knee-jerk opposition and litigation from various sources.

The permitting regulations associated with the National Environmental Policy Act (NEPA), which govern the building of anything of consequence in this country, effectively serve as an automatic brake (if not an immovable barrier) to building out a complete domestic supply chain for advanced batteries.

Noah Smith, a non-partisan economics analyst, describes the broader predicament in terms of a "build-nothing country." As he puts it: "Money is not physical . . . if permitting holds up the process for years . . . then you still haven't built a damn thing."

RECOMMENDATIONS

Significantly larger tax incentives and market-shaping mechanisms are needed to level the competitive playing field with Chinese companies that their government heavily subsidizes and protects.

First, impose a much stiffer tariff on all Chinese batteries that also covers all battery components of ultimate Chinese origin imported for integration or use within the United States. And do that irrespective of the countries – including otherwise friendly trading partners – those components pass through in their journey here. We could waive the import tariff on other countries that impose similar tariffs on parts and materials exported from China. The ultimate purpose is to block content from China, not create more obstacles for U.S. allies and other trade partners. But that barrier only works if the third-country loophole is closed for battery components. In this respect, the tariff ideas of former U.S. Trade Representative Robert Lighthizer have immense merit, though the facts warrant even higher rates than proposed.

Second, provide extensive tax credits for capital expenditures that are required to process minerals and make battery components within this country.

Third, allow investors to channel unrealized capital gains (several trillion dollars' worth in total) tax-free into domestic battery mineral processing and component making.

Tax incentives are a genuinely American response to the Chinese unfair trade challenge. Unlike direct subsidies, tax incentives keep pivotal decisions in the hands of entrepreneurs rather than government officials.

While these incentives are essential, they will have little impact without changes to the environmental permitting process.

My recommended permitting changes would:

- Speed up the years-long NEPA permitting process to 6 months and appeals to 3 months each.
- Curtail injunction abuse of the courts by ending private party lawsuits; suing power would remain with our elected representatives in the states and localities.

Most fears of pollution resulting from mineral processing – and thus opposition to permitting changes – are based on dated assumptions. While it was a dirty process decades ago in the United States, technology gains now make building "closed-loop" systems with minimum risk to ecosystems, wildlife, or people possible. For example, a semiconductor foundry is, in many ways, an advanced mineral processing plant, primarily of silicon origin. Yet, there is limited environmental and political opposition to semiconductor plants. Quite the opposite, as states and localities compete vigorously to become the site of microchip foundries. Modern refining of critical minerals for batteries is not necessarily any less "clean" than for semiconductors. It is all a matter of designing and engineering the facility right.

Accelerate the Department of Defense's move away from reliance on Chinese-based battery materials.

The Congress should mandate, through the next NDAA:

- A phased-in schedule to move sourcing of battery materials and components used for weapons and critical infrastructure exclusively towards supply chains secure from Chinese coercion or control.
- Issuance of Requests for Proposal (RFPs) with dollar targets and certain contracts awarded under the condition that Chinese battery components are not used.

Conclusion

Americans have seen a steadily declining return from our investments and technological achievements for too long. Whole industries have outsourced production overseas – first for basic goods, then for more advanced and higher-value items. Now, America relies on its principal global competitor and military pacing threat for materials and products essential to national security. It will take years to unwind these vulnerabilities in our battery supply chains. But that provides no excuse for failure to fast-track changes in tax incentives, tariffs, and laws. Quite to the contrary, it only increases our obligation to act now and, conversely, increases the deserved opprobrium of history for failure to act.

###

COMMISSIONER WESSEL: Commissioner Cleveland?

ACTING CHAIRMAN CLEVELAND: I think I'm going to wait a round. Thanks.

COMMISSIONER WESSEL: Commissioner Friedberg?

COMMISSIONER FRIEDBERG: Thank you. And thanks to all our witnesses for their excellent testimony. Dr. Rozo, if I could start with you. You described a situation in the biotech area which sounds very similar to those that we have seen in other domains. And the kinds of prescriptions that you point to are also similar to those that we've heard.

On the one hand, things that build up our own capacity to do things, and on the other, measures that if they don't slow China down, at least limit the ability that they have to extract from our system things that allow them to move forward.

I wanted to ask you about that half of the equation and if you could say more about that. Because it seemed like the recommendations you made pointed to two things, one data and the other kind of talent, for lack of a better term.

Do you think that U.S. laws should be changed so that scientists here can't participate in foreign talents programs, particularly in the biotech area. And on data, should there be regulations or laws that prohibit the use of Chinese companies for processing genetic data or storing that information?

DR. ROZO: Yeah, thank you, Commissioner for the question. So I will note that on both of those topics our Commission has not developed and endorsed policy recommendations on either of those topics.

So I can share some of what we are seeing in terms of the overall problem statement, but we will stop short of actually offering a recommendation on either of those areas.

So, yes, you know, to your original point, there is a lot of similarities that we are seeing with biotech and with other sectors. Some notable differences, a lot of biotech is still in a research phase, right? It is an R&D heavy enterprise. So when you compare it to other fields like semiconductors or others that are more established and where some of these policies have been applied before that is one distinction of, you know, this still being more in the lab, if you will. So, you know, options around talent and data may apply in a different way for the biotech sector than it does for other elements.

In terms of these checkpoints, what we are looking at, as you mentioned, are two kind of options, right? There is a duality here. Either we can run faster or we can slow competitors down.

And so, again, we are still looking at what -- how those recommendations may take place and what options are. But, you know, there are policy proposals on the table already in Congress about limiting the ability for federal funds to be used to support Chinese providers of critical enablers of the biotech industry like genetic sequencing.

COMMISSIONER FRIEDBERG: You mentioned that Chinese entities were taking advantage, I think was the term you used, of the openness of the pre-competitive research that is going on.

Isn't that, by its nature, publicly available information? Is it possible to restrict that? It seems in this area particularly, there is a lot that's going on that is essentially basic science.

DR. ROZO: Sure. So a couple distinctions. The Chinese GeneBank that I referenced is a closed facility. So we have some information around how many samples there are, what information is there. But that is not accessible outside of China to researchers.

In contrast, U.S. equivalent and certainly in other parts of the world, these sort of biological databases are open. Researchers can access them. Innovators can access them. And so that is a distinction between these systems where the Chinese enterprise is not subscribing to open research and the type of information that they are collecting, which could come from the United States, is not freely available in the same way that ours is.

COMMISSIONER FRIEDBERG: So what might be the options for dealing with that imbalance?

DR. ROZO: What might be options for dealing with that?

COMMISSIONER FRIEDBERG: For dealing with that, yeah.

DR. ROZO: Yeah. So potential options for dealing with that are looking at data flows, right? Again, we do not have a position on this particular issue. But I will say that, you know, in my personal capacity, I don't know that we can or would want to completely subscribe to the Chinese model, right, locking this down.

And so it's looking at how do you make the data accessible but secure? And if we can create and build out -- this is a run faster option. But if we can create and build out bigger databases to rival what the Chinese system may have, does it create sort of a situation where there trove of data becomes less important if we have something that rivals them.

COMMISSIONER FRIEDBERG: So accessible but secure would mean accessible to those who are participating in --

DR. ROZO: It could be accessible to those who are participating. There could be different elements of different data sets that are accessible by certain researchers. Secure also, cyber secure, so that you can understand the integrity of those data sets. That is critically important for this type of --

COMMISSIONER FRIEDBERG: But not generally available to anyone?

DR. ROZO: Again, we don't have a position on this right now. There are different ways that one could go about doing this. As you rightfully say, when you talk about research data, it becomes very different than when you are talking about data that relates to, you know, intellectual property.

COMMISSIONER FRIEDBERG: Thank you.

COMMISSIONER WESSEL: Commissioner Glas?

COMMISSIONER GLAS: Dr. Rozo, I just had a follow-up to Commissioner Friedberg's question because I don't know this field. But in terms of genetic sequencing, do we have knowledge to what extent the Chinese actually have genetic sequencing information from the United States, people who have participated in various studies? I am trying to understand the open data and that sort -- can you walk me through that?

DR. ROZO: So we don't have -- again, the information of what exists in the Chinese GeneBank, we have some information that is probably outdated now, of the number of sequences. This is primarily looking at genetic sequences from plants, animals, microorganisms, which is helpful to understand what types of products can be made.

There have been examples of hacks on U.S. health insurers, like the Anthem 2015 hack, of which information was stolen, including health and identification numbers, names, Social Security numbers. So there is anecdotal evidence, right, of some of this. But in terms of a comprehensive assessment of what exists in Chinese biological databases, what of that is U.S. information is something we don't have access to.

COMMISSIONER GLAS: Well, it just strikes me in this age where people are constantly getting solicitations on social media to do DNA, you know --

DR. ROZO: That's right.

COMMISSIONER GLAS: -- for ancestry.com and whatnot, you know, to what extent do the Chinese potentially have access to that data?

DR. ROZO: That's right. And you could -- to the point of the previous commissioner, and I mentioned the cybersecurity, right, there is both illicit and licit means to access this type of information. One could be, you know, Chinese service providers collecting it. Another could be just hacking into U.S. databases.

COMMISSIONER GLAS: Go ahead, Robin.

ACTING CHAIRMAN CLEVELAND: Doesn't BGI own 23 and -- what's the ancestry.com? Don't they own -- a Chinese company owns the largest collector of genetic data in this country, I thought.

COMMISSIONER GLAS: I didn't know that.

DR. ROZO: I don't know the ownership of BGI and 23andMe, if there's a relationship there. I'm not sure. But I do think, again, it's sort of a complex web of, you know, business entanglements.

ACTING CHAIRMAN CLEVELAND: Well, in your future work, that we had a recommendation, what, two years ago, Mike -- I can't remember -- where we strongly recommended that there be transparency both in transparency and ownership.

DR. ROZO: Yeah.

ACTING CHAIRMAN CLEVELAND: Because I think the largest collector of ancestry data is a Chinese-owned company. It is not marketed as that, but yeah.

DR. ROZO: Yeah. And I do want to commend the Commission for your long history of work on biotech and China. You know, you all were one of the first, I think, or the first to talk about, you know, the strategic domain. So I appreciate the long history of the work from this Commission on the topic.

COMMISSIONER GLAS: Great. And just -- I think I have two minutes left, but Dr. Nadaner, I appreciated your comments. You know, personally I am in full agreement with what you're saying.

Given your experience, do you think we've really invested in the right things in terms of the sequencing of our investments? Meaning there is a lot -- you know, there has been a lot of prioritization on producing the finished product, potentially more finished product here, have we done these kinds of investments the right way?

I know you're talking about trade, you know, remedies and safeguards and things like that. But from your perspective, you know, are these investments being done appropriately to ensure longevity of the investment?

DR. NADANER: I think that question is right on point because this is a wider American trend over four to five decades. If it involves a lot of capital expenditures and the profit is lower -- I'm not saying it's a not a good profit, but the profit is lower, then we say, okay, let other countries -- in the last few decades let China assume those capital expenditures.

So we like -- you know, I think we are biased as an economy in many ways because of shareholder value, the way the tax system works. We are very much biased towards industries like financial services and software, which don't often have the same capital expenditures you have in terms of mineral processing.

So the profit is greater and hence we like to focus on the end product, the integration, of certain manufactured goods. But I think that's a problem fundamentally. And that's a problem with incentives in the economy. It's not a question of just preaching to people. But if we gave the

right tax incentives, there would be no reason for companies and entrepreneurs not to jump on them.

COMMISSIONER WESSEL: Co-Chair Helberg?

COMMISSIONER HELBERG: Thank you. And thank you to our witnesses for their insightful testimonies. Mr. Nadaner, how old is China's EV industry?

DR. NADANER: I cannot give you an exact date. But they have been working on EVs for at least 30 years. And early on it was mostly stolen technology from the U.S.

COMMISSIONER HELBERG: Is it an established fact that China's EV makers now rank as the number one exporters in the world?

DR. NADANER: China has reached that status from all the data that I have seen.

COMMISSIONER HELBERG: Elon Musk recently made news stating that the Chinese EV makers would destroy the entire Western EV industry without tariffs on Chinese EVs. Do you agree with that?

DR. NADANER: 110 percent.

COMMISSIONER HELBERG: So do you support tariffs on Chinese EVs?

DR. NADANER: Yes, I support tariffs on Chinese EVs and also the component parts. We have a huge domestic auto industry, as do the Germans, as do the Italians and French, Japanese and Koreans. If we do not protect the lower level suppliers, they will simply not be able to compete against the Chinese subsidies.

COMMISSIONER HELBERG: And, Ms. Rozo, do you believe that bio warfare should be viewed by the U.S. government as a standalone warfighting domain and a national security issue? And how vulnerable are we to a bio attack in light of recent advances in biotechnology?

DR. ROZO: Yeah, thank you for the question. So I think in terms of the second half, we saw, you know, the response to COVID-19 and sort of the ability of our system to detect, respond and treat individuals was benefitted by biotech, right? We saw an ability to get to a vaccine in a shorter period of time than ever before, the potential to revolutionize the ability to create new diagnostics and new threats. But by no means I think would anyone we are prepared for what is coming.

And in terms of how technology is changing that landscape, we have actually, as our commission just put out a couple of papers on the intersection of AI and bio, where we look at the applications of large language models to biotechnology and how that's changing the threat landscape.

So in particular, the distinctions between large language models trained on human information, like ChatGPT, and not trained on biological information, which we call biological design tools.

So in our findings, it is the latter, the sort of AI models trained on biological information, that has the potential to create novel biological agents in the future. We don't assess that that capacity is something that is robust today. It still takes a lot of expertise to use these systems. But it is something we should be mindful of as we are developing these tools and put guardrails in place.

COMMISSIONER HELBERG: It is my understanding that it's now technically possible to develop pathogens that are explicitly targeted at specific -- at individuals with a specific genetic profile or specific groups with a genetic profile. Is that true?

DR. ROZO: I have not seen that that's technically possible.

COMMISSIONER HELBERG: Can you help us understand a little bit if China views biotech as a national security issue or priority as part of their policy planning?

DR. ROZO: Sure. I think it is clear that China views biotech as both an economic and national security priority. They, of course, have a stated goal of civil military fusion, right? So any technology or knowledge they will receive from commercial entities will be used for military advantage.

And military advantage with respect to biotech could mean many different things. It could look like weaponization of biotech in ways that don't align with our system. It could also look like enhanced supply chains and critical capabilities provided for the military by biotechnology.

COMMISSIONER HELBERG: Do you believe that the U.S. government should explore and consider the feasibility, need and desirability of establishing a new defense bio force of the Department of Homeland Security to protect our homeland against potential bio attacks from our adversaries?

DR. ROZO: So as part of the commission, I don't have a specific viewpoint on that. I will note that our commission is particularly focused on biotech. Our mandate is not necessarily bio defense, but we are looking at bio defense where it relates to advances in those technologies.

COMMISSIONER HELBERG: Okay. So just to clarify, you do believe biotechnology has serious implications for national security?

DR. ROZO: Yes, of course, yes.

COMMISSIONER HELBERG: And are you able to comment a little bit on the bio labs uncovered in California?

DR. ROZO: No. Sorry. I don't -- I'm not tracking that. The bio labs?

COMMISSIONER HELBERG: Chinese bio labs were uncovered -- illegal Chinese bio labs were recently uncovered in California with thousands of mice, you know, pathogens ranging from HIV to COVID to a lot of different strains. Is that something you were aware of?

DR. ROZO: No. Sorry. I'm not tracking that.

COMMISSIONER HELBERG: All right.

COMMISSIONER WESSEL: Vice Chair Price?

VICE CHAIR PRICE: First of all, thank you all for your testimony today. This has been very interesting.

Ms. Luong, I want to go back to your second recommendation and for you to flesh it out a little bit more, specifically the changes that you are suggesting from exclusively used to intended and exactly why. Could you talk about that a little bit more?

VICE CHAIR PRICE: Yes, absolutely. Thank you for the question. I have spent a lot of time thinking about, you know, what the definition of ordinary AI system is, and I think at least according to the Treasury's ANPRM, the definition of AI system is quite broad.

The policy objective here is to restrict investment coming from the United States to China, specifically for AI systems that are used for military purposes. And the language in that ANPRM is stated to say exclusively used for military purposes.

And according to my research, it is really quite difficult to delineate the difference between military purpose -- an AI system that is exclusively used for military purposes because there is a profit motivation behind that as well.

When an AI developer thinks about what model is to put on commercial space, they do want to create an adjustable foundational base that could potentially be fine-tuned for many purposes for commercial uses, for military uses.

So it is quite difficult to capture transactions that are going towards AI companies that exclusively develop AI systems for military purposes.

That said, I think if we revise the language to intended in part used for military purposes, we can capture the AI systems that could potentially be transforming between military space to civilian space and vice versa seamlessly.

VICE CHAIR PRICE: Thank you. And Mr. Nadaner, we cut you off a little bit when you got to the point on your recommendations. I think you got most of it in, but is there anything else you want to expand on in two minutes?

DR. NADANER: I would say for the NEPA permitting process, the process should be limited to six months and then appeals to three months each.

And then we have to curtail injunction abuse. This is an abuse of the courts. By ending private party lawsuits, instead the suing party should remain with our elected representatives in the states and localities.

VICE CHAIR PRICE: Thank you.

DR. NADANER: Thank you.

VICE CHAIR PRICE: That's all I have.

COMMISSIONER WESSEL: Commissioner Schriver?

COMMISSIONER SCHRIVER: Thank you. And thank you to all our witnesses for your excellent statements and your contributions here today. Ms. Luong, I wanted to start with you and also the same recommendation that Commissioner Price asked you about.

Your recommendation restricts capital investment in the areas of AI for military purposes. Is that just the right thing to do or would that actually have an impact? I mean, what magnitude are we talking here? What percentage are they relying on U.S. capital? Because you've described a very heavy investment on the part of the Chinese state.

MS. LUONG: Absolutely. Thank you for that question. In my research, when I look at the extent and scope and size of U.S. capital flows into China's AI development, it's really small. U.S. investors are not dominant investors in China. It is actually domestic investors.

And that is a quite common thing in the, you know, private investment world, similar in the U.S. U.S. investors are dominant investors in our ecosystem. That being said, there are other components that are quite important that the U.S. investors are bringing to China. That includes not just the actual money itself but also the intangible benefits that come along with capital.

And I think that is the one component that is concerning to a lot of policymakers here in DC because the expertise, the networks, the manageable opportunities for these investors that they are bringing to China is helping the Chinese venture capital ecosystem maturing. It is a more nascent ecosystem compared to the United States. And so that is quite an important component.

That said, the military part is quite small because, again, it is difficult to differentiate, you know, different applications of AI between the fund space and the commercial space.

But in China, because of the military civil-fusion policy that can be transformed very easily between the commercial space and the military space. And I actually have a caveat to that. By easily, I mean there is an effort or there is a pathway for that to happen.

But when you adopt an AI system that is developed in the commercial space, it is quite difficult because the data has to be trained for military purposes. It has to be fine-tuned. So it will take a long time for the Chinese government to figure out how to do that more effectively, and there are a ton of problems the way for the MTF policy as well.

COMMISSIONER SCHRIVER: Thank you. Mr. Nadaner, you concluded your statement by saying it will "take years to unwind this." Can you take your best stab at it? What does wild success for us look like if you adopted some of these measures, tariffs, investment incentives? I mean, what's the magnitude of this?

DR. NADANER: It's a large magnitude. But we have shown the ability to do significant things when we allow ourselves to do it. I would say that if we adopted those -- let's say by the end of this year, we adopted the tariffs, the tax credits for large capital expenditures for batteries and then followed along the lines of Senator Tim Scott and Cory Booker on capital gains, freeing them up for investment, I think within 10 years we would be in very good shape. But if we go very slowly, and we allow NEPA to continue its operations, we will find that 40 years will go by with nothing.

COMMISSIONER SCHRIVER: So wild success is 10 years?

DR. NADANER: That's pretty good in the manufacturing business.

COMMISSIONER SCHRIVER: Dr. Rozo, I wanted to ask you about a different wild success. What if the Chinese are wildly successful on the investment and research and development side, particularly this nexus you described between AI and biotech?

I think we had a conversation earlier today that some of the threat and risk is abstract and therefore people aren't moving with the sense of urgency. I am grateful your commission exists, and you are working on these problems. But sometimes I think we still grapple a little bit with what does worse case look like? What does Chinese wild success look like?

DR. ROZO: Thank you for the question. I think it is multifaceted. We talked a little about the potential for misuse of biotechnology, right, and what that would look like if an adversary that has different ethics and different values around using biotechnology, what that would mean. There are some very human aspects of this technology that we have to grapple with.

But one thing I want to talk about that we haven't chatted about is supply chain and how mastery of biotechnology could impact supply chains and how that might impact our relationship with China.

I think the medical implications of biotech are more well understood. When we hear biotech, we think pharmaceuticals. But on the supply chain side, this is a growing part of the biotech sector is really using bio and biomanufacturing to create novel roots of production of critical chemicals.

So an example of this that BCG has published is a chemical called BDO. This is a chemical that is right now derived from petroleum. And it is a $5 billion industry for this one chemical. It's in water bottles right in front of me.

This right now is mainly manufactured in China and mainly in Xinjiang. But there is a U.S. firm that uses synthetic biology to create a cell factory that can now produce bio-based BDO. And they are building a facility in Iowa to make this bio version of this chemical, so bringing the supply chain back from China, creating jobs in Iowa and using corn as the starting material. So this is a great news story. And the potential of how many parts of our supply chain we can do that for, we are really just beginning to scratch the surface of that.

But this is an area where the market may not exist today for products, right? If we are replacing products in our supply chain that are already very cheap, the market, you know, may not be there today.

And so it is an area where we see that China may have an advantage with state down economic policies and incentives for things like manufacturing infrastructure for industrial biomanufacturing. They could outperform us at this sector that is still advancing.

So it is something to be mindful of. And it is an area that we are particularly viewing as something where with absent action we may fall behind because the market doesn't yet exist for these type of products.

COMMISSIONER WESSEL: Thank you all. We got a lot of questions. But, Dr. Rozo, let me start with you. And to emulate my colleague, try and keep some of the responses short so I can get through these.

It appears to me that at least in the biotech, the synthetic biotech, your comment about a ChatGPT moment, that it seems there is more capital constraint in the sector over the last couple of months that what was -- and I am very appreciative of what you have done throughout your career in serving on this commission. But the inflection point here in the U.S. seems to be a little farther down the road. What do you attribute that to?

DR. ROZO: Yeah, I think exactly as you say, the markets look very different today than they did a few years ago. And so borrowing money is expensive right now. And for an industry like biotech where it is still relatively expensive to do the R&D and to get a product from lab to market, again, there are certain sectors where I think we accept that economic cost, like in high value pharmaceuticals. You know, the margins will bear out the cost of development.

But right now, for the industrial products, for products for the ag sector, the same costs still exist today, but the margins are not there on the other side for the products. And so it creates an imbalance. And we are seeing more capital, as always, flowing towards medical products where there are high margins than some of these industrial or defense applications.

Now don't get me wrong. The cost will come down as technologies increase. But the funding cycle that we are in, the climate that we are in right now with the markets being the way they are, impacts certain sectors of biotech different than others.

COMMISSIONER WESSEL: I seem to remember, and I can be corrected later, but I think Senators Grassley and Ernst had spoken out about amino acids and other biotech products being produced in China, many of them food additives, I think Vitamin K and others, that are necessary for the strength of our livestock, you know, our food supply.

What visibility do you have into that from the commission? What are you doing? Is that accurate? And it seems we are putting ourselves in the potential for China to be able to weaponize those products for what is a critical need here.

DR. ROZO: Yeah, and I appreciate the question. I think as I just described, you know, biotech can help us with creating more resilient supply chains, but it could also be used to entrench supply chain balances that exist today vis-a-vis the United States and China.

And by and large we don't have great visibility into biotech supply chains, whether that be medical or agriculture. I was actually feeling a sense of -- what is the word -- jealousy of my colleague who was talking in great detail about the battery supply chain and the different sectors and how well-defined that is.

On the biotech side, that is really not there in terms of what are the critical inputs, the raw materials, the reagents, the consumables, where those come from, where those exist, the visibility is not there. So it becomes very difficult to make policy decisions.

If you will allow me one extra detail here, the way that our system classifies biotech with the way that we count sort of biotech economic activity under what is called NAICS codes doesn't really apply well to biotech. Because it can be used in agriculture and industry and pharmaceutical, we don't have good ways of measuring our own economy with respect to biotech.

So, again, it becomes very difficult to make policy decisions without understanding where we are, without understanding where China is. And so we are looking at ways to improve our own economic accounting. If that is something the Commission is interested, we are happy to chat further on that.

COMMISSIONER WESSEL: We have looked in the past about accounting and data acquisition and certainly looking at redefinition of NAICS codes, which is under the Department of Commerce is something which is within their jurisdiction and does not require a new statutory authority as I recall. So something we will take under advisement.

Mr. Nadaner, I appreciate everything you are saying and spot on. I wanted to go, as I mentioned to you earlier, to a different component of the battery supply chain, not the commodities, the cobalt, et cetera, but the technologies that are embedded in there.

There was a recent report that the authorities at Camp Lejeune indicated to the local authorities, local power authority, that they could not put load balancing batteries sourced from China as part of the reserve power system for the camp. And there have been increasing questions about the security of these larger batteries, not that the same thing isn't true about, you know, an EV in a Tesla auto.

But with the drive towards green energy, load balancing batteries, whether at the industrial facility or on the grid itself are increasingly important. I just, you know, and I've raised other issues earlier today, to me it sounds like we are allowing pre-placed Chinese munitions on the U.S. mainland, homeland because these batteries are all remotely maintained, serviced, accessed.

What within the technology sphere do you think we need to be doing about the battery supplies that we are not doing presently?

DR. NADANER: These are remote vehicles for our destruction. They are embedded for electronics. They can be used for a variety of purposes. A battery is in many ways chemicals with wires and sensors and semiconductors included. The chemicals can be highly explosive. And that just takes a little bit of computer code to change.

I think in terms of those kinds of electronics, they get embedded, particularly in larger, more complex batteries, that is something that we can make. But there still has to -- no one is going to make it unless the battery is also made here. It has to be something that goes in.

COMMISSIONER WESSEL: Thank you. Commissioner Cleveland?

ACTING CHAIRMAN CLEVELAND: Oh, sorry. I want to thank you all for your testimony. It is extremely helpful. I have one question for Dr. Rozo.

You talked about Syngenta potentially withholding ongoing biofuel advancements from the U.S. military. Could you talk a little bit more about that? It was in your written testimony, Page 9.

DR. ROZO: Thank you.

ACTING CHAIRMAN CLEVELAND: On Page 9. It's in talking about the fact that ChemChina bought Syngenta, and there is this increasing consolidation in the ag --

DR. ROZO: Yeah, I think --

ACTING CHAIRMAN CLEVELAND: -- biotech space. And I'm just curious, what do you see as the threat or the risk?

DR. ROZO: Sure. So I think broadly the acquisition of Syngenta by ChemChina and then the ongoing combining of the assets with Sinochem under the Syngenta name is just concerning because this supply chain and this agriculture biotech is winnowing, right?

The number of companies, which used to be much larger, and represent a lot more countries is now much smaller. And so that is a concerning trend. We wanted to note also that

the purchase of ChemChina was cleared through CFIUS. And it, again, just points to the differing understanding or viewpoints of what constitutes national security concerns.

We made some recommendations around increasing the visibility of national security at the USDA as part of ongoing work related to the Farm Bill. But looking at the number of cleared individuals at that agency, at the ability for individuals to participate in national security conversations, is not, of course, what it is in other national security agencies.

And so the point being, I think it is unclear what this consolidation will do, how that will impact, you know, or could impact our military, our own domestic economic sector. But it is clear that Syngenta has perhaps the world's best information around the seeds that are grown here in the United States. And that potential information could be, you know, used against us.

So it's a point of taking into account not only the basic biotech sector but also all of the economic sectors at which it applies to.

COMMISSIONER WESSEL: Commissioner Friedberg?

COMMISSIONER FRIEDBERG: Mr. Nadaner, I am sympathetic to your description of the problem, and I found your proposals very clear. But I want to raise with you a number of obvious objections and see how you would respond.

First would be the question of the impact of the substantial stiffer tariff that you advocate on U.S. consumers and producers who are currently incorporating products that are made with these important components. That's one.

The second related question is the impact of stiffer tariffs and the tax credits that you propose on our relations with our allies. So we have been through this with the IRA. This sounds like it could be the same thing, maybe even on a larger scale. How would you respond to someone who raised those concerns?

DR. NADANER: Well, I think as a county, we cannot have pass-throughs from friends. It is not a very friendly act. And they have a similar problem to us. We can solve the problem together, but we certainly can't suffer the problem alone. We can't be just the great sponge.

So I believe that if we put the tariffs in the right place and have the right diplomacy, the kind of diplomacy that, you know, Dr. Kissinger and Dr. Shultz did years ago. It's very intense. It's laborious. But to put in place the right kinds of agreements, you could have a joint tariff among allies. And then we would all benefit.

In terms of consumer costs, I think currently the situation right now is a very bad deal for average Americans who are not in the upper class. We don't have these industries anymore. We don't have those middle-class jobs. We have communities that are bereft of manufacturing to an unhealthy extent.

So I believe that if we had a revival of industry, that would be far better than getting a cheaper battery but not having a job and not having a community.

COMMISSIONER FRIEDBERG: Is it conceivable that we could solve this problem for ourselves acting on our own or is this something that is necessarily going to require a high level of cooperation from our allies?

DR. NADANER: I believe that it would be extraordinarily difficult for us to do alone. With allies, it is imminently possible because, as we have seen, Korea, Japan have extraordinary technologies. And we benefit when they come here. And we benefit when there is balanced trade.

Germany has some great chemical technologies as well, too. We didn't talk about France. France is doing some very nice things on batteries. So I think to do this together will be much,

much easier than to do it alone. But someone has to take the first step. And right now the easy situation is for the U.S. to be the great absorbent.

COMMISSIONER FRIEDBERG: Thank you.

MS. LUONG: Can I add one point if that's okay?

COMMISSIONER FRIEDBERG: Sure, please.

MS. LUONG: I did spend some time looking at the Chinese EV industry, and it seems to me that they not only are exporting to the U.S. but they also are mostly exporting to Europe. So a potential on Chinese EV in the United States might leave us behind in the competition sphere. That is just one point.

And also, half of Tesla's EVs that are manufactured in China in its Shanghai Gigafactory is also going to Europe. So that could potentially be convoluted in the export data that is reported publicly.

COMMISSIONER FRIEDBERG: Thank you.

COMMISSIONER WESSEL: Commissioner Glas?

COMMISSIONER GLAS: I will pass.

COMMISSIONER WESSEL: Co-Chair Helberg?

COMMISSIONER HELBERG: No further questions.

COMMISSIONER WESSEL: Well, I am going to come back to me it sounds like, which is fine.

Dr. Rozo, you mentioned ChemChina. I was going back to the BGI that was a complete genomics back in 2012. Do you think the -- those who serve on the CFIUS committee now have a better understanding/appreciation for some of the risks in this area? I think the work you did at the NSC and, you know, the creation of this Commission is partially a sign of that. Are you, in your discussions at the commission, aware of, you know, greater sensitivity?

DR. ROZO: Yeah, thank you for the question. I think by and large when we're looking at the government, and we have a suite of work all around bio literacy, how we improve the understanding of biology in the federal government, we need more individuals at all agencies who have more familiarity with biotechnology.

Being one of those individuals for some time before I stepped out of government, I can say that there are great, really intelligent scientists working in the government, but there is not many of them. And they are not at high enough roles within the government.

And so whether it's CFIUS, whether it's other policy decisions, without having people, individuals in the room who understand biotech and understand the complexities with this technology, it becomes difficult, you know, to inform these discussions.

So we are looking at ways to improve what we are calling bio literacy across the federal government as well as, you know, across the general public.

COMMISSIONER WESSEL: And another question is when one looks at biotechnology, and we did a hearing of -- Commissioner Cleveland and I co-chaired that four years ago I believe it was with your co-chair and others. We talked about fermentation capacity and many of the sort of building blocks to be able to convert the ideas to industry level production.

DR. ROZO: Right.

COMMISSIONER WESSEL: What is the state of the industry? China certainly cleaned our clock when they took over everything from penicillin to other, you know, fermentation approaches. Are we building capacity here?

DR. ROZO: Yeah, thank you for that question. It is one thing that I am personally concerned about.

So when we look at the medical sector, vis-a-vis biotech, we have a lot more information, right? The facilities have to be approved by regulatory bodies, the products have to be approved. And so we have a lot more visibility into manufacturing capacity, of which the majority for high value products, at least, biologics, exist in the U.S. and the EU. Low value products, we know we have some dependencies on China.

On the industrial sector, the understanding is much less. But I will say anecdotally, and certainly, you know, in response to imbalances that exist in industrial manufacturing capacity, the administration has put out, and DOD actually released yesterday, an RFP for increasing industrial biomanufacturing capacity in the United States. So that's at the early stages, but it is, I think, you know, for industry, a welcome development of potentially supporting and increasing domestic biomanufacturing capacity.

It's an area, again, where we don't have good aggregate data on what exists in China. But we know anecdotally that there is state support for manufacturing facilities on the industrial side. And they have a long history of just fermentation. There are large public companies that aren't using -- have these novel engineering techniques but are still using kind of fermentation, which is an old manufacturing science.

And so with all of that in play, again, it's a potential for the Chinese system to have an advantage over ours. Right now companies are facing difficult decisions between financing their own facilities or paying high fees to contract out that capacity.

So, again, the Department of Defense released a new funding program yesterday, which we, at the commission advocated for and were in support of increasing that capacity in the United States.

COMMISSIONER WESSEL: Great. Thank you. Ms. Luong, a question for you. On Page 4 of your testimony, you refer to venture capital firms having received nearly $224 billion. Is that within the Chinese market or does that include foreign venture capital, understanding that there is the outbound investment screening mechanism that's still in development but, you know, that's not yet fully applicable. So was that just domestic Chinese or was that all global?

MS. LUONG: That's all-encompassing.

COMMISSIONER WESSEL: So any idea what percentage might be global? Any idea what percentage might be U.S. of that 224?

MS. LUONG: I will be happy to check that for you.

COMMISSIONER WESSEL: Great.

MS. LUONG: I believe that is the data for the little Chinese companies that are receiving investment from venture capitalists.

COMMISSIONER WESSEL: Okay.

MS. LUONG: Yes.

COMMISSIONER WESSEL: If you could, that would be very helpful.

MS. LUONG: Absolutely.

COMMISSIONER WESSEL: Any other questions from my colleagues? If not, in closing thank you to all of our witnesses throughout the day for your excellent testimonies. The public can find those testimonies as well as a recording of the hearing on our website.

I would like to note that the Commission's next hearing will take place on Friday, March 1. That hearing is titled, Chinese Consumer Products, Safety, Regulations and Supply Chains. And with that, we are adjourned. Thank you.

(Whereupon, the above-entitled matter went off the record at 3:05 p.m.)

STATEMENT FOR THE RECORD

RESPONSE OF CHRISTOPH HEBEISEN, DIRECTOR OF SECURITY INTELLIGENCE RESEARCH, LOOKOUT

February 1st, 2024
Christoph T. Hebeisen - Director, Security Intelligence Research, Lookout, Inc.
Statement for the Record before the U.S.-China Economic and Security Review Commission
Current and Emerging Technologies in U.S.-China Economic and National Security Competition

Software Development Kits

Software Development Kits (SDKs) are software packages that enable a developer to include specific functionality into their code without having to develop and maintain that functionality themselves. For example, a developer who wants to accept credit-card payments in their iOS or Android app may include the Stripe SDK[1]. If social networking functionality through Facebook is desired, the developer may leverage Meta's Facebook SDK[2] and if they want to monetize their app by displaying advertising to app users, they may deploy Google Mobile Ads SDK[3]. The functionality provided by SDKs is invoked by the code of the app through an Application Programming Interface (API).

The abstraction of implementation details of functionality that is not part of the core purpose of an app is beneficial to app developers. It avoids re-implementation of the same functionality for many apps and the reuse of an SDK in a multitude of scenarios usually results in higher-quality code, at least in the case of well-maintained SDKs.

Much of the discussion in this statement applies to SDKs in general. However, this panelist's expertise is in mobile systems (Android and iOS) and examples as well as technical details and considerations below are specific to mobile apps and mobile SDKs.

SDKs as a Potential Security Threat

While not having to know or understand the implementation details of an SDK is a great advantage, SDKs contain code that is not developed or controlled by the creator of the app. The user may choose to trust an app's developer based on their reputation and install the app on their device. However, they have no way of knowing which SDKs developers are utilizing in the app.

SDKs therefore provide an opportunity for a malicious actor to place code inside third-party apps - either by creating a useful SDK with well-hidden malicious functionality already included or by adding malicious functionality to an already existing, well-established SDK. Note that SDKs created by Chinese software companies and developers are well-represented in the mobile app space.

[1] https://stripe.com/docs/libraries/android
[2] https://developers.facebook.com/docs/ios/
[3] https://developers.google.com/admob/android/sdk

The creators of SDKs are usually software companies, which act primarily in their own business interest. If an SDK contains malicious code and that code is discovered, it is likely to reduce their future revenue. As a result, they are unlikely to add malicious code to their SDK voluntarily (unless there is significant business benefit to them - see examples below). However, a nation state might be able to compel or pay a software company to integrate malicious code to spy on users or perform other attacks such as Denial of Service (DoS).

However, adding malicious code to the SDK may not be necessary to gain access to some sensitive pieces of data. Much of the data collected by an SDK legitimately is sent to cloud infrastructure. For example, an in-app advertising provider may decide to display ads based on the location of the user as well as their past buying behavior. For this purpose, they need a way to identify the user as well as their geolocation. An advertiser may have a legitimate interest in both pieces of data but the use of the same data for any other purposes could well be considered a violation of privacy and - in the hands of an adversary - a serious risk. Similarly, billing or analytics SDKs may, in the normal course of operations, collect sensitive information about a user. Neither the user nor the creator of the app using a third-party SDK have a way to verifiably determine who can access the collected data and for what purpose. Examples such as TikTok's tracking of journalists[4] and Cambridge Analytics's abuse of Facebook data[5] demonstrate how data originally collected for non-malicious reasons can be used for spying and political manipulation purposes.

Operations of an SDK are only limited by the constraints the operating system imposes on the host application via the app sandbox. For example, if an application has the permission to access the microphone or the precise location of the device, the SDK code has the same access, even if it is not required for its stated functionality. And while mobile operating systems prevent apps from accessing other apps' private data, an included SDK has full access to the private data of the app. As a result, app developers have to trust an SDK to be "well behaved."

Examples of Malicious Use of SDKs, Code, and Data

Despite the risk of negative business impacts, multiple Chinese companies have been found to use malicious code to further their interests:

- In 2019, the BeiTaAd advertising SDK (created by CooTek) was found to aggressively flood users with ads[6] in violation of Google Play store rules.
- In 2020, it was discovered that MIntegral, a popular Chinese advertising SDK for Android and iOS, used malicious code to attribute clicks on advertising displayed by third-party SDKs to their SDK[7].

[4] https://www.nytimes.com/2023/03/17/us/politics/tik-tok-spying-justice-dept.html
[5] https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html
[6] https://www.zdnet.com/article/440-million-android-users-installed-apps-with-an-aggressive-advertising-plugin/

[7] https://snyk.io/blog/sourmint-malicious-code-ad-fraud-and-data-leak-in-ios/

- In 2023, PinDuoDuo was discovered to contain malicious code that exploited vulnerabilities in the Android operating system[8] in a version of the app distributed in some parts of mainland China. PinDuoDuo is PDD Holdings' app for the Chinese market. Their online shopping app for the North American market is Temu.

While CooTek's business appears to have suffered significantly after their SDK was banned from Google Play, the MIntegral SDK is still available and popular on U.S.-based advertising mediation platforms. At the time of writing, Temu is the top shopping app on both the Apple App Store and Google Play.

To the best of our knowledge, all of these cases were aimed at increasing revenue rather than spying on users.

Types of SDKs

While there are many different types of SDKs for mobile applications, the most commonly used ones fall into the following categories:

- Advertising
- Analytics
- Billing
- Storage
- Social Media
- Identity

In the following sections we will discuss common types of Chinese SDKs we observe integrated mobile apps. Data on presence of SDKs in apps presented in this document is for January 16th, 2024.

Advertising SDKs

Advertising SDKs are used by developers to generate revenue from their (usually free) apps. This means that in contrast to other types of SDKs, the integration of Ad SDKs is often not driven by technical requirements but by the expected payouts to app creators. This process is facilitated by so-called ad mediation platforms. Examples of popular US-based ad mediation platforms are

- Google AdMob[9]
- AppLovin MAX[10]
- Unity Ads[11]

[8] https://arstechnica.com/information-technology/2023/03/android-app-from-china-executed-0-day-exploit-on-millions-of-devices/
[9] https://developers.google.com/admob/android/choose-networks
[10] https://dash.applovin.com/documentation/mediation/android/mediation-adapters
[11] https://unity.com/products/mediation

With ad mediation, developers are incentivized to add as many ad network integrations as possible to maximize monetization potential. Integrating with an ad provider may also require installation[12,13] of the upstream ad provider's SDK.
Thus, app developers may end up bundling Chinese ad SDKs even in cases where the transaction was initially brokered by a non-Chinese third party marketplace.

Popular China-based ad networks that integrate with mediation platforms are

- MIntegral[14] (partners with AdMob and AppLovin)
- Bytedance Pangle[15] ("Ad Network of TikTok for Business", partners with AdMob and AppLovin)

Unsurprisingly, ad SDKs are the most common Chinese SDKs found in Google Play top 150 grossing apps. MIntegral and Pangle were each found to be present in 20 of these 150 apps. MIntegral was also found in four of the 100 top grossing apps on the Apple App Store. While most of the Android apps are games, including titles such as Township, Solitaire, Lily's Garden and Heart of Vegas, the list also includes Grindr (social media / dating). The iOS apps are more varied, including ReelShort (streaming), GoodNovel (e-books) and CapCut (video editing).

Analytics SDKs

Analytics SDKs are used to collect information on how users engage with an app and on bugs and other issues with the app containing the SDK. Well-known Chinese analytics SDKs are Bugly (by Tencent)[16] and UMeng Analytics[17]. While Bugly was present in nine of the 150 top-grossing apps on Google Play and one of the top 100 apps in Apple's App Store, at the time of writing UMeng does not have a presence in the top apps of either store. All of the apps containing Bugly in the two stores' top apps were games.

Billing SDKs

While there are a considerable number of Chinese billing SDKs, these are usually not observed in mobile apps available in official app stores. Apps that are not available through these channels are unlikely to gain much traction in the U.S. and other western countries. This strongly entices app developers to distribute their apps through Google Play / the Apple App Store. Historically, these marketplaces require most categories of in-app purchases to be conducted using the marketplace's own billing system (App Store rules for in-app purchasing[18],

[12] https://developers.google.com/admob/android/choose-networks
[13] https://dash.applovin.com/documentation/mediation/max/get-started-with-max
[14] https://www.mintegral.com/
[15] https://www.pangleglobal.com/
[16] https://bugly.qq.com/v2/
[17] https://www.umeng.com/analytics
[18] https://developer.apple.com/in-app-purchase/

Google Play payment policy[19]). Notable Chinese billing SDKs include WeChat Pay[20] and Alipay[21].

Data and Cloud Infrastructure

As of January 16th, 2024, both MIntegral and Pangle ad SDKs appear to use U.S.-based endpoints for their cloud infrastructure (operated by Amazon CloudFront and Akamai, respectively). However, the geolocation of the endpoint the SDK connects to has no bearing on the location of the ultimate processing and storage location of the data. Even if the data is stored and processed in the US, foreign actors may have access to query or pull data remotely. The geolocation of the endpoints used by an SDK should therefore by no means be taken as an indication that the data is kept in the U.S. (or some other place).

Recommendations

Two classes of threats posed by SDKs were introduced in this document.

- Malicious code contained in an SDK
- Malicious use of the data collected by an SDK

Both types of threats are difficult to defend against but each type can be targeted through a number of mitigation measures.

Malicious Code / Behavior by an SDK

By design, app creators use third-party SDKs without exactly understanding their code. It is unrealistic to expect that individual developers fully understand all aspects of third-party code they use and determine if the code is behaving in a malicious manner. However, as described earlier, many app creators use advertising mediation platforms that integrate third-party ad networks. Bringing app developers and ad networks together is the core part of their business so mediation platforms may be in a better position to vet ad SDKs. Regulation holding mediation platforms responsible for malicious code found in ad SDKs supported by their platforms would create an incentive to ensure that ad networks they offer are well behaved. Note, however, that audits of large code bases such as ad SDKs are expensive and require specialized reverse engineers. If such measures were used specifically for SDKs from particular countries, they could be seen as a trade barrier.

The security of U.S. users from malicious code in SDKs could be further strengthened through the development of technical protections built into the the platforms on which the apps in question are executed. As an example, Google is developing SDK Runtime[22] for Android, which isolates SDKs from the host app, protecting private app data from being accessed by a rogue

[19] https://support.google.com/googleplay/android-developer/answer/10281818?hl=en
[20] https://developers.weixin.qq.com/doc/oplatform/en/Mobile_App/WeChat_Pay/Android.html
[21] https://global.alipay.com/docs/ac/dws2/mobilesdkintegrationguide
[22] https://developer.android.com/design-for-safety/privacy-sandbox/sdk-runtime

SDK. Similar core security developments as well as research into other privacy-enabling technologies should be encouraged and promoted.

Abuse of Collected Data

As explained above, it is essentially impossible for an outsider to determine how data is used once it reaches the SDK's backend infrastructure, who can access it and from where. While it is probably impossible to completely prevent abuses of such data by an adversary (short of a heavy-handed and impractical blanket ban on any foreign SDKs), limiting the collected data to the minimum required for the business purpose of the SDK can help mitigate the damage that would result from such abuses.

App privacy labels are provided by both Apple and Google in their app stores. Both platforms provide mechanisms to facilitate the (mandatory) inclusion of use of data by third-party SDKs in privacy labels. However, both approaches ultimately fall short of being a full, reliable solution since they ultimately rely on self reporting. Strengthening of privacy legislation and penalties for knowingly making false claims about app or SDK data use will strengthen users' control over the privacy of their data.

SDK Transparency

The current situation, in which users are largely unaware of the SDKs contained in their apps, leaves them without the ability to make decisions about which SDKs they are comfortable loading on their devices and which ones they want to avoid. Mandatory disclosure of SDKs developers use in their apps would empower users to make their own decisions. Especially if malicious behavior or a privacy problem with a particular SDK has been reported, being able to scrutinize the "ingredient list" would empower users to vote with their feet, creating cascading incentives for app developers, ad mediation platforms and SDK developers to protect users from spying and other malicious behaviors.

QUESTION FOR THE RECORD

RESPONSE OF IVAN TSARYNNY, CHIEF EXECUTIVE OFFICER, FEROOT SECURITY

Questions for the Record
following the Commission's February 1st, 2024, hearing on "Current and Emerging Technologies in U.S.-China Economic and National Security Competition."

Answers by Ivan Tsarynny
CEO, Feroot Security.

1. *Beyond TikTok, what other Chinese companies associated with popular e-commerce platforms or mobile applications are known to have developed pixel trackers that are used in U.S. websites by ordinary consumers?*

Answer:
Many Chinese companies have developed pixel trackers, especially those used on U.S. websites by ordinary consumers. It's essential to clarify that while the term "pixel" might imply an image-based tracker, the reality is much broader. In addition to "Pixel" other, commonly used terms include web trackers, tags, scripts, beacons, JS libraries, and a number of other umbrella terms. All of these are based on sophisticated computer code that is executed by websites to monitor and collect data on user interactions. These tools can capture a wide range of information, and are much more comprehensive than the traditional understanding of pixels.

Examples of types of data that these advanced tracking tools can collect are:
- User session data: Insights into how long users stay on a site, which pages they visit, and how they interact with content.
- Geo-location: Determining a user's physical location based on their IP address, aiding in targeted advertising and content localization.
- Screen recordings: Capturing the user's navigation through a site, including clicks, scrolls, and mouse movements, to analyze user behavior and improve website design.
- IP address: Tracking the user's IP address for location data, security measures, and personalized content delivery.
- Inputs on online forms: Recording sensitive information entered by users, such as passwords, home addresses, travel plans, and even medical conditions.

List of some of the most popular Chinese companies that use the above-mentioned technologies are:

1. **Alibaba Group:** Known primarily for its e-commerce platforms like Alibaba.com and AliExpress, Alibaba Group also offers marketing and cloud services that might use tracking technologies to analyze user behavior and improve service delivery.

2. **Tencent:** As a major player in social media through platforms like WeChat and QQ, as well as in gaming and online services, Tencent may use pixel trackers for advertising purposes, user behavior analysis, and improving user experiences.

3. **ByteDance:** in addition to products managed by its subsidiary TikTok, ByteDance has developed and uses tracking technologies to understand user preferences and behavior, both for improving user experiences and for targeted advertising purposes.

4. **Baidu:** also referred to as the "Google of China," Baidu's search engine and its advertising services use tracking technologies to collect data on user behavior, preferences, and search histories to refine ad targeting and improve services.

5. **JD.com, Inc**.: Another giant in the e-commerce sector, JD.com, uses tracking technologies to analyze user behavior on its platforms, enhance customer experiences, and deliver personalized advertisements.

6. **Huawei:** Primarily known as a telecommunications equipment and consumer electronics manufacturer, Huawei also provides a suite of cloud services and operates its own apps and tools, which has user data analysis and tracking technologies.

7. **ZTE:** Similarly to Huawei, ZTE is another major player in the telecommunications and consumer electronics field. While its primary business is focused on network equipment and smartphones, it also ventures into areas that may use data tracking.

8. **Xiaomi:** A major electronics and smart device manufacturer that provides a wide range of products from smartphones to smart home devices. Xiaomi's ecosystem includes services like Mi Cloud, and its internet services segment uses data analytics and tracking to enhance user experiences and offer personalized content.

9. **Weibo:** Often referred to as the "X" or “Twitter of China," Weibo is a popular social media platform in China with a significant global user base. It uses tracking technologies for advertising and to analyze user interaction and engagement.

10. **NetEase:** Specializing in internet technology, NetEase operates in gaming, education, music, and email services. It's known for some of the most popular online games as well as its streaming music service, both of which likely involve user tracking for personalization and analytics.

11. **OPPO:** A consumer electronics and mobile communication company, known for its smartphones. Like other smartphone manufacturers, OPPO collects data through its mobile application and associated services for user experience enhancement and marketing.

12. **Vivo:** Another major player in the smartphone market, Vivo uses software and services that potentially include tracking technologies for understanding user preferences and behavior.

13. **iQIYI:** Often referred to as the Netflix of China, iQIYI is a major video streaming platform with a significant user base. It uses tracking technologies for various purposes.

14. **Sina Corp:** The parent company of Weibo, Sina is a technology company that focuses on online media and services. While Weibo has been mentioned, Sina Corp's broader range of services also utilizes data analytics and tracking for personalized content and ads.

15. **Perfect World:** A game developer and publisher, known for creating online games, including massively multiplayer online role-playing games (MMORPGs). Perfect World uses tracking to enhance user experiences and offer personalized gaming content.

16. **Tencent Music** Entertainment (TME): Operating popular music apps like QQ Music, Kugou, and Kuwo, TME uses tracking technologies to recommend music, analyze user preferences, and tailor advertising to its listeners.

17. **Bilibili:** A video sharing website geared towards younger audiences, offering a wide range of content including animation, comics, and games. Bilibili uses tracking to analyze viewer preferences, enhance user engagement, and personalize content recommendations.

During our research, 879 instances of such Chinese technologies and tools were identified. These are directly or indirectly under control of China's Big Tech companies listed below:

- Alibaba Group
- Huawei Technologies Co., Ltd.
- Weibo (Sina Corporation)
- Tencent Holdings Ltd.
- Baidu, Inc.
- ByteDance Ltd. (in addition to tools managed by TikTok)
- MarkMonitor Information Technology (Shanghai) Co., Ltd.
- Taobao (China) Software Co., Ltd.

2. *On what scale are they used and what kinds of data are harvested from U.S. users?*

Answer:
As of March 2023, 8.61% of all private business websites that were analyzed, had data collection tools that are associated with Chinese companies. Breakdown by industry is below:

- Financial Services and Banking - 5%
- Healthcare and Telehealth - 2%
- Technology and SaaS - 7.8%
- e-Commerce - 20.8%
- Airlines - 6.7%

In December of 2023 the presence of specifically TikTok tracking pixels increased by 75% on financial services and banking websites—rising from 5% to 8.5%; and increased by 178% on healthcare service provider websites—rising from 2% to 5% of all healthcare websites.

Our upcoming research will identify the overall increase of data harvesting of U.S. users by Chinese technologies and companies in 2024.

As mentioned in answer to the first question as these types of tracking tools can collect multiple kinds of data, including:

- User session data: Insights into how long users stay on a site, which pages they visit, and how they interact with content.
- Geo-location: Determining a user's physical location based on their IP address, aiding in targeted advertising and content localization.
- Screen recordings: Capturing the user's navigation through a site, including clicks, scrolls, and mouse movements, to analyze user behavior and improve website design.
- IP address: Tracking the user's IP address for location data, security measures, and personalized content delivery.
- Inputs on online forms: Recording sensitive information entered by users, such as passwords, home addresses, travel plans, and even medical conditions.

We found pixel tracking tools that belong to Chinese companies collecting more user information than similar tracking technologies developed by companies outside of China. For instance, search keywords, search results that are shown to consumers, text that is shown to customers on webpages they visit and more.

3. *What risks does the harvesting of this data create for U.S. consumers?*

Answer:
The harvesting of U.S. consumers data by Chinese companies, or any entities that are under the jurisdiction of China, poses several potential risks to U.S. consumers, primarily revolving around privacy, security, and geopolitical concerns. Here are some examples:

Breach of Confidentiality and Privacy: The collection and analysis of personal data by companies can lead to significant privacy infringements. Users may not be fully aware of what data is being collected, how it is being used, or who it is being shared with, leading to concerns over personal privacy.

Surveillance and Censorship: There are concerns that data collected by Chinese companies could be accessed by the Chinese government for surveillance purposes, given the legal and regulatory framework in China that requires companies to cooperate with state intelligence work. This raises fears about the potential for censorship or manipulation of information accessible to or about U.S. consumers.

Targeted Propaganda and Misinformation: The detailed user profiles generated from harvested data could be used to target U.S. consumers with propaganda or misinformation campaigns, potentially influencing public opinion and interfering in democratic processes.

Data Security Risks: The storage and processing of data by companies, especially on servers located in other countries, may expose users to increased risks of data breaches and cyberattacks. Such incidents can lead to sensitive personal information being leaked or sold on the dark web.

Economic Espionage: There are concerns that sensitive business information or intellectual property could be collected and used to benefit Chinese companies at the expense of U.S. businesses, leading to economic disadvantages.

Trust and Reputation: The knowledge that data is being collected by foreign companies, particularly those associated with countries having different values and regulations around privacy, can erode trust in the digital ecosystem, impacting the willingness of consumers to engage with online services.

Legal and Regulatory Compliance Risks: companies that serve U.S. consumers may find themselves at risk of violating privacy laws and regulations, such as the General Data Protection Regulation (GDPR) in Europe, which have strict requirements on data collection, processing, and transfer which can expose them to significant fines.

National Security: The aggregation of data by foreign companies, particularly those from a geopolitical rival such as China, raises national security concerns. This data could potentially be

used to map out social networks of government employees, identify vulnerabilities in critical infrastructure, or track the movements and activities of individuals in sensitive positions.

QUESTION FOR THE RECORD

RESPONSE OF NGOR LUONG, SENIOR RESEARCH ANALYST, CENTER FOR SECURITY AND EMERGING TECHNOLOGY

Questions for the Record following the Commission's February 1st, 2024, hearing on "Current and Emerging Technologies in U.S.-China Economic and National Security Competition."

Response by Ngor Luong
Senior Research Analyst, Center for Security and Emerging Technology

1. In your testimony you assert that small and medium-sized Chinese companies, also known as "Little Giants," have received nearly $224 billion in funding from venture capital firms since 2018. What percentage of this $224 billion in venture capital funding is from sources outside of China? What percentage of that funding might be from the United States?

Response:

I went back and checked my citation for the $224 billion figure (on page 4 of my written testimony), and the source didn't have an immediately available breakdown of U.S. investor involvement. That said, I am planning to look at this issue for a small project down the road and can share any results I find once I have them.

QUESTION FOR THE RECORD

RESPONSE OF EDWARD PARKER, PHYSICAL SCIENTIST, RAND CORPORATION

Testimony

EDWARD PARKER

The Chinese Industrial Base and Military Deployment of Quantum Technology

Addendum

CT-A3189-2

Document submitted March 15, 2024, as an addendum to testimony before the U.S.-China Economic and Security Review Commission on February 1, 2024

For more information on this publication, visit www.rand.org/t/CTA3189-2.

Testimonies

RAND testimonies record testimony presented or submitted by RAND associates to federal, state, or local legislative committees; government-appointed commissions and panels; and private review and oversight bodies.

Published by the RAND Corporation, Santa Monica, Calif.

Limited Print and Electronic Distribution Rights

www.rand.org

The Chinese Industrial Base and Military Deployment of Quantum Technology

Testimony of Edward Parker[1]
RAND[2]

Addendum to testimony before the U.S.-China Economic and Security Review Commission

Submitted March 15, 2024

Following the hearing on February 1, the U.S.-China Economic and Security Review Commission sought additional information and requested an answer to the question in this document. The answer was submitted for the record.

Question

In your oral testimony, you alluded to six or seven distinct technical approaches to quantum that have non-overlapping supply chains, and observed that it is difficult to discern which approach may "win." Please provide an assessment of the mature/near-term quantum technologies that should be updated or clarified within export control regimes.[3]

Answer

The U.S. government has two main mechanisms for administering export controls. The first is the International Traffic in Arms Regulations (ITAR), which are administered by the

---

[1] The opinions and conclusions expressed in this addendum are the author's alone and should not be interpreted as representing those of RAND or any of the sponsors of its research.

[2] RAND is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest. RAND's mission is enabled through its core values of quality and objectivity and its commitment to integrity and ethical behavior. RAND subjects its research publications to a robust and exacting quality-assurance process; avoids financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursues transparency through the open publication of research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. This testimony is not a research publication, but witnesses affiliated with RAND routinely draw on relevant research conducted in the organization.

[3] All questions are presented verbatim as they were submitted to RAND.

Department of State and cover military technologies,[4] and the second is the Export Administration Regulations (EAR), which are administered by the Department of Commerce and cover dual-use technologies with both military and civilian uses.[5] All quantum technologies are dual-use, so I believe that the EAR is the most logical mechanism for administering any export controls on quantum technology.

Quantum technology is a complex field with widely varying levels of technology readiness, and I believe it is worth separately discussing its major subfields of quantum sensing, quantum communications, and quantum computing.

Broadly speaking, quantum sensing is the most technically mature of the three subfields of quantum technology. Moreover, quantum sensing technologies have several potential applications that are particularly relevant for defense, such as subsurface sensing and navigation in GPS-denied environments.[6] The Office of the Under Secretary of Defense for Research and Engineering has publicly identified several quantum sensing technologies, such as certain classes of atomic clocks, quantum magnetometers, and quantum inertial sensors, as both being relatively technically mature and having high potential military impact.[7] Any export controls covering these more-mature technologies should reflect the current state-of-the-art understanding of quantum sensing technology.

There are currently no export controls on "quantum sensors" as a category, but there are many existing export controls that would apply to specific quantum sensors. For example, there exist EAR export controls for very high-sensitivity magnetometers, gravimeters, and superconducting electromagnetic sensors that would cover certain types of quantum sensors under development today.[8] These regulations should reflect subject-matter experts' best technical understanding of the capability thresholds for military operational utility—and they should be updated if they do not—but there is no need to completely start from scratch.

In my view, export controls are most effective when applied to end-user systems with operational military capabilities rather than to basic components. For example, if a magnetometer reaches a performance threshold that delivers a useful military capability, then that magnetometer should be export-controlled regardless of whether it uses quantum technology "under the hood." Under this capability-focused approach, U.S. export controls would probably

---

[4] U.S. Department of State, "Directorate of Defense Trade Controls," webpage, undated, https://www.state.gov/bureaus-offices/under-secretary-for-arms-control-and-international-security-affairs/bureau-of-political-military-affairs/directorate-of-defense-trade-controls-pm-ddtc/.

[5] International Trade Administration, "U.S. Export Regulations," webpage, undated, https://www.trade.gov/us-export-regulations.

[6] Edward Parker, Richard Silberglitt, Daniel Gonzales, Natalia Henriquez Sanchez, Justin Lee, Lindsay Rand, Jon Schmid, Peter Dortmans, and Christopher A. Eusebi, *An Assessment of U.S.-Allied Nations' Industrial Bases in Quantum Technology*, RAND Corporation, RR-A2055-1, 2023, https://www.rand.org/pubs/research_reports/RRA2055-1.html.

[7] Parker et al., 2023, p. 3, Figure 1.1.

[8] Code of Federal Regulations, Title 15, Subtitle B, Chapter VII, Subchapter C, Part 774, "Part 774 – the Commerce Control List," Sections 6A996–6A997, last updated March 7, 2024.

not require extensive changes until quantum technology becomes capable of delivering *qualitatively* new capabilities, such as decryption.

By contrast, quantum computing and quantum communications technologies are at a lower technical maturity than quantum sensing (with the exception of one application, quantum key distribution, whose likely military impact is low),[9] and their practical applications are probably further out.

As the question mentions, there are currently a wide variety of technical approaches being researched in parallel, which require very different critical components. Some technical approaches are somewhat further along than others: For example, quantum computers based on superconducting, trapped-ion, or neutral-atom qubits are currently somewhat more advanced than quantum computers based on photonic, silicon-spin, or topological qubits.[10] But there is no clear evidence that *any* of these approaches will deliver military operational utility in the near term.

Export controls could impose challenges on U.S. companies whose revenues are still modest, thereby risking their financial health. The administration's goal for its export control policy is to have effective and narrowly targeted controls on critical *military* technologies—a "small yard" with a "high fence."[11] In my judgment, it would be very difficult to impose such export controls on quantum computing or communication systems until experts have a better technical understanding of either (a) their concrete military end-user applications or (b) the most-promising technical pathways and timelines for creating them. Both of these critical data points remain highly uncertain today.

Some experts take a different perspective: They believe that the risk of a competitor nation gaining access to these critical technologies is so high that the highest priority should be to delay competitor nations from gaining these technologies, even if doing so might slow the development of the U.S. commercial industry. Those who take this perspective would endorse a strategy of broadly scoped export controls.[12] But I do not believe that such a strategy is likely to work. I believe that export controls on emerging technologies can reliably set back the targeted nations in the short run, but in the longer run the targeted nations will likely find alternative sources or will develop their own indigenous production capacity. (For example, there is some evidence that China is already mitigating some of the impacts of the 2022 U.S. export controls

---

[9] Parker et al., 2023, p. 3, Figure 1.1; National Security Agency, "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)," webpage, undated, https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

[10] Edward Parker, Daniel Gonzales, Ajay K. Kochhar, Sydney Litterer, Kathryn O'Connor, Jon Schmid, Keller Scholl, Richard Silberglitt, Joan Chang, Christopher A. Eusebi, and Scott W. Harold, *An Assessment of the U.S. and Chinese Industrial Bases in Quantum Technology*, RAND Corporation, RR-A869-1, 2022, https://www.rand.org/pubs/research_reports/RRA869-1.html.

[11] The White House, "Remarks by National Security Advisor Jake Sullivan on the Biden-Harris Administration's National Security Strategy," October 13, 2022.

[12] The White House, "Remarks by National Security Advisor Jake Sullivan at the Special Competitive Studies Project Global Emerging Technologies Summit," September 16, 2022.

on advanced semiconductors).[13] I am not confident that any export controls imposed today will necessarily delay the targeted nations from developing quantum computing or communications technologies that are still many years from maturity. Moreover, targeted countries could take several responses to mitigate or retaliate against quantum technology export controls imposed by the United States.[14] For example, the Chinese government already appears to be shoring up China's domestic quantum computing supply chain to reduce its dependence on foreign suppliers.[15] Therefore, I believe that export controls on quantum technology should remain narrowly scoped to concrete and near-term military capabilities.

I will conclude with three cross-cutting suggestions for how any export controls on quantum technology could be designed to be most effective:[16]

1. The export controls should make clear and unambiguous exactly which technologies (and which potential customers) are covered. Those crafting the regulations should consider feedback from industry on publicly proposed rules—not to give those companies a veto but to verify that the affected companies understand exactly how the regulations would apply to them. Two topics in particular should have clear regulations:
    a. When a U.S. person releases certain technical information to a foreign person who is working within the United States, the U.S. government considers this to be a *deemed export* that is subject to control.[17] Foreign nationals form a very important part of the U.S. quantum development ecosystem,[18] so U.S. firms should receive clear guidance on allowed information-sharing with noncitizens.
    b. Many quantum computing companies do not sell hardware but instead operate under a cloud-access model whereby customers submit tasks remotely and the companies perform the actual computations in-house. Any export controls on quantum computing should clearly address the permissibility of selling computing *services* to foreign customers, even if no physical hardware ever leaves the United States.

---

[13] Gregory C. Allen, "In Chip Race, China Gives Huawei the Steering Wheel: Huawei's New Smartphone and the Future of Semiconductor Export Controls," Center for Strategic & International Studies, October 6, 2023; Megan Hogan, "Export Controls Are Only a Short-Term Solution to China's Chip Progress," *War on the Rocks*, December 22, 2023.

[14] Kevin Klyman, "The U.S. Wants to Make Sure China Can't Catch Up on Quantum Computing," *Foreign Policy*, March 31, 2023.

[15] "China to step up quantum computing, AI in tech self-sufficiency drive," Reuters, March 5, 2024.

[16] Further discussion of export controls on quantum technology can be found in Edward Parker, *Promoting Strong International Collaboration in Quantum Technology Research and Development*, RAND Corporation, PE-A1874-1, February 2023, pp. 15–18, https://www.rand.org/pubs/perspectives/PEA1874-1.html.

[17] Bureau of Industry and Security, U.S. Department of Commerce, "Deemed Exports," webpage, undated, https://www.bis.doc.gov/index.php/policy-guidance/deemed-exports.

[18] Subcommittee on Economic and Security Implications of Quantum Science, Committee on Homeland and National Security, National Science and Technology Council, *The Role of International Talent in Quantum Information Science*, October 2021.

2. Any licensing requirements should have a minimally burdensome compliance process, because many quantum technology companies are small and do not have legal teams with expertise in export control procedures.
3. Quantum technology is developing rapidly, so export controls should be regularly updated to reflect the current state of the art. The update process should not be a one-way ratchet that always adds new restrictions; it should also remove restrictions on items that are no longer critical.