AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

COUNTERING THREATS POSED BY THE CHINESE COMMUNIST PARTY TO U.S. NATIONAL SECURITY

HEARING

BEFORE THE

COMMITTEE ON HOMELAND SECURITY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

MARCH 5, 2025

Serial No. 119–6

Printed for the use of the Committee on Homeland Security

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

U.S. GOVERNMENT PUBLISHING OFFICE

60–878 WASHINGTON : 2025

COMMITTEE ON HOMELAND SECURITY

MARK E. GREEN, MD, Tennessee, *Chairman*

MICHAEL T. MCCAUL, Texas, *Vice Chair*
CLAY HIGGINS, Louisiana
MICHAEL GUEST, Mississippi
CARLOS A. GIMENEZ, Florida
AUGUST PFLUGER, Texas
ANDREW R. GARBARINO, New York
MARJORIE TAYLOR GREENE, Georgia
TONY GONZALES, Texas
MORGAN LUTTRELL, Texas
DALE W. STRONG, Alabama
JOSH BRECHEEN, Oklahoma
ELIJAH CRANE, Arizona
ANDREW OGLES, Tennessee
SHERI BIGGS, South Carolina
GABE EVANS, Colorado
RYAN MACKENZIE, Pennsylvania
BRAD KNOTT, North Carolina

BENNIE G. THOMPSON, Mississippi, *Ranking Member*
ERIC SWALWELL, California
J. LUIS CORREA, California
SHRI THANEDAR, Michigan
SETH MAGAZINER, Rhode Island
DANIEL S. GOLDMAN, New York
DELIA C. RAMIREZ, Illinois
TIMOTHY M. KENNEDY, New York
LAMONICA MCIVER, New Jersey
JULIE JOHNSON, Texas, *Vice Ranking Member*
PABLO JOSÉ HERNÁNDEZ, Puerto Rico
NELLIE POU, New Jersey
VACANT
VACANT
VACANT

ERIC HEIGHBERGER, *Staff Director*
HOPE GOINS, *Minority Staff Director*
SEAN CORCORAN, *Chief Clerk*

CONTENTS

Page

STATEMENTS

Honorable Michael Guest, a Representative in Congress From the State of Mississippi:
Oral Statement 1
Honorable Mark E. Green, a Representative in Congress From the State of Tennessee, and Chairman, Committee on Homeland Security:
Closing Statement 82
Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:
Oral Statement 3
Prepared Statement 5

WITNESSES

Mr. Michael Pillsbury, Private Citizen:
Oral Statement 7
Prepared Statement 8
Mr. William R. Evanina, Founder and Chief Executive Officer, The Evanina Group:
Oral Statement 17
Prepared Statement 19
Mr. Craig Singleton, Senior Fellow and China Program Senior Director, Foundation for Defense of Democracies:
Oral Statement 26
Prepared Statement 28
Mr. Rush Doshi, Ph.D., Private Citizen:
Oral Statement 44
Prepared Statement 47

FOR THE RECORD

Honorable Bennie G. Thompson, a Representative in Congress From the State of Mississippi, and Ranking Member, Committee on Homeland Security:
Article, *CNN*, March 1, 2025 83
Article, *New York Times*, February 5, 2025 84

APPENDIX

Questions From Chairman Mark E. Green, MD for Michael Pillsbury 89
Questions From Chairman Mark E. Green, MD for William R. Evanina 89
Questions From Chairman Mark E. Green, MD for Craig Singleton 90

COUNTERING THREATS POSED BY THE CHINESE COMMUNIST PARTY TO U.S. NATIONAL SECURITY

Wednesday, February 5, 2025

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOMELAND SECURITY,
WASHINGTON, DC.

The committee met, pursuant to notice, at 10:06 a.m., in room 310, Cannon House Office Building, Hon. Michael Guest presiding.

Present: Representatives McCaul, Guest, Pfluger, Brecheen, Ogles, Biggs of South Carolina, Evans of Colorado, Mackenzie, Thompson of Mississippi, Swalwell, Correa, Thanedar, Magaziner, Goldman, Kennedy of New York, McIver, Hernandez, and Pou.

Mr. GUEST. The Committee on Homeland Security will come to order.

Without objection, the Chair may declare the committee in recess at any point.

The purpose of today's hearing is to examine the threats posed by the Chinese Communist Party to U.S. national security. I now recognize myself for an opening statement.

Today's hearing focuses on the generational threat that the Chinese Communist Party poses to our homeland. The first step is to recognize the nature of our adversary.

For decades China has steadily pursued a long-term grand strategy to replace the United States as the leading global power. We cannot afford wishful thinking or willful ignorance about the nature of the Chinese regime and its on-going efforts to undermine the United States.

We also need proactive measures to counter the CCP's actions that jeopardize our Homeland Security, especially given that most of the threats they pose are unfolding now below the threshold of traditional conflict.

One of our distinguished witnesses, Dr. Michael Pillsbury, has persuasively argued that China is engaged in a 100-year marathon, a grand strategy to surpass and overtake the United States on the world stage, and reorder the world according to the CCP's priorities and their values.

This long-term strategy is comprehensive. It is not limited to military capabilities. It includes the full range of economic, diplomatic, technological, and political competition.

Critically China is willing to play the long game and build up its power over the course of decades. The CCP's ultimate aim is not to enjoy a peaceful balance of power with the West but to establish its position as the dominant world power.

A world oriented around the vision and values of the CCP would look very different from the unparalleled freedom and prosperity produced by the Pax Americana.

In contrast, the Chinese vision would mean a global order subordinate to the desires and the interests of a totalitarian Communist regime.

In recent years, the People's Republic of China has engaged in sustained campaigns of transnational repression, intellectual property theft, and espionage here in the United States.

Over the past 4 years, there have been more than 60 espionage cases across 20 States linked to the CCP, operations to gather intelligence on sensitive military information and the theft of technology and trade secrets.

Just this past December, a Chinese citizen was arrested for flying a drone over Vandenberg Space Force Base in California. He was apprehended at the airport, trying to board a flight back to China.

Additionally, agents of Beijing have targeted dissidents and regime critics within the United States through covert Chinese police stations in New York City and other major cities.

Espionage, including economic and technology theft, are key to the CCP's strategy to undermine the United States, while fueling its own technological advancement.

Today the United States remains unmatched as a hub for technological innovation, but the PRC routinely and systematically steals technology and research from American companies and universities for the benefit of the Chinese state industrial complex.

Many Chinese corporations are state-owned enterprises, and China's national security laws give the regime the power to force companies to hand over any information or data.

Moreover, the CCP has implemented a national strategy of military-civil fusion to position the People's Liberation Army as the dominant military power by 2049.

Part of this strategy is mass intellectual property theft of sensitive information from both U.S. military and civilian targets.

The CCP exploits American research and development to the tune of several hundred billion dollars every single year, and this theft directly affects all Americans.

As one of our witnesses today will state, these losses cost the average American family of 4 between $4- and $6,000 yearly.

This is happening through traditional espionage tactics and targeted cyber attacks affecting industries engaged in innovative developments, ranging from military technology and artificial intelligence to semiconductors and medical research.

Here in the 119th Congress, this committee has the opportunity to advance significant legislation to counter the CCP's effort to undermine our national security.

Working together, we can find practical policy solutions to shift the playing field in our favor. Whether we are countering acts of transnational repression, strengthening our cybersecurity with legislation by the Cyber PIVOTT Act, or shoring up our economic security and supply chain resilience, we can make major headway on meeting the challenges posed by the PRC.

The freedoms and prosperity of the American people in the decades to come depend on our courage, on our foresight, and our ability to take decisive action now.

I look forward to a serious discussion on the critical threats posed by the CCP to the United States homeland as we kick off this committee's effort to protect the homeland against foreign actors.

I now at this time recognize the Ranking Member, the gentleman from Mississippi, Mr. Thompson, for his opening statement.

Mr. THOMPSON. Thank you very much, Mr. Chairman, and before I begin my statement, let me say with a heavy heart that we've been informed that a Member of this committee, Mr. Sylvester Turner, former mayor of Houston, passed earlier this morning.

At some point, we will do a more formal recognition of his tenure on the committee by the committee, so I wanted to make that part of just people knowing.

Good morning and welcome to our panel of witnesses. Today the committee is examining the threats posed by the Chinese Communist Party to our national security.

The threats are very real. The CCP is looking for every opportunity to undermine our security and get the upper hand on the global United States.

The problem is Congressional Republicans' tough talk on China is at odds with the Trump administration's actions, which are hurting America's ability to counter threats from the CCP.

For example, China is carrying out cyber attacks, or espionage, to preposition for attacks against our critical infrastructure in the event of future conflicts.

According to the intelligence community's 2024 Worldwide Threat Assessment, China remains the most active and persistent cyber threat to the U.S. Government, private sector, and critical infrastructure networks.

Unbelievably, President Trump has fired key cybersecurity personnel at the Department of Homeland Security and dismissed members of the Cyber Safety Review Board investigating recent Chinese attacks.

We are hearing that up to 50 percent of the remaining work force of the Cybersecurity Infrastructure Security Agency might be targeted in the days ahead.

Let's be clear. The Trump administration gutting U.S. cyber defenses makes it harder to protect Americans against Chinese cyber attacks and makes us less safe.

What are Congressional Republicans doing to preserve the work force that protects our cyber networks?

Nothing.

Meanwhile, in its rush to fire Government employees, the Trump administration sent out an unclassified email with the names of CIA analysts and operatives working to counter China. One former CIA officer referred to the email as a, "counterintelligence nightmare".

What are Congressional Republicans doing to stop the White House chaos and protect intelligence information from Chinese hackers?

Nothing.

China is also on a mission to steal our economic secrets and personal data to gain a competitive advantage. Fortunately for China, Elon Musk is lending a hand.

Musk and his DOGE lackeys have made key Federal data systems more vulnerable and put millions of Americans' data at risk by snooping in sensitive cyber networks without adequate security protections.

What are Congressional Republicans doing to protect Americans' personal data from Musk, DOGE, and possible exploitation by China?

Nothing.

Additionally, China is using its Belt and Road Initiative to leverage investments to expand its influence in the developing world.

Rather than protecting America's interests globally, the Trump-Musk administration slashed U.S. foreign investment and alienated allies and partners, undermining our ability to compete with China for influence on the global stage.

This morning, the Supreme Court rejected the Trump-Musk administration efforts to end the U.S. foreign investment, clearing the way for the State Department and USAID to restart nearly $2 billion in payments.

But what are Congressional Republicans doing to protect American interests around the world?

Nothing.

The Trump administration is weakening America against China while Elon Musk sits inside the White House asserting seemingly limitless influence over the Executive branch of government. That's no coincidence.

Musk has troubling close ties with China. Though the full extent of his entanglements are unknown because he refuses to file a public financial disclosure and has failed to disclose meetings with Chinese officials.

Still, it's clear Musk's businesses rely heavily on China for their success, and he has over a billion dollars in loans from state-owned Chinese banks.

Musk has taken public stances to the benefit of China and has even suggested giving some control over Taiwan to China.

His own former DOGE co-chair raised concerns about Musk's ties to China, saying, "I have no reason to think Elon won't jump like a circus monkey when Chinese President Xi Jinping calls in the hour of need." That doesn't sound like America first. It sounds like China first.

What are Congressional Republicans doing to sound the alarm about someone beholden to China running our government?

Nothing.

Democrats agree that the CCP poses a threat to U.S. security and want to keep Americans safe. If Republicans want to counter China's influence and protect U.S. interests, they should start by holding their own administration accountable.

Talking tough on China but bending the knee to Trump and Musk plays right into the CCP's hands. Let's hope the other side remembers their oath is to the Constitution and not to the man in the White House or his unelected billionaire co-president.

Mr. Chairman, I yield back.

[The statement of Ranking Member Thompson follows:]

STATEMENT OF RANKING MEMBER BENNIE G. THOMPSON

MARCH 5, 2025

Today, the committee is examining the threats posed by the Chinese Communist Party to our national security. These threats are very real. The CCP is looking for every opportunity to undermine our security and get the upper hand on the U.S. globally.

The problem is, Congressional Republicans' tough talk on China is at odds with the Trump administration's actions, which are hurting America's ability to counter threats from the CCP. For example, China is carrying out cyber attacks for espionage and to position itself for attacks against our critical infrastructure in the event of a future conflict.

According to the intelligence community's 2024 World Wide Threat assessment, "China remains the most active and persistent cyber threat to U.S. Government, private sector, and critical infrastructure networks."

Unbelievably, President Trump has fired key cybersecurity personnel at the Department of Homeland Security and dismissed members of the Cyber Safety Review Board investigating recent Chinese attacks.

We are hearing that significant cuts are coming for the remaining workforce at the Cybersecurity and Infrastructure Security Agency. Let's be clear—the Trump administration gutting U.S. cyber defenses makes it harder to protect Americans against Chinese cyber attacks and makes us less safe.

What are Congressional Republicans doing to preserve the workforce that protects our cyber networks? Nothing.

Meanwhile, in its rush to fire Government employees, the Trump administration sent out an unclassified email with the names of CIA analysts and operatives working to counter China. One former CIA officer referred to the email as a, quote, "counterintelligence nightmare."

What are Congressional Republicans doing to protect this information from Chinese hackers? Nothing.

China is also on a mission to steal our economic secrets and personal data to gain a competitive advantage. Fortunately for China, Elon Musk is lending a hand. Musk and his DOGE lackeys have made key Federal data systems more vulnerable and put millions of Americans' data at risk by snooping in sensitive cyber networks without adequate security protections.

What are Congressional Republicans doing to protect Americans' personal data from Musk, DOGE, and possible exploitation by China? Nothing.

Additionally, China is using its "Belt and Road Initiative" to leverage investments to expand its influence in the developing world. Rather than protecting America's interests globally, the Trump-Musk administration has slashed U.S. foreign investment and alienated allies and partners, undermining our ability to compete with China for influence on the global stage.

What are Congressional Republicans doing to protect American interests and influence around the world? Nothing.

The Trump administration is weakening America against China, while Elon Musk is exerting seemingly limitless influence over the Executive branch of government. That's no coincidence. Musk has close ties with China, though the full extent of his entanglements is unknown because he refuses to file a public financial disclosure and has failed to disclose meetings with Chinese officials.

Still, it is clear Musk's businesses rely heavily on China for their success, and he has over a billion dollars in loans from state-owned Chinese banks. Musk has also taken public stances to the benefit of China and has even suggested giving some control over Taiwan to China.

His own former DOGE co-chair raised concerns about Musk's ties to China, saying "I have no reason to think Elon won't jump like a circus monkey" when [Chinese President] Xi Jinping calls in the hour of need." That doesn't sound like "America First"—it sounds like "China First."

What are Congressional Republicans doing to sound the alarm about someone beholden to China running our Government? Nothing.

Democrats agree that the CCP poses a threat to U.S. security and want to keep Americans safe. If Republicans want to counter China's influence and protect U.S. interests, they should start by holding their own administration accountable.

Talking tough on China but bending the knee to Trump and Musk plays right into the CCP's hands. Let's hope the other side remembers their oath is to the Constitu-

tion and not to the man in the White House or his unelected billionaire co-President.

Mr. GUEST. Before we move forward, in light of the announcement by Ranking Member Thompson regarding the passing of Sylvester Turner, I would like us to please take a moment of silence to remember him and to recognize his service.

[Moment of silence.]

Mr. GUEST. Thank you.

The other Members of the committee are recognized and reminded that opening statements may be submitted for the record.

I want to thank our witnesses for being here this morning. I had the opportunity to visit with each of you very briefly before the commencement of this hearing, so thank you for your dedication, your commitment.

I know that you are all subject-matter experts in this field, something that is extremely important to us, to this committee, to this Congress, and to this administration.

I want to, again, thank you for being here. I would ask, if you would at this time, please raise your right hand as I issue the oath.

[Witnesses sworn.]

Mr. GUEST. Thank you. Let the record reflect that the witnesses have answered in the affirmative, and thank you for taking such an oath.

I would now like to formally introduce our witnesses. First, Dr. Michael Pillsbury, he is a renowned China scholar and author of "The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower."

He has served in many distinguished governmental roles, including as an assistant under secretary of defense for policy, planning, special assistant—he started as special assistant for Asian affairs in the Office of the Secretary of Defense.

He is a member of the Council on Foreign Relations and the International Institute for Strategic Studies and a senior fellow for China's strategies at The Heritage Foundation. Dr. Pillsbury earned his Ph.D. from Columbia University.

The Honorable William Evanina is a former director of the National Counterintelligence and Security Center, in which he led the United States Government's counterintelligence activities. As director, he oversaw key national programs dedicated to countering intelligence collection efforts by foreign adversaries.

Prior to serving as director of the NCSC, he served as the chief of the CIA's counterespionage group. He has over 31 years of service in the Federal Government, including 24 years as a special agent with the Bureau of Investigations, including service as assistant special agent in charge of the FBI's Washington field office.

Next is Mr. Craig Singleton. Craig is a senior director of the China Program at the Foundation for Defense of Democracies. He is a leading expert on U.S./China relations, an expert on China's technological threat, and China's military-civil fusion strategy.

He previously served as a U.S. diplomat focusing on national security issues dealing with China, North Korea, and the Indo-Pacific.

Finally, Dr. Rush Doshi is the C.V. Starr senior fellow for Asian studies and director of the China Strategies Initiative at the Council on Foreign Relations.

Dr. Doshi was deputy senior director for China and Taiwan on the National Security Council from 2021 to 2024. He is also an assistant professor in the Security Studies Program at Georgetown's Walsh School of Foreign Service.

I want to thank all of our witnesses for being here today. I would now like to recognize each of you for 5 minutes to summarize your remarks in the form of an opening statement.

I will begin with Dr. Pillsbury.

STATEMENT OF MICHAEL PILLSBURY, PRIVATE CITIZEN

Mr. PILLSBURY. Thank you Mr. Acting Chairman and Ranking Member Thompson.

Mark Green, your Chairman, advised me I should try to say something new and fresh and assume that the Members of the Homeland Security Committee are all highly informed about China already and don't need the presentation from me that says, you know, the capital city is Beijing, and the population is 1.4 billion. So I'll try to meet his challenge.

He said, "Why don't you go back to your book 10 years ago where you recommended 12 steps in the last chapter and then tell us which of the 12 remain to be implemented."

It's kind-of hard because only the first one was implemented. The first one was to recognize our long-term competition with China.

Ten years ago, that was kind-of strange. Now, pretty much everybody talks as though it's common knowledge. So that's 1 out of 12.

The other 11, I'm not going to mention all, but I'm going to mention 3 that are, I think, relevant to this Homeland Security Committee because I used to be a Senate staffer.

My first job in 1978 in the Senate staff was the Senate Budget Committee, and I learned a lesson fairly quickly: The jurisdiction of committees is something Senators fight over.

So, if we could have something unique that Homeland Security does itself with your Senate partner Rand Paul as well, there's some areas that need to be looked at that could be done just by your committee.

Now, don't get angry at me, but one of the first things is to consider this committee going to Beijing, not just Foreign Affairs and Foreign Relations and Armed Services travel, but Homeland Security, with a well-organized agenda agreed to in advance by the Chinese, could answer questions you have and also would be a kind-of healthy pressure on how the Chinese see America's request.

The second idea I have is that Homeland Security's jurisdiction includes a lot of agencies, and one of my most important recommendations 10 years ago is we try to do a survey, even annual if necessary, of exactly what each Government department or agency is doing to assist China.

The head of OMB tried to do this. He's back now again as the head of OMB. He put out a very specific kind of document to all Government agencies: Define what you're doing to help China one way or another—it was defined very broadly—how much money is

involved, and yes or no, do you have authority from Congress to do this?

The study ran into enormous difficulties. Agencies did not want to admit that they each had a program with China, and none of them had Congressional authorization to do what they were doing.

One of these was helping the labor union disputes. The Labor Department was sending mediators. Another one was that Chinese banks were in trouble. So a team from the Controller of the Currency went out to show Chinese banks, state-owned banks, how better to measure nonperforming loans.

All of these programs or maybe as many as 20 were designed originally when our relationship with China was one of sort-of the older brother helping China get into the world.

All that has changed, but these programs continue on. Many of them are under the jurisdiction of this committee.

The other idea—because of limits of time, let me kind-of just dwell on it for 30 seconds—the other idea was, if we're in a long-term competition with China, how do we know where we're going? How do we know the most effective measures that need to be adopted?

You all know the Mad Hatter in "Alice in Wonderland." When any road—if you don't know where you're going, any road will take you there. That's kind-of the situation we're in now with the picture of the long-term competition.

How is it going to end? I can tell you what the Chinese say. A very common scenario, talking with Chinese or reading their materials, is they think America is looking for another Gorbachev and wants the collapse of the Chinese Communist Party, Russian-style. Very, very similar concerns.

Xi Jinping has spoken on this himself many times. There's never going to be a China Gorbachev. So they're very defensive about it. They're prepared for it.

Rather strangely, we're not doing this. As far as I know, the U.S. Government is not trying to put a Gorbachev in China and overthrow the CCP, anything from it.

There are several other scenarios. Each scenario, each outcome suggests a different set of measures we should do, but to measure how we're doing in the competition, I propose, has not been done. There's no annual report on how are we doing vis-à-vis, let's say, 20 or 30 indicators with China. So we're working in the dark.

Some professors have worked on this. There's several good books about it. But there's no White House Annual Report on how we're doing in the competition with China, let's say, for 20 or 30 indicators. That's a vacuum that this committee could help to fill. Thank you very much.

[The prepared statement of Mr. Pillsbury follows:]

PREPARED STATEMENT OF MICHAEL PILLSBURY

WEDNESDAY, MARCH 5, 2025

Good morning Chairman Green, Ranking Member Thompson, and Members of the Committee on Homeland Security.

Thank you for the opportunity to be one of your witnesses to comment on the subject of dealing with the China threat to U.S. national security.

I am a fan of this committee's work on China. One vivid example is your February report on the committee website titled "China Threat Snapshot," which provides vot-

ers with a detailed description of Chinese espionage in the last 3 years.[1] The revelation of these details will sicken American patriots. Another example: The committee has been rightly skeptical about the 2025 Annual Homeland Security Threat Assessment, raising questions about how China is described. I would hope that the authors within the Department's 800-person Intelligence and Analysis unit are doing something more about China than the report seems to indicate.

My first recommendation today is that the committee provide focus by developing a list of specific initiatives on China to win the much-discussed strategic competition. There are some good ideas in Senator Tom Cotton's new national No. 1 bestseller, *Seven Things You Can't Say About China.* I would recommend that everyone buy this short book of 30,000 words. I can't resist revealing the seventh point he makes: "China May Win." Now, as Chairman of the Senate Intelligence Committee, Senator Cotton describes a world in which China will "supplant" America as the dominant superpower.[2] This is an important concept that I'll return to. Our new CIA Director, John Ratcliffe, has also committed at his confirmation hearing to focus on the greatest threat: China. In this context, what exactly can the Committee on Homeland Security do? What is its comparative advantage among other committees and with respect to the Executive branch?

Today, there is no shortage of ideas about how to deal with the threat from China. The problem is these ideas are often not relevant, filled with loopholes, or may never be implemented. The challenge we face is that 10 years of complacency may stretch into 10 more years. I served as a co-editor of one of the Heritage Foundation's special reports, *Winning the New Cold War: A Plan for Countering China.*[3] We assembled as many legislative ideas as we could find to deal with the China threat. We found more than 80 and broke them down into 4 categories in our publication. Many of the ideas were proposed by single sponsors and a few co-sponsors, but didn't make it past committee.

China is watching this American inactivity. During my visits to China since my 2015 book, *The Hundred-Year Marathon,* was published, Chinese officials and scholars have pointed out how weak the American Congress has been in dealing with the China threat. Chinese think tanks and professors keep careful track of our China policy. A common Chinese view is that efforts by America's Congress to counter China have been vague and often watered down to mere rhetorical flourishes. Still other legislative proposals just disappeared in conference. Remember that Communist China's experts on American politics usually have American university degrees and read our press carefully. We lack equivalent coverage of China's politics, in part due to massive Chinese secrecy about issues we care the most about.

When I ask Chinese experts on America to score who is ahead, the answer is always "China."

In 2000, the National Defense University published my book on how the Chinese government scores power among nations using complex quantitative formulas. To my surprise, the Chinese translated that book and it was sold in China as *China Debates the Future Security Environment.*[4] I revealed estimates by the PLA and other government sources that China would be equal or surpass America by around 2020—not in terms of GDP, but based on a more complex scoring system called Comprehensive National Power, or CNP. Soon after, China stopped making these forecasts public, although Xi Jinping himself often refers to the concept of CNP.

My recommendation is that we need to score our competition with China like any other game or match, just like how we count football touchdowns. But first, we need to decide what to cover.

The Heritage Foundation's *Winning the New Cold War* did not evaluate through an index of indicators the extent to which we are succeeding or failing in the marathon against China. My speculative scoring (over the last 2 years since it was published) of the 80 legislative initiatives it assembled would be China: 80, America: 0. We would do better if we had concrete indicators showing what we should accomplish over the long term. This would enable legislative initiatives to turn into tangible outcomes which would give us what President Trump called "leverage" in his

---

[1] House Committee on Homeland Representative [sic] Subcommittee on Counterterrorism and Intelligence, "China Threat Snapshot," *https://homeland.house.gov/wp-content/uploads/2025/02/CCP-Threat-UPDATED-Feb-2025.pdf.*

[2] Tom Cotton, *Seven Things You Can't Say About China* (New York: Broadside Books, 2025), 154.

[3] Heritage Foundation, "Winning the New Cold War: A Plan for Countering China," *https://www.heritage.org/sites/default/files/2023-07/SR270.pdf.* See executive summary, 5–15. See also the final chapter by Michael Pillsbury, "The Way Forward," 116–118.

[4] Michael Pillsbury, *China Debates the Future Security Environment* (Washington: National Defense University Press, 2000), *https://nuke.fas.org/guide/china/doctrine/pills2/index.html.*

2015 book.[5] Frankly, we might have to go beyond legislative initiatives, embracing ideas like committee letters to the President or Cabinet Secretaries or a Congressional committee visit to Beijing to convey seriousness and learn the source of Chinese arrogance stemming from their rise, as Xi Jinping repeats in speeches.

Why is this happening? The Heritage Foundation's special report, *Winning the New Cold War,* has highlighted that 1 source of China's success has been its successful lobbying by unregistered agents supported by the CCP who exploit a loophole in the Foreign Agents Registration Act.[6] In the past few weeks, the U.S. Attorney General, Pam Bondi, has been seeking comments on tighter control of Americans acting as agents for China, but the public commentary to Justice seeks to block these crucial improvements. You can see for yourself by going to the DOJ website to read the debate.[7] Foundations and universities who want to be rewarded for their pro-China advocacy fear the shame they would suffer if they had to register publicly as "foreign agents." If the on-line replies to Bondi's effort are any guide, Chinese lobbying operations inside our country will have free rein. After all, the criminal penalty for failure to register is 5 years in prison for each count.

Last month marked the 10-year anniversary of the publication of my book, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower.* In 2015, despite clear indications to the contrary, Washington was only just coming to the realization that China represents an existential, geopolitical threat to the United States. The book thus outlined 12 steps at the end that American policy makers would need to follow to compete in the so-called marathon against China, the long-term race to the position of global superpower that we find ourselves in today.

Ten years after my attempt to alert Washington to the urgency of the 100-year marathon, we have made almost no progress. It might be fruitful for me to walk through each of my 12 steps—which are even more pertinent today—to pinpoint the path that we need to follow in order to make up for our delayed start in the marathon.

I must note the parallel recommendations offered in another best-selling book that appeared 10 years ago called *Great Again: How to Fix Crippled America.* As I alluded to earlier, the author was President Donald J. Trump. Mr. Trump asserted correctly that there are 2 different kinds of Chinas: a good China that built great cities and provided housing and education for millions of people, and a "bad China," the one that "is the one mostly hidden to outsiders."[8] Its government controls internet access, engages in political repression, stifles free expression, arrests dissidents, restricts individual freedoms, and launches cyber attacks.

Mr. Trump was one of the first to identify the long-term China threat to our country. His stark conclusion in 2015 was the same as mine: We've been losing the battle to China for a long time. Trump warned that our economies are tied together in a very negative way. In his assessment, he used the exact same word as I did: "replace," writing that "economists have made predictions that within the next decade, China will replace the United States as the world's largest economy."[9] Then, he raised the subject of this hearing today: "What have we done to beat them?" His answer was "I'll tell you what we've done. We've rolled over."[10] They have "destroyed entire industries by utilizing low wage workers, cost us tens of thousands of jobs, spied on our businesses, stolen our technology, and have manipulated and devalued their currency, which makes selling our goods more expensive—and sometimes, impossible."[11]

Mr. Trump and I had parallel recommendations about the idea of leverage. Trump asked, "So what should we do about it? We're going to use the leverage we have to change the situation so that it favors America and our people. I've negotiated with Chinese companies. I know how they do business."[12]

Mr. Trump's diagnosis was more poignant than my book. He created a sentence I wish I had written which is still valid today: "When dealing with China we need to stand up to them and remind them that it's bad business to take advantage of

---

[5] Donald Trump, *Great Again: How to Fix Our Crippled America* (New York: Threshold Editions, 2015), 45.

[6] Heritage Foundation, "Winning the New Cold War," 7.

[7] "Amending and Clarifying Foreign Agents Registration Act Regulations," *Federal Register,* January 2, 2025, *https://www.federalregister.gov/documents/2025/01/02/2024-30871/amending-and-clarifying-foreign-agents-registration-act-regulations#.*

[8] Trump, *Great Again,* 42.

[9] Trump, *Great Again,* 43.

[10] Trump, *Great Again,* 43.

[11] Trump, *Great Again,* 43.

[12] Trump, *Great Again,* 45.

your best customer."[13] In words that sound like they were only spoken yesterday, Trump wrote, "We should sit down and figure out how to make this a more equitable relationship."[14]

Let's turn to my 12 recommendations, which remind us that we have been addicted to China and that we need to end our dependence and instead use our leverage, as Mr. Trump advised, to get back on track.

The first step I proposed then was the most basic one, and fortunately, perhaps the one where we can say that we have made some limited progress: recognizing that China is a competitor. Even if we have come to a general recognition, there are still strikingly some voices on both sides of the political aisle that hold out naive hopes about Beijing's future. Just recently, Senate Minority Leader Chuck Schumer—who has expressed great concern over Trump's China tariffs [15]—was spotted posing for photos with CCP officials who have spread CCP propaganda and denied allegations about the mistreatment of Uyghurs in China.[16] Although it is frequently repeated in Washington that China presents an existential threat to the United States' geopolitical predominance, words do not equate to actions. Key politicians on both sides of the political aisle are hesitant to take decisive action that would harm their relationship with the CCP.

The second step that I proposed in my book was for Congress to enact an annual reporting requirement of all the assistance flowing from American agencies and departments to China. This has still not happened at a broad, Congressional level. Various agencies have taken it upon themselves to verify whether they are directly or indirectly benefiting China. The Department of Defense's annual reports on military and security developments relating to China [17] and the Commerce Department's tracking of whether key technologies are being transferred to China [18] are 2 examples. But these agency-specific directives fall short of documenting the total financial assistance flowing from American coffers to the Chinese government.

The same pattern repeats itself for my third step. I had suggested that the White House "provide Congress with an annual report that includes trends and forecasts about how the United States is faring relative to its chief rivals."[19] There is still no single, consolidated report that does this, but just like the assistance reporting, some agencies are partially fulfilling this requirement. The ODNI's Annual Threat Assessment, the White House's periodic National Security Strategies, and the U.S.-China Economic and Security Review Commission Annual Report are 3 examples of initiatives that are already under way that could be combined into a single, comprehensive report measuring U.S. competitiveness vis-à-vis China.

This ties in to the next recommendation which I included in the book, which was for the United States to create a competitiveness strategy. Again, we have made significant progress in terms of acknowledging the military, political, technological, and economic threat posed by China in our key defense and intelligence reports, but we are lacking multi-agency documents—somewhat like the IC's National Intelligence Estimate—which regularly outline a strategy for competitiveness that we should follow to beat China in the marathon. We don't quite know what the finish line is, which makes it hard for us to determine what we are competing for. If this were well-articulated in a coherent strategy, it would save a lot of time and dissonance between Federal agencies all adopting their own unique strategies.

The fifth step which I proposed was to find common ground at home. There is admittedly a more broad consensus today compared to 2015 that China represents a critical threat to the U.S.-led world order. That being said, as just mentioned, we are missing a grand strategy as to how we should approach this threat. Nancy Pelosi's 2022 Taiwan visit and the subsequent backlash which this triggered was an example of an American failure in this regard. This episode signaled that we

---

[13] Trump, *Great Again,* 47.

[14] Trump, *Great Again,* 47.

[15] Kevin Scott, "Schumer Melts Down Over Trump's China Tariffs," Knewz, February 24, 2025, *https://www.msn.com/en-us/news/politics/schumer-melts-down-over-trump-s-china-tariffs/ss-AA1zDkGj?ocid=BingHPCNews*.

[16] Andrew Mark Miller , Cameron Cawthorne, "Schumer spotted posing for photo with CCP official as warnings swirl about China influence," Fox News, February 19, 2025, *https://www.foxnews.com/politics/schumer-spotted-posing-photo-ccp-official-warnings-swirl-china-influence*.

[17] U.S. Department of Defense, "Military and Security Developments Involving the People's Republic of China 2024," *https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF*.

[18] U.S. Department of Congress, "U.S. Trade with China," 2022, *https://www.bis.doc.gov/index.php/country-papers/3268-2022-statistical-analysis-of-u-s-trade-with-china/file*.

[19] Michael Pillsbury, *The Hundred-Year Marathon: China's Secret Strategy to Replace America as the Global Superpower* (New York: Henry Holt and Company, 2015), 217.

have 2 divergent China strategies—one provocative and the other conciliatory—which we cannot agree on.[20] In our competitiveness strategy, we need to get both parties and people from private companies, civil society, and Government united behind a single approach as to how we should approach China in the decades to come.

The sixth step I had proposed is one where we are not doing as poorly. I had argued for the necessity of building a vertical coalition of nations. There has been some laudable bipartisanship in terms of U.S. rapprochement to our Asian allies. The United States has spearheaded trilateral cooperation with Japan and Korea, both administrations have reinforced our contributions to the Quad, both have supported the Philippines in the face of Chinese bellicosity in the South China Sea, and our bilateral talks with Indian Prime Minister Narendra Modi have been regular and productive.[21] Secretary of State Marco Rubio's decision to exempt Taiwan and the Philippines from the recent foreign aid freeze demonstrates the Trump administration's willingness to reinforce its coalition of Asian allies to encircle China.[22]

In my seventh step, I had noted our obligation to shine a light on China's political dissidents pushing back against the authoritarian system from which they have fled. I criticized the Obama administration for not including human rights in the 2009 Strategic and Economic Dialogue. Once again, we have failed to be on the side of dissidents exposing China's humanitarian crimes. Admittedly, Trump's 2 administrations took a tough stance against China with regards to the Uyghurs. Former Secretary of State Mike Pompeo systematically highlighted the religious persecution happening in China, which drew responses from human rights organizations in the United States and inspired a series of legislative efforts from several U.S. Federal agencies.[23] Current Secretary of State Marco Rubio recently condemned Thailand for sending Uyghurs back to China.[24] Since then, however, most of that progress has grinded to a halt because of how much Beijing has tightened its security apparatus. The United States will have to continue funding outlets which give dissidents the ability to criticize the regime from afar. This will be discussed more further in my remarks.

The eighth step in the 100-Year Marathon is one that has dominated headlines in the past decade, and often not for the right reason: stemming Beijing's anti-American competitive conduct. The United States has still failed to decouple its military supply chain production from China.[25] Chinese cyber espionage has recently targeted American telecommunications[26] and NATO military systems.[27] Chinese hackers have targeted intellectual property to match the pace of American research—which has become especially concerning as of late in the AI sphere.[28] There is a constant tension between transparency and geopolitical competitiveness in the American system: We have a tendency to make our models open source and to reveal more than we should about the details of our military programs, which allows competitors to replicate our strengths. One need only look at the plagiarism in Chinese military aircraft and ships.[29] Since there is an obligation for Chinese citizens

---

[20] Isaac Chotiner, "The Provocative Politics of Nancy Pelosi's Trip to Taiwan," *The New Yorker,* August 4, 2022, *https://www.newyorker.com/news/q-and-a/the-provocative-politics-of-nancy-pelosis-trip-to-taiwan*.

[21] Derek Grossman, "The State-and Fate-of America's Indo-Pacific Alliances," RAND, November 1, 2024, *https://www.rand.org/pubs/commentary/2024/11/the-state-and-fate-of-americas-indo-pacific-alliances.html*.

[22] Jimmy Quinn, "Rubio Exempts Taiwan and Philippines Security Programs from Aid Freeze," *National Review,* February 23, 2025, *https://www.nationalreview.com/corner/rubio-exempts-taiwan-and-philippines-security-programs-from-aid-freeze/*.

[23] United States Holocaust Museum, "US Responses to China's Crimes Against the Uyghurs," *https://www.ushmm.org/genocide-prevention/countries/china/us-responses-to-chinas-crimes-against-the-uyghurs*.

[24] Michael Martina and David Brunnstrom, "US condemns Thailand's return of 40 Uyghurs to China," Reuters, *https://www.reuters.com/world/asia-pacific/us-condemns-thailands-return-40-uyghurs-china-2025-02-27/*.

[25] Dan Nidess, "Face the facts: America has outsourced its military supply chain to China." *The Hill,* January 17, 2025, *https://thehill.com/opinion/5090860-us-china-trade-war-impact/*.

[26] Amir Daftari, "Major Chinese Cyber Espionage Targeting US Telecom Networks Uncovered by FBI," *Newsweek,* November 14, 2024, *https://www.newsweek.com/fbi-chinese-cyber-espionage-multiple-telecom-networks-1985617*.

[27] Micah McCartney, "China's Spies Hacked NATO Allies Defenses, Official Says," *Newsweek,* February 8, 2024, *https://www.newsweek.com/china-spies-hacked-nato-ally-netherlands-defenses-1868006*.

[28] House of Representatives Committee on Foreign Affairs, "Egregious Cases of Chinese Theft of American Intellectual Property," *https://foreignaffairs.house.gov/wp-content/uploads/2020/02/Egregious-Cases-of-Chinese-Theft-of-American-Intellectual-Property.pdf*.

[29] Alex Hollings, "Counterfeit Air Power: Meet China's Copycat Air Force," *Popular Mechanics,* September 19, 2018, *https://www.popularmechanics.com/military/aviation/g23303922/china-copycat-air-force/*.

abroad to report back to the CCP, States will have to tighten their security to prevent CCP-controlled firms from collecting information on American citizens, buying farmland, and infiltrating American military infrastructure. Arkansas Governor Sarah Huckabee just recently took a stand against this by introducing new legislation to curtail the ability for CCP-operated firms to operate in her State—a move in the right direction.[30]

My ninth step leads us to the topic of pollution. At the time, I had suggested that American public officials emphasize China's failure to uphold climate agreements and unacceptable pollution levels. It is more difficult to make this argument today with regards to electric vehicles, since Beijing strives to have 40 percent of the vehicles sold at home be EVs by 2030.[31] China has also determined that it is in its own interest to refine its early warning systems and launch ozone pollution reduction programs by the end of 2025 to address the smog and air contamination problem it has been facing for several decades.[32] Whether or not it will succeed in this goal remains to be seen. There seems, at least, to be some effort on China's side to reduce pollution and the harm it has done to the planet, though with self-interested goals in mind, of course. If anything is to be learned from the past few years, though, it is that if the United States slows down its industrial production for climate objectives, other countries like China will not necessarily follow suit. Climate agreements, from China's eyes, are only valid so long as they benefit Beijing's national security.

My tenth recommendation revolved around the fight against China's Great Firewall. I commended Wikipedia's battle against Chinese censorship, but encouraged the United States Government to take the company's side and boost activity through Radio Free Asia. Unfortunately, there is little success to report in this regard. Last year, Radio Free Asia shut off all operations in Hong Kong due to fears that it would not comply with a security law.[33] This is understandable, since the families of Radio Free Asia journalists are often at risk, especially if they are of Uyghur descent.[34] But if Washington isn't able to penetrate the Great Firewall through outlets like Radio Free Asia, it should devise a concerted soft power or communications strategy that allows its information to infiltrate into Chinese society. Why is it that an application like TikTok has divided American society while no comparative American app like YouTube is able to convey information to Chinese people? Cracking the code of the Great Firewall will be one of the most pressing challenges for private companies assisting Washington.

Xi Jinping's authoritarian crackdown has made the eleventh step which I outlined excruciatingly difficult. I had suggested that the State Department fund more projects to promote the development of the rule of law and civil society in China. There has, of course, been no progress in this vein since Beijing strictly monitors State Department activities and the flow of money going to local initiatives and elected village officials. This should not prevent the American Embassy in Beijing from coordinating with Americans involved in the educational and private sector in China to provide support encouraging pro-democracy reform (or at least more separation from the CCP) to local institutions, however difficult that might be.

Finally, although Washington has recognized that China poses a threat to our global predominance—as stated at the start of my testimony—we still are dreadfully unfamiliar with the internal debates happening between the so-called "hardliners" and "reformers" in Chinese society. Since Xi runs the country in an authoritarian manner, we assume that China is a monolith, which disincentivizes us from having serious discussions in Washington about the disagreements that divide the CCP regarding China's future. The United States can only follow the strategies previously outlined—such as creating a competitiveness strategy—if we are aware of which faction within the CCP is prevailing at a given time. When the hawks are in power, we can expect a more violent response from China every time we undertake some sort of rapprochement with our Asian allies or rid ourselves of Chinese technology

---

[30] Eric Shawn, "The plan to confront China and kick out companies controlled by the Chinese Communist Party from the U.S.," Fox News, February 26, 2025, *https://www.foxnews.com/politics/plan-confront-china-kick-out-companies-controlled-chinese-communist-party-u-s*.

[31] Jennifer Conrad, "China is Racing to Electrify its Future," *WIRED,* June 29, 2022, *https://www.wired.com/story/china-ev-infrastructure-charging/*.

[32] "China aims to eliminate severe air pollution this year," Reuters, February 25, 2025, *https://www.reuters.com/business/environment/china-aims-eliminate-severe-air-pollution-this-year-2025-02-25/*.

[33] David Pierson, "U.S.-Funded Broadcaster Leaves Hong Kong, Citing Security Law," *The New York Times,* March 29, 2024, *https://www.nytimes.com/2024/03/29/world/asia/hong-kong-security-media.html*.

[34] Jay Nordlinger, "A Uyghur Daughter, and Journalist," *National Review,* May 4, 2021, *https://www.nationalreview.com/2021/05/a-uyghur-daughter-and-journalist/*.

in our military supply chains. Our strategy must be tailored to the internal dynamics within China, or else we risk missing opportunities to be more forward-leaning in our approach when reformers are more prominent in the CCP's leadership.

When we analyze the 12 steps that I proposed in the 100-Year Marathon, it becomes obvious that we have made little progress in the past decade. Yes, it is generally recognized in Washington that China is a threat, but that has translated to little concerted Governmental action. Instead, the way it currently works is that each agency has mechanisms to verify whether the United States is funding China or how Chinese military and economic metrics have changed. There are few oversight methods that unite every agency and create clear indices pointing to whether we are beating China in the 100-Year Marathon. Now that 10 years have passed, it is about time to move from recognition to action, or else we risk being unable to recover from such a slow start.

EXCERPTS FROM THE 12 STEPS IN THE HUNDRED-YEAR MARATHON

It's easy to win a race when you're the only one who knows it has begun. China is thus on its way to supplanting the United States as the global hegemon, creating a different world as a result. Yet it doesn't have to end this way.

STEP 1—RECOGNIZE THE PROBLEM

If America is going to compete in the Marathon, its thinking about China must change radically. This means recognizing that China is a competitor, not a welfare case.

STEP 2—KEEP TRACK OF YOUR GIFTS

Every year, a small fortune of American tax dollars is being spent to aid China's rise. Most of this aid is kept low-profile, unnoticed by the media and the public. This is done intentionally.

Labor Department experts who the U.S. Government had sent to China to boost Chinese productivity . . . the Treasury Department and the comptroller of the currency offered China to improve its banking practices . . . the Federal Aviation Administration's assistance to Chinese aircraft manufacturers . . . other U.S. Government agencies have facilitated hundreds of science assistance programs in China.

There is still no available accounting of all the activities funded by the U.S. Government to aid China. Not only is America funding its own chief opponent; it doesn't even keep track of how much is being spent to do it.

To compete in the marathon, Congress should enact an annual reporting requirement of all agencies and departments of their assistance to China. If such programs were identified and publicized, 3 beneficial results would follow.

STEP 3—MEASURE COMPETITIVENESS

Many of the warring states stories involve carefully measuring the balance of power before strategies are chosen. It is a classic American business principle that "What you measure improves." The lesson is simple but profound: You can't improve unless you know what you need to improve. You can't come from behind in a race against your competitors unless you know the respects in which you have fallen behind. Every year, the Chinese create an annual analysis of their competitiveness relative to the United States. Why isn't America doing the same thing?

The U.S. Government should be conducting a similar—but more robust—measure of American competitiveness. The White House should provide Congress with an annual report that includes trends and forecasts about how the United States is faring relative to its chief rivals. Many departments of the U.S. Government, including the intelligence community, would have to be involved. It need not cover all other nations, just the top 10—beginning with China.

STEP 4—DEVELOP A COMPETITIVENESS STRATEGY

Stratagems of the warring states frequently describes how leaders compete by adopting "reforms" to grow their power more rapidly than their competition. The point was to be open-minded enough to recognize and act when one's strategy needed to change, and then impose new tactics to achieve one's desired result.

The public policy analysts Robert Atkinson and Stephen Ezell have proposed a multiagency program to enhance American competitiveness, but they fear that it will be hampered or eliminated because of partisan political considerations.

STEP 5—FIND COMMON GROUND AT HOME

Warring states leaders tried to keep their allies closely aligned and built ever-shifting coalitions united behind a common goal. Disunity was dangerous. There are many advocates for reforming American policy toward China—inside and outside of the U.S. Government—but they are fractured into factions that often do not see each other as allies. Since at least 1995, Chinese scholars in Beijing have delighted in telling me stories of how Americans who criticize U.S. policy toward China are so divided by their political differences that they never cooperate.

STEP 6—BUILD A VERTICAL COALITION OF NATIONS

There is a reason why China has been expanding its South China Sea claims, bullying Philippine fishing boats, cutting the cables of Vietnamese seismic survey ships, and recently establishing an Air Defense Identification Zone in the East China Sea. China wants to guarantee access to a wealth of natural resources in the region and is hoping to intimidate its neighbors so they are too scared of China to unite and oppose its ambitions.

Whether you play wei qi or not, you know that encirclement by a group of adversaries is dangerous. China's natural fear is that its neighbors will form such an alliance. That's exactly what the United States should be encouraging with nations including Mongolia, South Korea, Japan, and the Philippines. Even the threat of such a coalition—through movements in that direction—might give Beijing pause and temper its bellicosity. China knows how America and its allies contained the Soviet Union. As the United States increases aid and facilitates cooperation among China's neighbors, China's hawks will get the blame when China feels isolated and alone in the region.

STEP 7—PROTECT THE POLITICAL DISSIDENTS

Many of the soldiers on the front line of the Cold War were Soviet and Eastern European dissidents who refused to surrender to an unending future of censorship, propaganda, religious persecution, and economic enslavement. Their field marshals were men such as Václav Havel, Lech Wałęsa, and Aleksandr Solzhenitsyn. And with their courage and passion and principles, they brought down the Soviet Union and the Iron Curtain. But they didn't do it alone. Presidents from Truman to Reagan championed their cause. When they were imprisoned, American Presidents demanded their release. When they needed money, Americans sent them funds. When they needed a platform for the free speech their regimes denied them, Americans shared their printing presses and broadcast their battles and beliefs into millions of homes through Radio Free Europe.

Today China has increased its persecution of Buddhist Tibetans and Muslim Uighurs. In Tibet, the government has imposed curfews, arrested protesters, killed innocent civilians, and transformed the region into, in the recent words of the Dalai Lama, a "hell on earth." In Xinjiang, the internet and phones are routinely shut off, and the percentage of Han Chinese in Tibet and Xinjiang has risen dramatically due to state-sponsored migration.

China also persecutes Christians. It is a common practice in China for foreigners to show their passports before being allowed to attend a church service in China. Why? Because China is ruled by the atheistic Communist Party, and its government wants to keep Chinese nationals out of non-state-run churches. Many experts estimate that there are 60 million to 100 million Christians in China and that the number is growing. Bob Fu, the founder and president of China Aid, seeks to equip the Chinese people to defend their faith and freedom. The organization's purpose is to promote legal reforms, fund "house churches" in China, and assist imprisoned Christians.

STEP 8—STAND UP TO ANTI-AMERICAN COMPETITIVE CONDUCT

China is not just a source of cyber spying against the United States; it is the primary source. According to some estimates, more than 90 percent of cyber espionage incidents against America originate in China.[14] Chinese hackers regularly infiltrate American businesses and Government entities. An abridged list of victims includes Google, Booz Allen Hamilton, AT&T, the U.S. Chamber of Commerce, Visa, MasterCard, and the Departments of Defense, State, Homeland Security, and Energy. Hacking is central to China's decades-long campaign to steal technologies it can't invent and intellectual property it can't create. A report by the Commission on the Theft of American Intellectual Property, led by the former Director of National Intelligence Dennis Blair and by the former U.S. Ambassador to China Jon

Huntsman, found that the theft of U.S. intellectual property likely costs the American economy more than $300 billion per year.[15]

STEP 9—IDENTIFY AND SHAME POLLUTERS

One of the more effective approaches to protecting the environment with regard to China occurred when Ambassador Huntsman authorized the U.S. embassy in Beijing to tweet the pollution levels in Beijing.[18] Similarly, Ma Jun the director of the Institute of Public and Environmental Affairs, a leading environmental watchdog organization in China, has compiled on-line maps of China's water, air, and solid waste pollution.

But is fostering greater awareness the best we can do? The United States needs to go from asking China to act in an environmentally responsible way to insisting that China do so, even if that means using far more leverage than past administrations have been willing to exert. Otherwise, China will be at a competitive economic advantage—with Washington constraining American businesses in an effort to protect the environment while China goes right on exporting its products and its pollutants at breakneck speed.

STEP 10—EXPOSE CORRUPTION AND CENSORSHIP

One of the Chinese government's greatest fears is of a free press. It knows that sunlight is a disinfectant for wrongdoing, and it is terrified of what its people would do if they knew the whole truth about Chinese leaders' corruption, brutality, and history of lying about the United States and our democratic allies. Yet it remains a mystery why the United States doesn't do more to fight China's censorship and propaganda campaigns against the Chinese people.

But the government in Beijing uses its various tools to prohibit such information from reaching the Chinese people. In 2012 the Chinese government blocked Bloomberg News after it published a story on the family wealth of Xi Jinping. The implicit deal of working in China seems to be this: you may report on China's fantastic growth, but if you start criticizing the Communist Party or its top officials you will be kicked out of the country.

During the Cold War, Radio Free Europe was an oasis for anti-Communist dissidents in a desert of Soviet censorship and propaganda. There's no reason why Radio Free Asia couldn't serve a similar purpose in the Hundred-Year Marathon, but its budget needs to be increased at least 3-fold.

STEP 11—SUPPORT PRO-DEMOCRACY REFORMERS

China's concern when it talks about a new Cold War is that the Americans will revive their Cold War-era programs that helped to subvert the Soviet Union from within by using the power of ideas. Most Chinese hawks believe that this plan to subvert Chinese democracy has already been put into motion, much as it was for the Soviet Union in 1947. At least 2 Chinese books claim the CIA leads it.

Former Secretary of Defense Robert Gates has noted that the 1975 Helsinki Accords galvanized pro-democracy groups inside the Soviet Union and played "a key role in our winning the Cold War." His view seems to be shared by the hawks of China, who write often about their fear that the United States has mounted a program to influence impressionable future civilian Chinese leaders to move toward democratic multi-party elections and a free market.[30] In October 2013, China's hawks revealed another fear—that America is seeking out a Chinese Gorbachev-like figure, a leader who will bring 1-party rule to an end. The hawks' distrust of China's own leaders is shown in the tone of a 90-minute video released in October 2013 called Silent Contest.[31] China's hawks fear their civilian leaders are susceptible to influence from Western leaders who want to see multi-party rule and an evolution toward democracy.

The truth is that there is no such concerted effort by the United States or the West to subvert China's Communist Party rule. The annual spending on programs to support democracy in China is less than $50 million.[33] While the U.S. Government has some underfunded civil society programs, they are not CIA covert actions, and they are small in scale compared to what will be needed. There are at least 6 such programs, originating during the Cold War and run by various American organizations with U.S. Government funds, including the AFL–CIO, the Chamber of Commerce, and both major U.S. political parties. They provide funding for a wide range of Chinese organizations inside China as well as for exile groups.[34]

STEP 12—MONITOR AND INFLUENCE THE DEBATES BETWEEN CHINA'S HAWKS AND REFORMERS

Today, as China pursues its own Cold War strategy against America, it monitors carefully various factions in Washington, DC—those who are supporters of Beijing and those who are skeptics, those who can be manipulated and those who have caught on to the marathon strategy. America used to be good at this, too. During the Cold War, the United States invested time, technology, and personnel into discerning the activities among various members of the Soviet Politburo—those who advocated a more harmonious relationship with America and those who viewed the United States as a dangerous rival that must be overtaken. Yet unlike our activities against the Soviets, America is far behind when it comes to China.

It is crucial that the United States possess an understanding of the various actors in Beijing's sensitive internal debates. Though the marathon strategy is moving apace, the Chinese government is not monolithic in its thinking. Hard-liners are certainly in the majority, but on the margins there are still sincere advocates of reform and liberalization who want a China that moves closer to an American-style model. They exist, and they must be identified and supported. The problem is that the U.S. intelligence community has not invested in the resources to determine who those true reformers are—as differentiated from the many Chinese leaders who make misleading reformist claims. This remains a massive intelligence challenge.

James Lilley, a former U.S. Ambassador to China and a 27-year veteran of the CIA testified in August 2001, 12 years after the Tiananmen Square massacre. Lilley told a Congressional commission that his greatest regret was learning a decade too late about internal Chinese documents revealing just how far China had moved toward democracy and how close the protests came to removing the Communist government. If only he had known at the time, the former Ambassador said, he would have urged President George H. W. Bush to intervene firmly on the side of the real reformers, rather than being deceived by Beijing's leadership into siding with it.

Mr. GUEST. Thank you, Dr. Pillsbury.

I now recognize Mr. Evanina for 5 minutes to summarize his opening statement.

STATEMENT OF WILLIAM R. EVANINA, FOUNDER AND CHIEF EXECUTIVE OFFICER, THE EVANINA GROUP

Mr. EVANINA. Acting Chairman Guest, Ranking Member Thompson, Members of the committee, it's an honor to be here today with my esteemed guests.

September 11, 2001, our Nation was attacked by committed terrorists. As a Nation, we were not prepared for this attack or how it would impact every aspect of American life for decades to come.

As a special agent in the FBI that day, I was part of the investigation of Flight 93. On that day and throughout my entire law enforcement and intelligence career, I often ask myself, "How did we not see this coming?"

Maybe we could've prevented it. We saw the lights blinking. As a Nation, we worked tirelessly for 25 years to prevent that from happening again. We were committed.

Today, our Nation faces an array of sophisticated diverse threats by terror organizations, cyber criminals, and nation-state threat actors. I proffer to you, the greatest threat to our Nation emanates from the Communist Party of China.

This threat is existential. It is complex, pernicious, and strategic with the U.S. private sector and academia the main battlefield. Xi Jinping drives a comprehensive and whole-of-country approach to the CCP's efforts to invest, leverage, infiltrate, paralyze, influence, and steal from every aspect and every corner of America.

As this committee is aware, the economic loss of theft of intellectual property and trade secrets, just from the Communist Party of China, is estimated between $300 billion and $600 billion per year.

To make that more relevant to everyone in this room, as the acting Chairman mentioned, it's about $4,000 to $6,000 per year per American family of 4 after taxes.

Additionally, it's estimated that 80 percent of all Americans have had all of their personal data stolen by the Communist Party of China in the past decade. The other 20 percent, just most of it.

Data has become the new goal in the world. The CCP's priorities to collect it are second-to-none like we've ever seen. As we all know, data is the bedrock, fundamental purpose for all artificial intelligence creation.

Layering on to our economic hemorrhaging is the unprecedented Volt and Salt Typhoon hacks which continue to persist in our critical infrastructure and telecommunications sectors respectively.

The CCP's recent actions also include sophisticated surveillance balloons, technical surveillance stations in Cuba, maritime port control, strategic land purchases near military bases, fentanyl, TikTok, malign foreign influence at the local level, et cetera.

Altogether, the collage begins to paint a bleak picture far beyond blinking red. Our current domestic vulnerability is unacceptable. The blinking lights are clear.

I believe we must approach this existential threat with the same sense of urgency, leadership, spending, and strategy, as we have done for the past 2 decades in defeating and preventing terrorism.

I would ask this committee, is it not a terrorism when our electrical grid or natural gas pipeline is disabled or damaged via Volt Typhoon malware? That will result in millions of households, hospitals, and buildings being without heat or electricity.

What about when our telecommunications infrastructure, to include Verizon, AT&T, T-Mobile, are all being disabled on the same day due to an organized cyber attack precipitated by Salt Typhoon?

If our financial services sector was impacted and had to go offline just for a few hours, it would cause immeasurable harm, as well as significant domestic and international chaos, societal panic, and disruption we have not seen since 9/11.

Are these not terrorism-type events? If these events incidentally occur on the same day as the CCP makes their inevitable move on Taiwan, are we even ready as a Nation to handle the paralysis and chaos the CCP will cause from every aspect of our American life in commerce, health, safety, and the way we live every day?

The CCP has strategically planned and implemented the ability to do just this, all at once, and all across our homeland, from our ports to our electrical grid.

Additionally, every aspect of these actions has a planned impact on societal chaos and panic; it is an integral part of the CCP's plan and strategy.

Hence, "terrorism" and "terror" must be redefined beyond our framework where we historically look at kinetic actions that harmed or killed our loved ones. The inability or unwillingness to look behind this curtain and visualize this clear, realistic scenario is no longer an option for anyone.

In fact, the proverbial curtain no longer exists. Our Nation needs strategic leadership now more than ever. Time is of the essence.

Additionally, this will take a whole-of-country approach. This approach starts here with the U.S. Congress. We all see the blinking

lights clearly. I offer a nationwide call to action, committing to reduce the brightness, reduce the cadence of these very clear and blinking lights.

Thank you for the opportunity to be here, and I look forward to your questions.

[The prepared statement of Mr. Evanina follows:]

PREPARED STATEMENT OF WILLIAM R. EVANINA

MARCH 5, 2025

Chairman Green, Ranking Member Thompson, and Members of the committee—it's an honor to appear before you today.

I have spent 32 years working in the U.S. Government, 24 of which as a special agent with the FBI, and as chief of counterespionage at the CIA.

I was tremendously honored to serve as the first Senate-confirmed director of the National Counterintelligence and Security Center (NCSC) in May 2020, leading our Nation's counterintelligence and security efforts. I served in that role since 2014.

I am here before you today as the CEO of The Evanina Group, LLC. In this role, I work closely with CEOs, boards of directors, and academic institutions, and senior executives of the U.S. Government to provide a strategic approach to mitigating corporate risk in a complicated global environment.

A DOMESTIC THREAT LANDSCAPE OVERVIEW

EXISTENTIAL THREAT

Our Nation continues to face an array of diverse, complex, sophisticated, and unprecedented threats by nation-state actors, cyber criminals, and terrorist organizations.

Unquestionably, the existential threat our Nation emanates from the Communist Party of China (CCP). This comprehensive threat posed by the CCP is the most complex, pernicious, strategic, and aggressive threat our Nation has ever faced. It is an existential threat to every fabric of our great Nation. Now, more than ever, the private sector and academia have become the modern battlefield for which Xi's holistic efforts manifest.

Xi Jinping has one overarching goal to be the geopolitical, military, and economic leader in the world. Xi, along with China's Ministry of State Security (MSS), People's Liberation Army (PLA), and the United Front Work Department (UFWD), drive a comprehensive and whole-of-country approach to their efforts to invest, leverage, infiltrate, influence, and steal from every corner of the United States. This is a generational battle for Xi and China's Communist Party (CCP), it drives their every decision.

REAL COSTS OF ECONOMIC LOSS

The estimated economic loss from the theft of intellectual property and trade secrets, just from the CCP, and just from known and identified efforts, is estimated between $300 billion and $600 billion per year (Office of the U.S. Trade Representative and Federal Bureau of Investigation).

To make it personal for you and your constituents, this theft equates to approximately $4,000 to $6,000 per year, per American family of 4 . . . after taxes.

China's ability to holistically obtain our intellectual property and trade secrets via illegal, legal, and sophisticated hybrid methods is like nothing we have ever witnessed. Actually, it is said by many to be the largest theft of intellectual property in the history of the world . . . and it has happened just in the past decade.

Additionally, it is estimated that 80 percent of American adults have had all of their personal data stolen by the CCP, and the other 20 percent has had most of their personal data stolen. For Xi, the overarching vison is how to counter, compete, and push past the United States is goal No. 1.

TERRORISM REDEFINED

Congress, and the entire American democratic and capitalistic ecosystems, must first clearly understand Xi's reprehensible intentions in order to effectively mitigate the accompanying threat with our own whole-of-society approach.

We must approach this existential threat with the same sense of urgency, spending, and strategy, as we have done for the past 24 years in preventing terrorism in our homeland.

To set the perspective, a simple definition of terrorism is "the use of threats or violence to achieve political or ideological goals."

I would offer to this committee that we are in a terrorism event. A slow, methodical, strategic, persistent, and enduring event which requires an increased degree of urgency of both Government and corporate action. It is clear that under Xi Jinping, the CCP's economic war with the United States has manifested itself into a clear terrorism type of framework.

Let me be more specific. The CCP's capabilities and intent are second to none as an adversary. Cyber breaches, insider threats, surveillance and penetrations into our critical infrastructure have all been widely reported. Adding in the CCP's crippling stranglehold on so many aspects of our supply chain and the result is a montage of domestic vulnerability of unacceptable proportions.

Recent nefarious and disturbing areas of the CCP's actions include VOLT and SALT TYPHOON, surveillance balloons, technical surveillance stations in Cuba, maritime cranes, Huawei, TikTok, strategic land purchases near military and strategic locations, influence at the State and local level, etc. When overlapped, the collage begins to paint a bleak mosaic which is beyond the blinking red metaphor. It is imperative to understand that the CCP maintains civil unrest and societal chaos as a primary pillar in any nefarious cyber penetration or attack.

EVERYTHING EVERYWHERE ALL AT ONCE

I would ask this committee: Is it not terrorism when our electrical grid or a natural gas pipeline is disabled via VOLT TYPHOON in a part of the United States, resulting in millions of households, schools, hospitals, and buildings being without heat or electricity? What about when our telecommunications infrastructure (e.g., Verizon, AT&T, and T-Mobile) being disabled on the same day due an organized cyber attack, precipitated by SALT TYPHOON? And if our financial services sector was impacted and had to go off-line, for even a few hours, it would cause significant domestic and international chaos, societal panic, and disruption.

Are these not terror-type events? If these events coincidently occur as the CCP makes their inevitable move on Taiwan, will the American people, and U.S. policy makers for that matter, have the sufficient appetite to actually defend Taiwan?

The CCP has strategically planned and implemented the ability to do just this, all at once, and all across our homeland. Hence, "terror" must be redefined beyond our framework which historically includes loved ones being injured or killed from a kinetic event.

The inability or unwillingness to look behind the curtain and visualize this clear and realistic scenario is no longer an option for anyone, especially the Congress, the administration, U.S. Governmental entities, academic institutions, and especially the private sector. In fact, the proverbial curtain to look behind no longer exists. We must immediately end the process of being victims to the CCP's actions.

SALT TYPHOON

The largest telecommunications hack, in the world, occurred in 2024. It occurred here, in the United States, by CCP-backed hackers, against the top 9 U.S.-based telecommunications carriers and hardware providers. The size and scope of this brazen hack has not yet been determined and will take extensive time to do so. This successful hack by the CCP provided comprehensive call and text data of subscribers, geolocation of the subscribers, and ability to listen to telephone conversations as they deemed interested. Per public reporting, the intent of the breach was to obtain court-ordered warrant data issued to the carriers by the U.S. Government on Chinese targets. Similar to the OPM breach, the CCP succeeded beyond their dreams and intentions. It is much worse than that, but that is for a closed session with your U.S. Government agencies.

As an intelligence and law enforcement professional, I am beyond concerned with this access for all the obvious intelligence and counterintelligence-gathering aspects. Additionally, the thought that a foreign adversary and competitor can access metadata call information and listen to conversations, is beyond astonishing, and very disheartening. As Members of this committee are fully aware, for this to happen here, legally in the United States, a FISA or Title 3 court order, signed by a U.S. Magistrate Judge or FISA Court would be required.

FENTANYL

Let us take a look at the fentanyl epidemic. Members of this Committee are very familiar with the epidemic and the numbers. But it is important to revisit and place into comparison perspective. Thankfully we have recently seen a significant reduction in deaths caused by fentanyl overdoses. However, with over 200 Americans dying of fentanyl overdose every day (107k+ in '23), China's effect is analogous to a Boeing 737 aircraft crashing, every day, and killing everyone on board. The fentanyl epidemic is delivering the same casualty rate within the United States as Germany and Japan delivered to American soldiers in World War II. Currently,

fentanyl overdoses per day are 50 percent greater than the World War I Killed-in-Action per day count. Let that sink in. And as Members of this committee are already aware, most of the fentanyl precursors are manufactured in China. The fentanyl epidemic starts, and ends, with the CCP.

MARITIME PORTS

Specific adversaries (Russia/China) have been historically creative in embedding intelligence collection capabilities into products which have a legitimate use in business, commerce, technology, or operating systems (see Kaspersky Labs). The CCP has taken this concept to increasingly strategic, and potentially paralyzing levels.

The new frontier, in my opinion, is the legitimate procurement by U.S. port terminals of Chinese-manufactured (Shanghai Shenhua Heavy Industries Company, Limited) ZPMC crane systems.

ZPMC is a subsidiary of China Communications Construction Company (CCCC). CCCC is a prominent contractor for the Peoples Liberation Army and Navy. Members of the committee are aware that it is currently estimated that approximately 80 percent of all of the ship-to-shore goods and services entering, and exiting, the United States are offloaded/loaded via Chinese-owned ZPMC crane systems. Additionally, these same ZPMC crane systems are used by the U.S. military to commission our Naval and Coast Guard vessels at numerous strategic ports.

ZPMC cranes offer the CCP a dual-use capability for intelligence collection (cameras, sensors, tracking technology, connected software) in U.S. ports servicing heavy commercial activity as well as U.S. military bases. The ZPMC crane systems provide a supply chain vulnerability of potentially paralyzing proportions. There is interconnectivity among all the ZPMC crane systems nationwide, and shared Chinese-developed software and labor. ZPMC, if ordered by the CCP, can immediately shut down maritime port operations throughout the United States in a time of conflict or to utilize a future economic lever.

Additionally, other elements of the product transportation supply chain are also required to enter into these contracts, including data-sharing agreements, and software collaboration while working at a U.S. maritime port ecosystem in order to interface with ZPMC cranes and technology.

When the ZPMC crane system threat is stacked onto the VOLT TYPHOON cyber malware penetration, the CCP will be able to systematically, and without delay, cause instant havoc in almost every aspect of American daily operations, commerce, and safety, and at the same time instill a level of societal and business panic not seen since September 1, 2001.

In my professional opinion, and from a civilian and military perspective, this might be the CCP's most strategic operational endeavor against the United States thus far, outdistancing Huawei. We cannot allow it to be their most successful.

INSIDER THREAT

The insider threat problem, originating from the CCP, has been nothing short of devastating to the U.S. corporate world, academic institutions, and research and development organizations in the past decade, plus. The Department of Justice's web site's catalog of economic espionage indictments and convictions is staggering. The result is hard to swallow and quantify. And those listed cases only represent what was identified, reported by a U.S. company, and then prosecuted.

We need to continually highlight this issue as a key facilitator for the CCP's strategic endeavors to steal intellectual property and trade secrets, especially those developed before they are classified by the U.S. Government, as well as the CCP's strategic placement for human-enabled cyber operations.

Corporate America and academia must make significant efforts to identify and mitigate insider threats to their organizations seeking to steal and/or do harm. It starts with a more substantive vetting process of applicants and incorporation of an insider threat or employee wellness program. It is too costly not to. The impacts ripple far beyond the victim company.

HOW DOES THE THREAT MANIFEST?

Intelligence services, joint ventures, science and technology investments, academic collaboration, research partnerships, front companies, mergers and acquisitions, and outright theft via insiders and cyber intrusions, initiate the comprehensive and strategic framework for how China implements their strategy.

China continues to successfully utilize "non-traditional" collectors to conduct a plurality of their nefarious efforts here in the United States due to their successful ability to hide in plain sight. The non-traditional collectors, serving as engineers, businesspersons, academics, IT professionals, and students, are shrouded in legitimate work and research. Oftentimes, the "non-traditional" collector becomes an unwitting tool for the CCP and its intelligence collection apparatus.

China's ability to holistically obtain our Intellectual Property (IP) and Trade Secrets via illegal, legal, and sophisticated hybrid methods is beyond demoralizing. Joint ventures, creative investments into our Federal, State, and local pension programs, collaborative academic engagements, Sister City Programs, Confucius Institutes, and similar programs on university campuses, talent recruitment programs, investments in emerging technologies, and utilization of front companies, continue to be the framework for strategically acquiring the thoughts and ideas of our researchers, as well as development of those ideas pre- and post-patent application.

ACADEMIA A LEADING TARGET

The threat posed by China to U.S academia, as well as research institutions (including Federal), is deep, pervasive, and decades-long. The past decade of indictments and prosecutions have highlighted the insidiousness of China's approach to obtaining early and advanced scientific research and data.

Additionally, China has expertly learned and manipulated the complexity and shrouding of gifts and funding at U.S. colleges and universities, particularly when tied to Federal grants. On-going academic partnerships by U.S. universities with CCP cultural programs (Confucius Institutes) and CCP-funded research institutions is increasingly problematic, and one-sided.

For example, the University of Michigan, and other universities, recently severed ties with China's Shanghai Jiao Tong University (SJTU). SJTU has historically been tied to the CCP's intelligence and cyber hacking programs. The University of Michigan's brave and bold decision was only possible after the university was provided briefings, intelligence, and data as to the nefarious history and activities of SJTU by this Congress, and the FBI.

Universities need to be sufficiently advised of on-going threats and risk in order to make sound risk-based decisions on said partnerships. Additionally, universities who continue to engage in these CCP partnerships with known nefarious activities need to be held accountable for such relationships.

There is a clear void in this problem set which requires immediate fixing. The U.S. Government, specifically the FBI, NSA, DHS, and others, must be forward-leaning in dissemination of known threat intelligence to academia and research institutions. Such effort is critical to enable immediate and strategic risk-based mitigation decisions to protect not only ideation and trusted development of intellectual property, but also individual university brands.

This is increasingly important as we are in a high-speed technology race with China and cannot afford for China's continuance of easy theft and hence, not earning their place in this critical 21st Century competition for technology dominance. I address this further in my recommendations.

ACADEMIC DUE DILIGENCE AND COMPLIANCE

U.S. academic and research institutes must engage in rigorous due diligence and compliance programs. I spend a considerable amount of business with academic institutions advising and informing them on due diligence and compliance efforts to identify and mitigate potential areas of concern with foreign students, professors, and researchers. Recently, an executive of a very prestigious U.S. university stated: "I assumed the Department of State vetted these students prior to coming on campus. What do you want us to do?" This assumption, and related question, is very common and very problematic.

The United States possesses the greatest catalog of academic and research institutions and entities the world has ever seen. The United States continues to not only be the leaders in the world, but with such, we attract the best and brightest from around the world. The collaborative nature of academia is primary to its success; however, it is also its greatest vulnerability.

Vetting of foreign national students, faculty and research, if it occurs, is nascent at best, and in just a few institutions. The dilemma and complexity I hear from institutions is understandable. However, we can no longer continue to allow the CCP to obtain the ideation, hard work, research, and patent-ready results, from U.S. academic and research institutions without any effort to defend such.

This situation is also similar to U.S. Government entities such as the National Institute of Health, National Science Foundation, Department of Energy, National Labs, and so many others. To ensure security of our hard work and related product, compliance and due diligence must be a priority if we have any chance at slowing down the CCP from obtaining classified, and unclassified, research with minimal difficulty.

INDUSTRIES LEADING AS TARGETS

China's key priorities for obtaining U.S.-based technology and know-how, pursuant to their publicly-available "Made in China 25 Plan" are Aerospace, Deep Sea

Technology, Biotechnology, Information Technology, Advanced Manufacturing, Clean Energy, Electric Battery Technology, and DNA/Genomics.

Any CEO or board of directors engaged in any of these critical industries, and within the vertical supply chain, must understand the threat posed to them and work to identify risk-based mitigation strategies. This is a zero-sum game.

"Military-Civil Fusion" is undoubtably a strategy employed by the CCP to drive Xi's movement to global technological and military dominance. However, it is too often viewed through a Western-based filter and related bias. In China, there is no fusion of military and civilian efforts. They are ONE, working together, and in unison. Unlike the U.S.- and other Western-based democratic nations, there does not exist a bifurcation between government, military, and the private sector. I would even include the education ecosystem in this mosaic. There is one China. Xi's China. Everything, and everyone, works toward a common goal in China, which is the betterment of China.

Additionally, the People's Liberation Army (PLA) and Ministry of State Security (MSS) have never been so collaboratively intertwined with respect to common goals and aggressiveness of action as they have been the past 5 to 10 years. If the PLA needs a specific technology for military capability to copy or reverse engineer, the MSS will acquire it through any means necessary and will employ every legal, and illegal, tool as referenced earlier, in obtaining the necessary technology.

CHINA DOES NOT PLAY BY ANY RULES

China plays by their own rules, only. China does not conform to any international or normalized set of regulations, guidelines, norms, laws, or value-based agreements throughout the global economic ecosystem.

To further the CCP's unlevel economic playing field, out of the 15 largest companies inside China, 13 are either owned by the CCP, or run by the CCP. The world has seen recently what the CCP is capable of when one of the largest companies in the world, Alibaba, pushes back on state-run efforts. Additionally, many of the CCP's largest corporate leaders and CEO's have gone missing.

Boards of directors and investment leaders must begin to think strategically about what the long-term threat impact the CCP presents and how their investments, decisions, and unawareness of the long-term threat impact their respective businesses and industries. This threat is woven with our national security, economic stability, and endurance of our republic. As a Nation, and if we truly want to compete with China, we must move toward a more intertwined risk-based intelligence sharing effort between the U.S. Government, corporate America, and academic institutions.

CHINA'S NEED TO KNOW LAWS

In 2017, the Communist Party of China issued new state laws to facilitate the perniciousness of their efforts to obtain data, from everywhere, and in any way. Three specific portions of these laws should be understood, and be an enduring reminder to CEOs, general counsels, chief data officers, CIOs, CSOs, and CISOs, throughout our private-sector ecosystems.

The first is Article 7 of the People's Republic of China National Intelligence Law summarily stating that all business and citizens shall cooperate with China's intelligence services and shall protect all national work secrets.

The second is Article 77 of the same National Security Law summarily stating that Chinese citizens and business shall provide anything required or requested by the Chinese government or intelligence services.

The third is Article 28 of the 2016 Cybersecurity Law summarily stating that all network operators must provide data to, and anything requested by, national, military, or public security authorities.

These laws carry with every Chinese citizen whether they reside in Beijing, or anywhere else in the world, regardless of their employer. Hence, a Chinese national working at a U.S. company is always at risk for answering to the CCP's data collection apparatus.

YOUR DATA IS CHINA'S DATA

As a cautionary tale, if you are a U.S. business seeking to enter a business relationship with a company in, or from, China, your data will be obtained and provided to the MSS or PLA for their usage, without exception. This includes any third-party data as well. The analogy is a U.S.-based company entered into a business deal or partnership with a company from another country. In order to do business, the U.S. company would be required to provide all relevant and requested data from their company, as well as the partner company, to their customer agency, such as the NSA, CIA, and FBI. To reiterate, the operational and legal tempo of the CCP is difficult to visualize and understand while looking through Western and democratic

lenses. There is no bifurcation between the CCP and corporate ecosystem. It is one China.

MALIGN INFLUENCE

Malign foreign influence has increased dramatically in the United States in the past decade. Russia, China, and others have been very active in this activity and with varying degrees of success. Measuring such activity has proven to be not a perfect science.

China is strategic and precise as they successfully influence at the State and local levels of the United States. I want to briefly touch on a few key areas.

The first is economic investment. Chinese investments in key industries such as real estate, agriculture, advanced manufacturing, and technology have raised significant concerns. These partnerships often take the form of "Sister City Programs but can also be business partnerships between a city or small town and a CCP-owned or -controlled company. Investments in U.S. critical infrastructure at the local level is also on the rise which creates an entire separate category of concern.

The CCP takes advantage of small towns and cities increasing need for economic solicitation of funds. CCP partnerships with Economic Development professionals provides the most immediate and impactful results. The town, or city, receive immediate investment and the CCP obtains a foothold, access, or future opportunity for strategic purposes. Local Economic Development professionals have no idea of the ultimate purpose or intent of such a partnership.

Political donations and lobbying are another serious concern. The CCP's strategic approach to identify current, and future, political leaders and elected officials and invest in their future continues to be problematic. The investment can take form in direct financial support to a campaign, lobbying, or placing CCP loyalists into the inner circle of an elected official to influence decision making to benefit CCP interests or individuals supporting CCP efforts.

The most common initial step is the official invite of a newly-elected Federal, State, or local official for an all-expense paid trip to China with family and friends where the CCP will offer investments and inexpensive solutions to the elected official's economic challenges. As well, the CCP will gain access to the elected official's mobile devices.

The obvious and immediate need is to have a platform where State and local (and even Federal) elected officials can receive substantive training and awareness of how these issues manifest in their State, city, or township.

THE NEED FOR STRATEGIC LEADERSHIP

In closing, I would like to thank this committee for acknowledging the significant threat posed by China by holding this hearing. Continuing to drive awareness, and more importantly, combat the threat posed by the CCP will take a whole-of-nation approach with a mutual-fund-type long-term commitment. Such an approach must start with robust and contextual awareness campaigns, like this committee holding this hearing. The WHY matters.

Regarding these awareness campaigns, we must be specific and reach a broad audience, from State and local governments to academia, from board rooms to business schools, educating on how China's actions impair our competition by obtaining our research and development, trade secrets and intellectual property, and degrading our ability to maintain our role as economic global leaders.

Our Nation needs strategic leadership now more than ever, particularly when we face such an existential threat from a capable competitor who is looking beyond competition to global dominance. We have to catch up, mitigate, and inflict costs on China in an expedited fashion. Doing such will entail strategic leadership leading a whole-of-society approach is imperative.

Last, I would like to state for the record the significant national security threat we face from the Communist Party of China is NOT a threat posed by Chinese people, as individuals. This is an issue pertaining to a communist country, with an autocratic dictator who is committed to human rights violations and will stop at nothing to achieve his goals. As a Nation, we must put the same effort into this threat as we did for the terrorism threat. The threat from China, particularly with respect to the long-term existential threat is hard to see and feel, but I would suggest it is as dangerous, if not more dangerous, than terrorism to our viability as a Nation.

RECOMMENDATIONS

The holistic and existential threat posed by the CCP is one of the few bipartisan areas of agreement in the U.S. Congress today. We must, as a Nation, compete at

the highest level possible while at the same time understand the gravity and urgency, and what is at stake.

Below are some recommendations:

1. Implement an aggressive real time and actionable threat sharing by the U.S. Government with private sector. *Create an Economic Threat Intelligence entity which delivers actionable, real-time threat information* to CEOs, boards of directors, State and local economic councils to enable risk-based decision making on investments and partnerships. This intelligence delivery mechanism should include the intelligence community, FBI, Department of Commerce, Department of Treasury, and CISA. The core constituency should be State and local entities at risk and utilize existing vehicles such National Governors Association and the Chamber of Commerce to increase threat awareness of illicit activities investment risk at the State and local level.

2. Congress must ensure U.S. Government agencies are leaning aggressively forward in providing collected intelligence to corporate America pertaining to plans and intentions, as well as nation-state activities, in software, coding, supply chain and zero-day capabilities. *The U.S. Government must be more effective in providing intelligence expeditiously to the private sector.* Enhanced declassification of collected intelligence (especially in the technology arena) with respect to threats to our economic well-being, industries, and companies must be delivered at speed to impacted entities prior to the threat becoming realized.

3. *Maintain bipartisan Congressionally-led public hearings* to advise and inform CEOs, governors, and boards of directors in critical economic, research, and manufacturing sectors of the threat posed by the CCP, and how they are targeted.

4. *Create a panel of CEOs who can advise and inform Congress and U.S. Government entities on perspectives, challenges, and obstacles in the investment arena and private-sector supply chain dilemmas.* I would recommend a Business Round Table type of framework. Membership should be diverse and include but not be limited to the following sectors: Financial Services, Telecommunications, Energy, Bio Pharmaceutical, Manufacturing, Aerospace, Transportation, Private Equity, and Venture Capital. This entity should be co-chaired by a CEO from the above group.

5. *Establish an over-the-horizon panel to discuss, in a public forum, emerging technology which may potentially pose a long-term threat (AI/ML, Quantum, Aerospace) to the long-term economic well-being of America.* The first topic should take a close look at the strategic investments the CCP is making into State and local pension plans, CCP's strategic land purchases, Sovereign Funds, as well as foreign investment into the Federal Thrift Savings Plan and other State/local retirements vehicles.

6. *Reestablish the National Security Higher Education Advisory Board (NSHEAB).* This board should have 25 college and university Presidents as members with a chair and co-chair and be housed and facilitated by the Federal Bureau of Investigation in partnership with the CIA and NSA. All members will be provided security clearances at the Top-Secret level in order to be provided real-time threat and awareness information the U.S. Government possess to help guide academia in risk-based decisions and partners. This entity existed until the FBI closed the program in 2014.

7. *Create a National Training Center for elected officials.* This center will provide baseline training to newly-elected officials and their staff on what malign influence looks like (examples of recent situations) and how to best mitigate such efforts. Additionally, what will surely occur on your first trip to China as an elected official, particularly with your mobile devices.

8. *Create a platform where each Governor of the United States can establish his/her own CIFIUS-Lite program to identify and mitigate nefarious economic investments and land purchases within their respective States.* This framework will provide intel and data sharing from the Treasury Department's CIFIUS Program, the FBI, DHS, and other law enforcement and intelligence entities to assist individual U.S. States on what to look, how such nefarious activity manifests at the local level, and how to most effectively mitigate.

Again, I am honored to be here today and thank the committee for holding this hearing to better understand and mitigate the existential risk posed the CCP to our national security.

Mr. GUEST. Thank you, Mr. Evanina.

I now recognize Mr. Singleton for 5 minutes to summarize his opening statement.

STATEMENT OF CRAIG SINGLETON, SENIOR FELLOW AND CHINA PROGRAM SENIOR DIRECTOR, FOUNDATION FOR DEFENSE OF DEMOCRACIES

Mr. SINGLETON. Acting Chairman Guest, Ranking Member Thompson, and distinguished Members of this committee, thank you for inviting me to testify today. I'm pleased to offer policy insights from the Foundation for Defense of Democracies, a nonpartisan research institute where I serve as a senior fellow.

Chinese Communist Party Chairman Xi Jinping has declared technological innovation the, quote, main battlefield in China's quest for global preeminence.

For Xi, Chinese-style modernization is not merely an economic goal. It's a historic mandate with grave implications for U.S. national security.

In seeking to dominate what he calls China's new productive forces—breakthroughs in batteries, biotech, LiDAR drones, robotics, and other cutting-edge technologies, Xi seeks to cement Chinese control over the drivers of the next industrial revolution.

In doing so, Xi intends to transform China into a global science superpower. Yet Xi's strategy is predicated on a glaring vulnerability. It depends, in part, on sustained access to U.S. capital markets and advanced technology, as well as near-unfettered reach into American data and critical infrastructure systems.

On this front, U.S. policy makers must act decisively and without delay.

Xi's broader technological ambitions underpin China's military-civil fusion strategy, a doctrine that breaks down barriers between the People's Liberation Army and China's civilian institutions, including Chinese universities and ostensibly private Chinese companies.

This fusion accelerates the transfer of scientific innovations directly into China's defense and intelligence sectors, ensuring that Chinese military capabilities evolve in lockstep with civilian progress.

Here at home, Beijing's strategy unfolds in 3 interlocking phases. First, Chinese actors relentlessly penetrate U.S. networks and critical infrastructure, harvesting vast troves of sensitive data in the process.

Recently exposed Chinese state-sponsored hacking campaigns—Salt, Volt, and Flax Typhoon—reveal how Beijing exploits software vulnerabilities, implants malicious code, and maintains persistent back doors.

More than a year after these breaches became public, Chinese hackers still enjoy near-persistent access to U.S. telecommunications networks, with Washington yet to impose any meaningful costs.

But hacking and data theft are just the opening gambit. Beijing's secondary goal is to systematically preposition itself within our networks to degrade or disrupt them at critical junctures, both in peace and in conflict.

By embedding compromised Chinese—compromised cranes in U.S. ports, Chinese-made LiDAR devices in traffic control, or drones that seamlessly integrate with civilian and military operations, Beijing gains a silent veto over our crisis response.

Whether through biotech innovations or batteries powering our grid, each dependency transforms market reliance into a strategic liability. In times of tension, the mere suspicion that these systems might be sabotaged could erode confidence, delay U.S. responses, and undermine our deterrent posture.

Third, China profits from this dual approach. Chinese high-tech exports, from advanced sensors and biotech to drones and surveillance cameras, generate billions in revenue every year for Beijing.

This revenue is funneled back into military-civil fusion programs, creating a self-reinforcing cycle of power.

What's more, by converting market access into geopolitical leverage, the CCP has weaponized Western dependence on its technologies, thereby undercutting U.S. competitiveness.

In response to these provocations, it's vital that policy makers act with both urgency and clarity. By levying meaningful penalties, including robust outbound investment screening, targeted export controls, and stringent procurement bands on high-risk Chinese technologies, Washington can deny Xi the leverage he seeks and compel China to reassess its aggressive posture.

If we fail to act, every hacked network, every compromised supply chain, and every dependency engineered by Beijing only heightens our vulnerability to disruption, sabotage, or even systemic failure during a crisis.

In many respects, today's predicament recalls the late stages of the Cold War when Washington's misguided embrace of peaceful coexistence inadvertently prolonged the Soviet system's survival, treating it as an immutable juggernaut rather than one susceptible to sustained internal and external pressure.

By minimizing accountability for Chinese espionage, coercion, and violations of international norms, we risk reinforcing Beijing's conviction that its revanchist ambitions need not be curbed.

We, therefore, must act and shift from a misguided policy rooted in reflexive de-escalation to one of assertive reprisal, from passive co-existence with China to purposeful competition on America's terms.

On behalf of the Foundation for Defense of Democracies, I thank you again for inviting me to testify today.

[The prepared statement of Mr. Singleton follows:]

CONGRESSIONAL TESTIMONY: FOUNDATION FOR DEFENSE OF DEMOCRACIES

House Homeland Security Committee

Countering Threats Posed by the Chinese Communist Party to U.S. National Security

CRAIG SINGLETON

China Program Senior Director and Senior Fellow
Foundation for Defense of Democracies

With contributions from Jack Burnham, M. Reece Breaux, and Kirin Atluru

Washington, DC
March 5, 2025

FDD
FOUNDATION FOR DEFENSE OF DEMOCRACIES

www.fdd.org

Introduction

Chinese Communist Party Chairman Xi Jinping has declared technological innovation the "main battlefield" in China's quest for global preeminence.[1] For Xi, Chinese-style modernization is not merely an economic goal — it is a historic mandate with global implications. In aiming to dominate what he calls "new productive forces" (龙质口产本) — breakthroughs in batteries, biotech, LiDAR, drones, and other cutting-edge technologies — Xi seeks to cement Chinese control over the drivers of the next industrial revolution.[2] In doing so, Xi intends to transform China into a global science superpower.[3]

Yet Xi's strategy rests on a glaring vulnerability. It hinges on sustained access to U.S. capital markets and advanced technology, as well as near-unfettered reach into American data and critical infrastructure systems. On this front, policymakers must act decisively and without delay, as Xi's ambitions pose an unprecedented threat to U.S. homeland security.

Xi's broader technological ambitions underpin China's military-civil fusion (军褊口淋) strategy, which breaks down barriers between military and civilian institutions to mobilize the latter in service of the former.[4] Military-civil fusion accelerates the direct transfer of data and advanced technologies — be they biotech discoveries or next-generation batteries — straight into China's defense sector. As a result, China's People's Liberation Army's (PLA) capabilities keep pace with rapid civilian technological progress, expanding Beijing's ability to challenge American interests at home and abroad.

Beijing's strategy is unfolding in three interlocking phases. First, Chinese actors and companies are relentlessly penetrating U.S. networks and critical infrastructure. Hacking campaigns like Salt, Volt, and Flax Typhoon demonstrate how state-sponsored entities are infiltrating our digital ecosystems to steal sensitive data and embed themselves in our communications, industrial, and defense networks.[5] These intrusions serve dual purposes: They collect intelligence and prepare for future sabotage. More than a year after these breaches were first made public, China still maintains persistent access to many compromised networks, having faced almost no penalty for its actions.

Second, Beijing prepositions its advantages by engineering dependencies that can be weaponized to advance China's national interests. China deliberately creates choke points in global supply chains and network infrastructures. Chinese-made LiDAR, compromised cranes in U.S. ports, and drones in both civilian and military applications illustrate this approach. Moreover, the U.S.

---

[1] "盆瞰猫设口疆强嚏"实现斑靼炸口疆口口口强 [Accelerating the Construction of a Science and Technology Powerhouse and Achieving High-Level Scientific and Technological Self-Reliance and Self-Reliance]," *Qiushi*, April 30, 2022. (https://archive.ph/pAqWG)

[2] Craig Singleton and Amaya Marion, "Safeguarding U.S. Interests in the Face of China's 'New Productive Forces' Strategy," *Foundation for Defense of Democracies*, May 2, 2024. (https://www.fdd.org/analysis/2024/05/02/safeguarding-u-s-interests-in-the-face-of-chinas-new-productive-forces-strategy); Arendse Huld, "China's New Quality Productive Forces: An Explainer," *China Briefing*, September 2, 2024. (https://www.china-briefing.com/news/chinas-new-quality-productive-forces-an-explainer)

[3] Ben Murphy, Rogier Creemers, Elsa Kania, Paul Triolo, and Kevin Neville, "Xi Jinping: 'Strive to Become the World's Primary Center for Science and High Ground for Innovation,'" *Stanford Cyber Policy Center*, March 18, 2021. (https://digichina.stanford.edu/work/xi-jinping-strive-to-become-the-worlds-primary-center-for-science-and-high-ground-for-innovation/#fn1)

[4] U.S. Department of State, "The Chinese Communist Party's Military-Civil Fusion Policy," 2020. (https://2017-2021.state.gov/military-civil-fusion)

[5] Craig Singleton, "Securing Communications Networks from Foreign Adversaries," *Testimony before the House Committee on Energy and Commerce*, February 15, 2024. (https://docs.house.gov/meetings/IF/IF16/20240215/116856/HMTG-118-IF16-Wstate-SingletonC-20240215.pdf)

Defense Department has warned that Beijing's cyber activities aim not merely to monitor but to compromise — and ultimately control — these sensitive systems and defense-related supply chains.[6] Whether it's biotech integrated into healthcare and defense or batteries powering our energy grid, each dependency represents a strategic vulnerability that endangers U.S. national security.[7]

Third, Beijing profits from this dual approach. The economic and military gains are immense. Chinese exports in high-tech sectors fuel rapid PLA modernization and undercut global competitors.[8] Every infiltration and dependency generates revenue that China reinvests in military-civil fusion programs, enhancing its capacity to wage war. By consistently converting market access into geopolitical leverage, the Chinese Communist Party (CCP) has significantly strengthened its influence over U.S. and allied decision-making, with the goal of weaponizing Western reliance on these technologies to force countries into accepting its strategic demands.

Today's stakes have never been higher. Beijing's three-phase strategy — penetrating our networks, prepositioning technological choke points, and profiting from those dependencies — poses a direct challenge to U.S. homeland security. In response, the United States must both fortify its networks and curtail China's ability to exploit these vulnerabilities to achieve its desired strategic ends. That effort demands robust outbound investment screening, paired with technology-specific controls and procurement bans, to safeguard America's critical infrastructure and national interests.

In sum, China's strategy threatens not only our technological edge but the security of our nation. As we enter an era of intensified great-power competition, policymakers must remain clear-eyed about the acute risks posed by Beijing's far-reaching ambitions and take immediate action to safeguard America's homeland security, preserve our leadership in innovation, and secure a free and open global order.

I. Xi's Strategic Vision for Technological Dominance

Xi regards technological prowess as the core pillar of China's "comprehensive national security" concept.[9] He has broadened the concept of security to encompass not only military strength but also the economic, political, and societal realms. In this framework, leading-edge technology undergirds everything from sustaining economic vitality to upholding the Communist Party's repressive surveillance apparatus. Although Xi acknowledges that China remains partially

---

[6] "Summary of the 2023 Department of Defense Cyber Strategy," U.S. Department of Defense, accessed February 13, 2024. (https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF)

[7] Craig Singleton, "Biotech Battlefield: Weaponizing Innovation in the Age of Genomics," *Foundation for Defense of Democracies*, January 15, 2025. (https://www.fdd.org/analysis/2025/01/15/biotech-battlefield); Craig Singleton, "Beijing's Power Play: Safeguarding U.S. National Security in the Electric Vehicle and Battery Industries," *Foundation for Defense of Democracies*, October 23, 2023. (https://www.fdd.org/analysis/2023/10/23/beijings-power-play)

[8] CEIC Data, "How High-Tech Has Taken a Greater Share of China's Exports," *CEIC Data*, 2024. (https://info.ceicdata.com/how-high-tech-has-taken-a-greater-share-of-chinas-exports); The Office of Senator Marco Rubio, "The World China Made: 'Made in China 2025' Nine Years Late," *Project for Strong Labor Markets and National Development*, 2024. (https://www.americanrhetoric.com/speeches/PDFFiles/Marco-Rubio-The-World-China-Made.pdf)

[9] Sheena Chestnut Greitens, "Xi's Obsession: Why China Is Digging In at Home and Asserting Itself Abroad," *Foreign Affairs*, July 28, 2023. (https://www.foreignaffairs.com/united-states/xis-security-obsession); Sheena Chestnut Greitens, "Internal Security & Grand Strategy: China's Approach to National Security under Xi Jinping," Statement before the U.S.-China Economic & Security Review Commission Hearing on "U.S.-China Relations at the Chinese Communist Party's Centennial," Panel on "Trends in China's Politics, Economics, and Security Policy," January 28, 2021. (https://www.uscc.gov/sites/default/files/2021-01/Sheena_Chestnut_Greitens_Testimony.pdf)

dependent on foreign technology, he has repeatedly warned that such reliance creates "stranglehold" (与口救)″ vulnerabilities, framing the pursuit of self-reliance as a matter of national survival.[10] His speeches emphasize that advanced fields like artificial intelligence, quantum computing, and biotech will determine the balance of global power in the decades ahead.

To realize this vision, Xi calls for fusing China's military and civilian capabilities into a single innovation engine. Under this strategy, state-backed companies and research institutes operate as dual-use platforms, ensuring that breakthroughs in commercial sectors directly benefit the PLA, as well as China's intelligence and security agencies. In Xi's view, this synergy not only accelerates military modernization but also positions China as a global technology leader. Official policies such as Made in China 2025 and China's most recent 14th Five-Year Plan mandate state involvement in strategic industries, from robotics and electric vehicles to high-performance computing.[11] By consolidating resources under CCP oversight, Xi believes China can outpace Western rivals and dictate the global technology agenda.

Global Leadership of Select Strategic Technologies, 2019-2023

Strategic Technology	Global Leader
Natural Language Processing	United States
Quantum Computing	United States
Advanced Aircraft Engines	China
Drones, Swarming, and Collaborative Robotics	China
Electric Batteries	China
Photovoltaics	China
Genetic Engineering	United States
Synthetic Biology	China

[10] "China Focus: Xi calls for developing China into world science and technology leader," *Xinhua* (China), May 28, 2018. (http://www.xinhuanet.com/english/2018-05/29/c_137213175.htm)

[11] China National People's Congress, "嘆华朝編蒜藁嚏嚏福经济藁口抵发寨口友嘱誰虫蒸规鋪藁2035蒸远邉口标纲口 (Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035)," May 13, 2021. (https://cset.georgetown.edu/publication/china-14th-five-year-plan); The Office of Senator Marco Rubio, "The World China Made: 'Made in China 2025' Nine Years Late," *Project for Strong Labor Markets and National Development*, 2024. (https://www.americanrhetoric.com/speeches/PDFFiles/Marco-Rubio-The-World-China-Made.pdf)

Hypersonic Detection and Tracking	China
Electronic Warfare	China

Source: *Australian Strategic Policy Institute*

An equally critical dimension of Xi's vision involves shaping international standards and norms. He has instructed Chinese firms and state agencies to take active roles in global standards-setting bodies, from the International Telecommunication Union (ITU) to the International Organization for Standardization (ISO).[12] By championing proprietary Chinese solutions — ranging from next-generation wireless protocols to AI ethics frameworks — Beijing seeks to establish global rules that align with its domestic priorities. Xi has underscored that controlling these technical rules of the game enhances China's ability to project influence abroad, effectively rewriting the architecture of global trade and communication to suit national interests.

At home, Xi's strategic vision also serves the CCP's political imperatives. The push for self-reliance in semiconductors, batteries, and other high-tech components reinforces state control over critical supply chains, reducing the risk that foreign sanctions or embargoes could undermine Chinese stability. Xi's domestic rhetoric frequently underscores that lagging behind in core technologies endangers both economic development and the Party's leadership. By placing key industries under direct Party supervision, Xi aims to ensure that private innovation does not become a breeding ground for dissent or foreign infiltration. This approach strengthens the Party's grip while speeding the pace of scientific discovery.

In tandem, Xi's ambitions extend well beyond China's borders. He frames technology not only as a means to catch up with advanced nations but also to surpass them, thereby reshaping global governance. From establishing digital payment systems that bypass Western financial networks to exporting surveillance platforms that promote a model of digital authoritarianism, Xi's strategy weds technology with foreign policy.[13] He portrays these exports as symbols of Chinese ingenuity, persuading other countries — especially in the Global South — to adopt Chinese standards and technology.[14] By weaving technology into broader diplomatic efforts, Xi solidifies Beijing's position as an alternative pole to the U.S.-led system.

---

[12] "China is writing the world's technology rules," *The Economist*, October 8, 2024. (https://www.economist.com/business/2024/10/10/china-is-writing-the-worlds-technology-rules); Matt Sheehan and Jacob Feldgoise, "What Washington Gets Wrong About China and Technical Standards," *Carnegie Endowment For International Peace*, February 27, 2023. (https://carnegieendowment.org/research/2023/02/what-washington-gets-wrong-about-china-and-technical-standards?lang=en)

[13] Barry Eichengreen, "Sanctions, SWIFT, and China's Cross-Border Interbank Payments System," *Center for Strategic & International Studies*, May 20, 2022. (https://www.csis.org/analysis/sanctions-swift-and-chinas-cross-border-interbank-payments-system)

[14] Bulelani Jili, "China's surveillance ecosystem and the global spread of its tools," *Atlantic Council*, October 17, 2022. (https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/chinese-surveillance-ecosystem-and-the-global-spread-of-its-tools)

These goals carry profound implications for U.S. homeland security and the global order at large. Xi's pursuit of technological dominance does not merely aim to strengthen China's economy; it seeks to reposition Beijing as the central architect of tomorrow's innovations, standards, and norms. While such objectives might appear purely aspirational, Xi's conception of "comprehensive national security" makes clear that technology leadership is also a means of political control and strategic leverage.[15] In short, Xi's vision threatens to remake the balance of power across critical sectors — from artificial intelligence to quantum computing — in ways that could challenge not only American competitiveness but also the security and freedom of open societies worldwide.

II. Penetrating U.S. Networks and Critical Infrastructure

China's move from high-level technological aspirations to tangible action began with a systematic push to penetrate U.S. networks and critical infrastructure. This effort has been neither opportunistic nor ad hoc; rather, it reflects a methodical plan to gather intelligence, undermine American defenses, and engineer dependencies that can be weaponized during both peace and wartime. Beijing's infiltration extends beyond mere data theft, delving into the very architecture of U.S. supply chains and physical systems in order to secure both economic and strategic leverage.

In the cyber domain, Chinese state-sponsored hackers routinely breach U.S. digital ecosystems. Campaigns such as Salt, Volt, and Flax Typhoon demonstrate the sophistication with which these actors exploit software and hardware vulnerabilities, implant malicious code, and maintain persistent access — even after detection.[16] According to warnings from the Department of Homeland Security (DHS), the Federal Bureau of Investigation, and the National Security Agency, these persistent footholds enable China to exfiltrate vast amounts of sensitive information — ranging from the contents of phone calls to proprietary corporate data — and lay the groundwork for future sabotage.[17] Minimal repercussions have only emboldened these activities, leaving unpatched vulnerabilities across defense and industrial networks.

Select PRC Cyber Intrusions, 2024-2018

Year	PRC Hacking Incident	Target
December 2024	Third-Party Vendor to U.S. Treasury Department	U.S. Treasury Department; Office of Foreign Assets; Control; Committee of Foreign Investment in the United States

[15] Katja Drinhausen and Helena Legarda, "'Comprehensive National Security' unleashed: How Xi's approach shapes China's policies at home and abroad," *Mercator Institute for China Studies*, September 15, 2022. (https://merics.org/en/report/comprehensive-national-security-unleashed-how-xis-approach-shapes-chinas-policies-home-and)

[16] House Committee on Homeland Security, "Cyber Threat Snapshot," November 12, 2024. (https://homeland.house.gov/wp-content/uploads/2024/11/11.12.24-Cyber-Threat-Snapshot.pdf)

[17] U.S. Department of Justice, "Court-Authorized Operation Disrupts Worldwide Botnet Used by People's Republic of China State-Sponsored Hackers," September 18, 2024. (https://www.justice.gov/archives/opa/pr/court-authorized-operation-disrupts-worldwide-botnet-used-peoples-republic-china-state); U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," February 7, 2024. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a); Matt Kapko, "Feds raise alarm on China-linked infiltration of telecom networks," *Cybersecurity Drive*, December 4, 2024. (https://www.cybersecuritydive.com/news/china-linked-attacks-infiltrate-networks/734576)

November 2024	Salt Typhoon	Telecommunications providers
September 2024	Flax Typhoon	Communications infrastructure; government agencies; critical infrastructure
May 2023	Volt Typhoon	Critical infrastructure
July 2023	Microsoft Email System	U.S. State Department; U.S. Commerce Department
May 2023	Guam	U.S. communications network
December 2022	U.S. Small Business Administration	U.S. COVID-19 relief funds
May 2022	U.S. private sector	Intellectual property from unidentified U.S. and European firms
October 2020	U.S. defense industrial base	Military secrets and intellectual property from unidentified U.S. firms
April 2020	U.S. healthcare system	Hospitals; pharmaceutical manufacturers; U.S. Department of Health and Human Services
March 2019	General Electric	Advanced aircraft engine designs
December 2018	U.S. defense industrial base	U.S. Navy contractors; ship maintenance data; missile plans

Source: Source: Cybersecurity and Infrastructure Security Agency China State-Sponsored Cyber Threat Advisories

Beijing's penetration strategy also targets the operational technology systems that undergird America's physical infrastructure. Devices like advanced LiDAR sensors, surveillance cameras, and drones — often from well-known Chinese brands — are embedded in energy grids, transportation networks, and industrial control systems.[18] By intertwining themselves with these systems, Chinese entities gain a vantage point over vital operations essential to U.S. homeland security. U.S. Department of Defense officials have voiced particular concern about Chinese influence over battery production, underscoring how reliance on these supply chains may grant

[18] Craig Singleton and Mark Montgomery, "Laser Focus: Countering China's LiDAR Threat to U.S. Critical Infrastructure and Military Systems," *Foundation for Defense of Democracies*, December 2, 2024. (https://www.fdd.org/analysis/2024/12/02/laser-focus-countering-chinas-lidar-threat-to-u-s-critical-infrastructure-and-military-systems); Nik Martin, "US bans Chinese telecom, surveillance cameras," *DW News*, November 26, 2022. (https://www.dw.com/en/us-bans-chinese-telecom-surveillance-cameras/a-63895206); Ana Swanson, "U.S. Weighs Ban on Chinese Drones, Citing National Security Concerns," *The New York Times*, January 2, 2025. (https://www.nytimes.com/2025/01/02/us/politics/drone-ban-china-security.html)

Beijing the power to disrupt or delay critical functions during a crisis.[19] A 2025 DHS bulletin warned that internet-connected cameras manufactured in China could potentially be exploited for espionage targeting the nation's critical infrastructure installations.[20]

Such infiltration does not end with a simple presence in foreign networks; it aims to transform global supply chain interdependence into a geopolitical weapon. China deliberately fosters reliance on its technology in advanced manufacturing, biotech, and other high-tech arenas, thereby creating strategic choke points. Dominance by Chinese battery giants like CATL and drone manufacturers like DJI exemplifies how entire U.S. industries — from automotive to agriculture — can become dependent on PRC-sourced parts and devices.[21] In a crisis, Beijing could withhold exports, inflate prices, or insert malicious features, effectively coercing U.S. decision-makers. Rather than hide their origins, these recognized Chinese brands benefit from market leadership, which makes it easier for them to entrench themselves in U.S. supply chains.

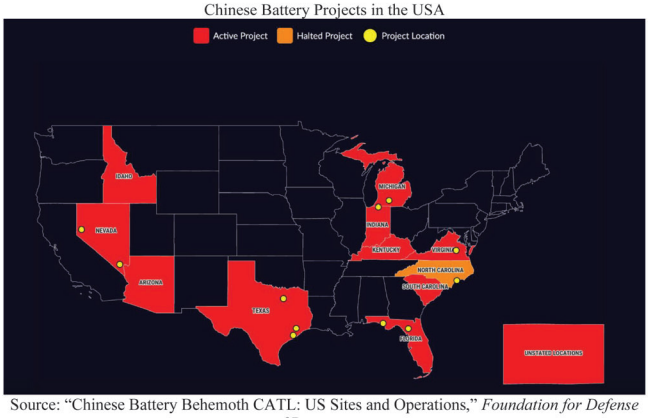
Leading Global Chinese Technology Firms

Industry	Chinese Champion	Global Market Share (%)
Drones	DJI	90
Batteries	CATL	38
Electric Vehicles	BYD	20
Agricultural Technology	Syngenta*	60
LiDAR	Hesai	47
Genomics	BGI Genomics**	5.8
Solar	Tongwei Solar	28

Source: *MIT Technology Review; South China Morning Post; International Energy Agency; Fitch Ratings; Yole Group; SanDiegomics; Fitch Ratings*
*Accounts for share of crop protection market
**Accounts for share of global sequencing market

[19] Ellen Nakashima, "Pentagon Adds Chinese Technology Firms to Blacklist over Security Concerns," *The Washington Post*, January 6, 2025. (www.washingtonpost.com/national-security/2025/01/06/pentagon-blacklist-china-technology-ev)
[20] "People's Republic of China: Exploitation of Internet-Connected Cameras Threatens US Critical Infrastructure," Department of Homeland Security, February 3, 2025. (https://wwema.org/wp-content/uploads/2025/02/Cybersecurity-DHS-IA-IF-2025-Peoples-Republic-of-China-Exploitation-of-Internet-Connected-Cameras.pdf)
[21] Craig Singleton, "Chinese Battery Behemoth CATL: U.S. Sites and Operations," *Foundation for Defense of Democracies*, 2023. (https://www.fdd.org/catlinusa)

Chinese Battery Projects in the USA



Source: "Chinese Battery Behemoth CATL: US Sites and Operations," *Foundation for Defense of Democracies*

The breadth of Beijing's penetration becomes evident when examining the key sectors at risk. In biotech and advanced manufacturing, Chinese firms infiltrate global research networks to acquire sensitive data that accelerates both civilian medical breakthroughs and PLA modernization. In energy and battery technologies, controlling production lines allows Beijing to create potential choke points in electric grids and vehicle fleets, leaving essential infrastructure vulnerable. In drones and autonomous systems, Chinese-made models integrate seamlessly into U.S. surveillance and logistics, opening covert pathways for data exfiltration or sabotage.

Similarly, in LiDAR and sensor technologies, Chinese devices capture real-time data from both smart city systems and military reconnaissance operations, enabling potential manipulation of critical monitoring functions. And, in surveillance cameras, millions of PRC-manufactured units — sometimes rebranded under U.S. labels — now secure airports, ports, and government buildings, raising concerns about remote access and unauthorized data extraction.

By embedding themselves in both digital networks and physical supply chains, Chinese entities gain unmatched visibility and control over critical U.S. systems. Each compromised link — be it a software backdoor or a key hardware component — adds another layer of risk. In a time of heightened tension, Beijing could exploit these vulnerabilities to disrupt communications, sabotage power grids, cripple ground transportation, or undermine emergency services.

Persistent intrusions also feed China's broader intelligence apparatus, sharpening its ability to plan and execute more sophisticated operations in the future.

Despite the seriousness of these breaches, Beijing has faced few consequences for these infiltrations. The absence of strong countermeasures only emboldens Chinese cyber actors and commercial giants to expand their presence. Moreover, repeated intrusions with minimal pushback allow Chinese cyber actors to refine their tactics, leaving critical networks and supply chains increasingly exposed. Over time, unchecked infiltration erodes America's ability to protect its own infrastructure, maintain a technological edge, and respond effectively to emergencies.

Ultimately, China's penetration of U.S. networks and infrastructure — coupled with its deliberate manipulation of weaponized supply chains — demands a forceful and multi-layered response. Policymakers must recognize that each infiltration is not just a theft of data but also a strategic maneuver to secure leverage during future conflicts or crises. Fortifying networks, scrutinizing outbound investments, and collaborating with trusted allies to rebuild resilient supply chains constitute the first steps in mitigating these threats. If left unaddressed, Beijing's penetration strategy will continue to undermine U.S. homeland security, national defense, and economic competitiveness — key pillars of American strength in the 21st century.

III. Prepositioning: Laying the Groundwork for Crisis Manipulation

China's infiltration of U.S. networks and infrastructure lays the groundwork for something more potent than mere data theft: prepositioning. Once embedded in vital systems, Beijing can do more than collect intelligence — it can prepare the battlefield for future crises by creating doubts about the reliability of America's own infrastructure.[22] This tactic reflects a guiding principle in PLA doctrine, which stresses that "the boundary between war and peace is fluid," and that forward-placed cyber and physical footholds allow China to gain mastery well before overt conflict begins. The concept resonates with the PLA's principle of xianfa zhiren (先发奉朝), or "gaining mastery by striking first," whereby effective prepositioning can degrade an adversary's defenses even in peacetime.[23]

Indeed, Xi's broader vision of "winning without fighting" finds direct application here: Infiltration itself can yield strategic victories by stalling or preventing U.S. action at critical junctures.

At its core, prepositioning transforms infiltration from an intelligence windfall into a means of exerting leverage when tensions escalate. If U.S. officials suspect that a communications network, electric grid, or drone fleet has been compromised, they may hesitate to rely on those assets in an emergency. The mere possibility of sabotage can induce self-imposed restrictions, effectively degrading America's crisis response. PLA theorists emphasize that instilling doubt in

[22] David DiMolfetta, "Chinese Hackers Embedded in U.S. Networks for Years, Pre-Positioning for Future Attacks, IC Warns," *NextGov*, February 7 2024. (https://www.nextgov.com/cybersecurity/2024/02/chinese-hackers-embedded-us-networks-years-pre-positioning-future-attacks-ic-warns/394009)

[23] James C. Mulvenon, Murray Scot Tanner, Michael S. Chase, David Frelinger, David C. Gompert, Martin C. Libicki, and Kevin L. Pollpeter, "Chinese Responses to U.S. Military Transformation and Implications for the Department of Defense," *RAND Corporation*, accessed February 26, 2025. (https://www.rand.org/content/dam/rand/pubs/monographs/2006/RAND_MG340.pdf)

an adversary's capabilities is often as effective as physical destruction.[24] By eroding confidence in U.S. systems, Beijing can blunt Washington's willingness to act decisively without firing a shot.

This prepositioning extends beyond code lurking in server backdoors; it includes the manipulation of hardware and supply chains that Beijing has painstakingly embedded in key industries. Chinese-manufactured batteries, LiDAR devices, and rebranded surveillance cameras can be remotely updated to alter their functionality at will.[25] Such hidden capabilities need not be activated frequently — only at moments when disruption is most advantageous to Beijing's strategic aims. In effect, these sleeper threats align with Xi's emphasis on achieving strategic objectives without direct conflict, using targeted interference or withheld components to stall American mobilization or sow confusion in the midst of a crisis.

The ramifications become even more acute if a conflict with China turns kinetic. In that scenario, prepositioned exploits could allow Beijing to degrade U.S. command-and-control functions at the outset of hostilities, paralyzing the rapid deployment of American forces or neutralizing critical logistics hubs. Military communications satellites, drone fleets, and other high-value transportation platforms might be disabled or manipulated, sowing confusion at a critical moment. Such disruptions could produce a cascading effect, crippling not only frontline operations but also broader U.S. infrastructure — such as port facilities and energy grids — on which those operations depend.

By compromising both military and civilian networks in advance, Beijing aims to slow the U.S. response, shift the balance of power early in the conflict, and potentially force a negotiated outcome favorable to Chinese interests.

From a homeland security perspective, prepositioning poses grave concerns because it exploits vulnerabilities that appear benign in ordinary times.[26] A port's container cranes, a municipal drone fleet, or even a hospital's medical equipment might operate smoothly for years — until a crisis. At that pivotal moment, compromised systems can fail, or merely be perceived as compromised, forcing operators to revert to slower, less capable backups. This dynamic extends China's influence well beyond direct confrontation, granting Beijing a silent veto over America's rapid-response capabilities.

Ultimately, prepositioning is the logical outcome of Beijing's infiltration efforts; penetration itself is not the end goal but rather the vehicle through which China creates latent threats in both digital networks and physical supply chains. By embedding malicious capabilities — ranging from dormant software code to critical hardware vulnerabilities — Beijing gains the ability to

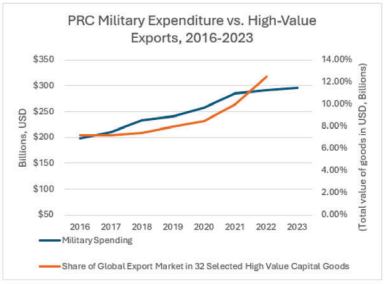
---

[24] Jeffery Engstrom, "Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare," *RAND Corporation*, February 1, 2018. (https://www.rand.org/pubs/research_reports/RR1708.html)
[25] Craig Singleton and Mark Montgomery, "Laser Focus: Countering China's LiDAR Threat to U.S. Critical Infrastructure and Military Systems," *Foundation for Defense of Democracies*, December 2, 2024. (https://www.fdd.org/analysis/2024/12/02/laser-focus-countering-chinas-lidar-threat-to-u-s-critical-infrastructure-and-military-systems); Craig Singleton, "Targeting Tiandy," *Foundation for Defense of Democracies*, December 1, 2022. (https://www.fdd.org/analysis/2022/12/01/targeting-tiandy)
[26] U.S. Department of Homeland Security, Cybersecurity Infrastructure Security Agency, "PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure," February 7, 2024. (https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a)

shape U.S. decision-making under duress. This capacity to degrade or disable key systems stands at the heart of Xi's vision for leveraging technology as a geopolitical tool.

IV. Profiting from Dependencies

Beijing's strategy of penetrating and prepositioning within U.S. networks is not solely about intelligence gathering — it is also designed to generate substantial economic leverage. Chinese high-tech exports, ranging from advanced sensors and biotech innovations to drones and surveillance systems, generate billions of dollars in revenue each year.[27] Major companies like DJI and CATL, for example, report multi-billion-dollar revenues bolstered by strong state support through subsidies, low-interest loans, and favorable industrial policies.[28] These financial gains are reinvested in research and development and military modernization, fueling the PLA's rapid expansion and creating a self-reinforcing cycle of power.



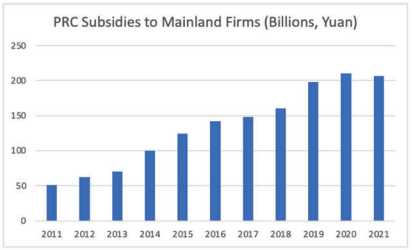
Source: Wall Street Journal; Statista; Department of Defense; Huawei; World Bank

By embedding its technology in critical supply chains, Beijing forces entire U.S. industries — from automotive and energy to healthcare and agriculture — to depend on Chinese components.[29] This dependency not only drives significant revenue for Chinese firms but also undermines American competitiveness. When U.S. companies rely on state-backed Chinese technology, market access transforms into a strategic vulnerability. In a crisis, Beijing could disrupt these supply chains by halting exports, manipulating pricing, or even inserting malicious features — thereby coercing U.S. decision-makers and weakening our economic foundation.

Chinese enterprises operating in key high-tech sectors benefit from extensive state backing. Favorable policies and direct financial support enable companies like CATL, DJI, and leading

[27] The State Council, The People's Republic of China, "Chinese Software and Info-Tech Sector Reports Revenue, Profit Growth in 2023," January 27, 2024. (https://english.www.gov.cn/archive/statistics/202401/27/content_WS65b48d3fc6d0868f4e8e3930.html)
[28] Curtis J. Milhaupt and Li-Wen Lin, "We Are the (National) Champions: Understanding the Mechanisms of State Capitalism in China," *Stanford Law Review*, 2013. (https://law.stanford.edu/publications/we-are-the-national-champions-understanding-the-mechanisms-of-state-capitalism-in-china)
[29] David Song-Penhamberger, "Controlling Tomorrow: China's Dominance Over Future Strategic Supply Chains," *The Diplomat*, August 21, 2024. (https://thediplomat.com/2024/08/controlling-tomorrow-chinas-dominance-over-future-strategic-supply-chains)

biotech firms to dominate global markets. Their commercial success translates into significant resources that Beijing channels into further technological innovation and military-civil fusion initiatives. In effect, every dollar earned through these channels not only strengthens China's economy but also reinforces its capacity to wage hybrid warfare and shape global standards.



Source: *Fitch Ratings*

Ultimately, converting market access into geopolitical leverage undermines U.S. competitiveness and national security. By profitably exploiting these dependencies, the CCP secures a dual advantage — reinforcing domestic military strength while exerting economic and diplomatic pressure on its adversaries. Disrupting these profit channels through robust export controls, stringent investment screening, and coordinated international measures is essential for protecting American industry and preserving our technological edge on the global stage.

V. Policy Recommendations

Beijing's systematic penetration of U.S. networks, its ability to preposition latent threats, and its profiteering from global dependencies underscore the urgency of a decisive policy response. The House Homeland Security Committee, in coordination with other congressional committees and executive agencies, can play a pivotal role in shaping legislation, funding priorities, and oversight mechanisms that protect America's critical infrastructure and strategic industries.

Below are key recommendations:

Overarching Measures for Homeland Security

- **Legislate Comprehensive Outbound Investment Screening, Enhanced Export Control Enforcement, and Targeted Sanctions:** Enact laws that rigorously scrutinize U.S. capital flows into Chinese firms involved in national security technologies and impose targeted sanctions on entities tied to military modernization or state surveillance — ensuring American investments do not bolster Beijing's coercive capabilities. Such a measure, modeled on the principles underpinning the

COINS Act, would ensure that American investments do not bolster Beijing's coercive capabilities, while protecting vital U.S. interests.

- **Close Export and Transshipment Loopholes:** Mandate interagency coordination among the Departments of Homeland Security, Commerce, State, Treasury, and Defense to track and penalize the rerouting of problematic Chinese technologies through third countries, with regular updates to the House Homeland Security Committee to track enforcement.

- **Establish a Critical Infrastructure Supply Chain Registry:** Direct the Department of Homeland Security to create a national registry that identifies critical components in high-risk sectors (energy, healthcare, transportation) and flags Chinese-linked vendors or products, thereby enhancing visibility into potential choke points.

- **Mandate Disclosure and Reporting for Chinese-Linked Components:** Require critical infrastructure operators to report within 72 hours any discovery of Chinese-manufactured or influenced hardware or software in sensitive systems, ensuring rapid federal response to potential infiltration.

- **Enhance Transparency for Chinese-Owned or -Controlled Firms:** Require clear labeling of high-tech products with ties to Chinese state-owned or military-linked companies — similar to existing FCC rules — so that government agencies and private operators can make informed procurement decisions and avoid hidden dependencies.

LiDAR and Sensor Technologies

- **Require DHS-Led Risk Certification:** Mandate that any LiDAR or sensor system intended for critical infrastructure (e.g., ports, airports, traffic control) undergo a DHS certification process verifying supply chain integrity and firmware security.

- **Conduct Supply Chain Audits for LiDAR Imports:** Direct DHS and the Department of Commerce to audit LiDAR and sensor imports, focusing on firmware vulnerabilities, Chinese ownership stakes, and potential remote-update backdoors.

- **Establish Sector-Specific Cybersecurity Standards:** Instruct the National Institute of Standards and Technology (NIST), in coordination with the Cybersecurity and Infrastructure Security Agency, to develop cybersecurity standards for LiDAR used in traffic management, smart cities, and other critical applications. Congress can pass legislation mandating compliance for federal contractors and grant recipients.

- **Mandate Regular Penetration Testing:** Require both public- and private-sector LiDAR users to perform periodic penetration testing and cybersecurity audits, potentially via amendments to the Federal Information Security Modernization Act (FISMA) to cover connected systems like LiDAR.

- **Ban DHS and Executive Agency Procurement of Chinese LiDAR Sensors:** Enact legislation prohibiting DHS and other federal agencies from procuring LiDAR systems manufactured by entities based in foreign countries of concern, ensuring no federal funds support risky vendors.

- **Enforce Strict LiDAR Data Localization:** Stipulate that LiDAR data collected by federal, state, or local governments be stored on U.S. soil, minimizing the risk of data exfiltration. Lawmakers could amend existing statutes (e.g., the CLOUD Act) to include LiDAR-specific data localization requirements.

- **Create a National Framework for LiDAR Data Security:** Direct the Department of Transportation (DoT), in coordination with the Transportation Security Administration (TSA) at DHS, to develop a framework governing LiDAR data in autonomous vehicles and transportation systems, mandating encryption standards, data retention policies, and data-sharing restrictions.

- **Evaluate Procurement Bans:** Consider legislation barring the Department of Transportation, DHS, and other government agencies from purchasing LiDAR sensors manufactured by companies in foreign countries of concern. This would also prevent Transportation grants (e.g., SMART Grants) from funding the acquisition of high-risk PRC-produced LiDAR systems.

- **Increase and Enforce Section 301 Tariffs on Chinese LiDAR:** Instruct the U.S. trade representative to raise tariffs on LiDAR imports from China above the current 25 percent threshold, while Customs and Border Protection conducts retroactive investigations to ensure proper enforcement and deter predatory pricing.

- **Create a DHS Task Force on Emerging LiDAR Threats:** Direct DHS, via CISA, to form an inter-agency task force dedicated to identifying and mitigating threats to LiDAR systems in transportation and critical infrastructure. Require the task force to issue regular public updates on vulnerabilities, mitigation strategies, and incident response.

- **Expand the FCC 'Covered List' to Include Chinese LiDAR Manufacturers:** Request DHS coordinate with the Federal Communications Commission to add major Chinese LiDAR producers to the "Covered List" of banned entities, blocking federal subsidies for their products and prompting a legislative review if necessary.

Batteries and Energy Technologies

- **Authorize a Comprehensive Intelligence Assessment of CATL and China's EV Industry:** Direct the intelligence community to assess the overlap between Chinese battery/EV firms (e.g., CATL, Gotion, etc.) and the Chinese Military-Industrial Companies List, as well as vulnerabilities in U.S. charging networks and energy storage systems that Beijing could exploit.

- **Institute Rigorous Regulatory Measures and Oversight Protocols:** Require federal and, where relevant, state authorities to monitor technology transfers, scrutinize investments, and ensure Chinese EV and grid-related projects adhere to stringent security and industry standards in the United States.

- **Ban DHS Procurement of Batteries from PRC-Aligned Companies:** Pass legislation prohibiting DHS and its agencies from purchasing battery systems produced by Chinese manufacturers such as CATL, BYD, Envision Energy, EVE Energy, Hithium, and Gotion High-Tech.

- **Expand CFIUS Review for Chinese Battery Investments:** Empower the Committee on Foreign Investment in the United States to more thoroughly review, limit, or condition investments by Chinese battery and EV firms in critical U.S. infrastructure or industries.

- **Strengthen Licensing Requirements for Chinese Energy Firms:** Mandate that Chinese companies operating in the U.S. energy sector undergo enhanced security reviews before receiving operational licenses, ensuring that potential risks to the grid or other vital systems are mitigated.

Biotech

- **Establish a Congressional Biotech and National Security Task Force**: Create a dedicated body to track threats posed by state-supported foreign entities — such as BGI and MGI — in the U.S. biotech sector. The task force would issue regular legislative and regulatory recommendations to safeguard sensitive research and supply chains.

- **Strengthen federal procurement restrictions**: Through measures like the BIOSECURE Act, prohibit U.S. federal agencies from purchasing BGI and MGI sequencers, ensuring no federal funds support entities linked to the CCP.

- **Amend Federal Grant Guidelines to Prohibit High-Risk Partnerships**: Bar federally funded research partnerships with Chinese biotech firms like BGI and MGI in sensitive fields, allowing exemptions only under strict oversight and transparency requirements to prevent unauthorized data transfers or infiltration.

Cameras and Surveillance Systems

- **Ban DHS Procurement of Cameras from High-Risk Vendors**: Prohibit DHS and its sub-agencies from purchasing or deploying surveillance cameras produced by entities linked to Chinese state or military organizations, ensuring that no federal dollars support compromised systems.

- **Mandate Comprehensive Risk Assessments**: Require federal and critical infrastructure operators to conduct periodic security evaluations of installed camera systems —

especially those from Chinese manufacturers — identifying remote-access vulnerabilities or hidden firmware backdoors.

- **Add Major Chinese Surveillance Firms to the 1260H List**: Request DHS coordination with the Department of Defense and other agencies to include key Chinese camera manufacturers, such as Tiandy, on the Chinese Military-Industrial Companies list, restricting their access to U.S. capital markets and federal procurement.

- **Sanction Firms Facilitating Human Rights Abuses**: Enforce targeted sanctions against Chinese companies that provide surveillance technology enabling human rights abuses, blocking them from U.S. financial systems and dissuading others from similar collaborations.

Conclusion

By enacting robust supply chain oversight, technology-specific restrictions, and rigorous investment screening, the House Homeland Security Committee can decisively blunt Beijing's infiltration, prepositioning, and profiteering. Each recommendation falls squarely within the Committee's legislative and oversight purview. By moving from a reactive stance to a proactive defense, Congress will safeguard U.S. critical infrastructure, deny Xi Jinping the leverage he seeks, and ensure that America's homeland security remains resilient in the face of China's aggressive techno-strategic ambitions.

Mr. GUEST. Thank you Mr. Singleton.

I now recognize Dr. Doshi for 5 minutes to summarize his opening statement.

STATEMENT OF RUSH DOSHI, PH.D., PRIVATE CITIZEN

Mr. DOSHI. Chairman Guest, Ranking Member Thompson, distinguished Members of the subcommittee, thank you very much for the opportunity to testify at today's hearing. I'll focus my remarks on some of the challenges China poses to Homeland Security.

Three questions: First, what are Beijing's ambitions; second, how does it threaten homeland security and the cyber domain; and,

third, how does it threaten homeland security with respect to transnational crime?

So, first, what are Beijing's ambitions?

The PRC has a grand strategy to displace U.S.-led order. It seeks to, quote, catch up and surpass the U.S. technologically to make the world dependent on China's supply chains economically, and to acquire the capability to defeat U.S. forces militarily.

It's a capable rival too. It's the leading industrial power with more than 30 percent of all global manufacturing. It's pursuing military bases around the world and in our backyard, and it's the first U.S. competitor to surpass 70 percent of U.S. GDP.

The second question: How does the PRC threaten homeland security?

Well, PRC cyber actors have compromised sensitive U.S. networks with multiple objectives. First, they want American personal data. In the last decade, the PRC has hacked the Office of Personnel Management, Equifax, Marriott, Anthem Health Insurance, and multiple airlines, compromising hundreds of millions of records.

Second, they want our IP. The PRC has infiltrated American companies to steal what some estimate is well over a trillion dollars of U.S. IP. That even includes compromising cloud providers that handle data for hundreds of companies.

Third, they want access to our Government systems. In the last 2 years, PRC actors compromised tens of thousands of emails from the State Department, Treasury Department, CFIUS, and even Presidential candidates.

Fourth and most concerning, as has been discussed already, they want to prepare the operational environment for wartime in the cyber domain.

That is no exaggeration. As we know, senior U.S. officials and corporate leaders, including Microsoft CEO Brad Smith, have indicated that the PRC is prepositioning for destructive cyber attacks on American power, gas, water, telecom, and transportation infrastructure that would affect the lives of millions of Americans.

So what do we in the cyber domain? In general, we need to shrink our attack surface and go after their attack surface. First, Congress should prohibit technology companies that sell to the USG from operating in China.

For example, the United States relies on Microsoft software, but to get market access in China, Microsoft provided source code for that software to Beijing.

The USG relies on Amazon and Microsoft cloud, but both Microsoft and Amazon turned over the operation of their cloud services in China to a Chinese company. All this creates vectors of vulnerability.

Second, Congress should codify the information and communication, technology, and services supply chain Executive order and fund the office that administers it.

This would let us prohibit certain PRC goods that connect to networks from being in the U.S. market.

The Biden administration's used this Trump-era tool to keep out PRC-connected vehicles, but that's just the start. Recently DHS-

CISA has found back doors in PRC medical devices. So the time for action is now.

Third, we need to go on the offense. If the PRC has accesses on our infrastructure, we need them on theirs as well, and that will take resourcing and staff.

The PRC has manpower for that. We don't have enough manpower. This committee has thought about a variety of steps that could help address that, including the PIVOTT Act.

We also have to protect our Federal work force from being cut at a time of peril.

Fourth, we need common-sense regulations in the private sector which right now has little incentive to upgrade its cybersecurity.

Third and final question, how does the PRC threaten homeland security through transnational crime?

Well, we all know that 200 Americans die every day from fentanyl overdose. We know the PRC is complicit, and we know that the PRC gives tax rebates and grants to Chinese chemical companies for manufacturing and exporting fentanyl precursors.

We know that it allows them to advertise their goods openly on PRC websites, and we know that its underground banks help cartels launder fentanyl profits.

They take hard dollars from the cartels in America. They provide them pesos in Mexico. They sell those dollars to Chinese citizens who want their cash out of China, and they take renminbi in compensation within China.

All that happens without any money transferring across a border. Well, the PRC has not taken real steps to address it. They tried in 2019, and again more significantly in 2023, but it wasn't enough.

They have the power to stop the precursor flow. They have the power to stop the money laundering which occurs, by the way, on apps that they control and that they monitor for dissident activity. If they can find dissidents, they can find money launderers.

But they won't do it because they prefer to keep this issue alive so they have leverage with Washington.

So what do we do?

First, we need to strengthen U.S. sanctions authority against entities involved in the fentanyl trade, including PRC financial institutions.

Second, Congress can link progress on fentanyl to other PRC priorities in consultation with the administration.

Third, Congress can pass the Corporate Transparency Act so we can track the beneficial owner of PRC shell companies and crack down on money laundering.

Finally, we should pass the Halt Fentanyl Act, to place fentanyl-related substances as a class into Schedule 1 of the Controlled Substances Act.

I'll end with this: The PRC poses many challenges to our security, but the issues that I focused on in my testimony today are the ones that affect the lives of tens of millions of Americans on a daily basis.

The China challenge is often abstract. I think it's important to link it to the lives of everyday Americans. With that, I thank you for your time and look forward to your questions.

[The prepared statement of Mr. Doshi follows:]

United States House Committee on Homeland Security

March 5, 2025

Threats from PRC Cyber Actors and Transnational Criminal Groups for the hearing on "Countering Threats Posed by the Chinese Communist Party to U.S. National Security"

Testimony by **Dr. Rush Doshi**
Assistant Professor of Security Studies, Georgetown University Walsh School of Foreign Service
C.V. Starr Senior Fellow for Asia Studies and Director of the China Strategy Initiative, Council on Foreign Relations

---

Chairman Green, Ranking Member Thompson, distinguished members of the Committee, thank you very much for the opportunity to testify at today's hearing.

I will focus my remarks on some of the challenges China poses to homeland security:

1. First, what are Beijing's ambitions?
2. Second, how does it threaten homeland security in the cyber domain?
3. Third, how does it threaten homeland security through transnational crime?

I. PRC Ambitions and Intentions

The Chinese Communist Party is a nationalist political party dedicated to the goal of national rejuvenation after what it perceives as a "century of humiliation" at the hands of imperial powers. Related to that objective, the PRC has a grand strategy to displace U.S.-led order.[1] It seeks to "catch up and surpass" the U.S. technologically; to make the world dependent on China's supply chains economically; and to acquire the capability to defeat U.S. forces militarily.

The PRC is a capable rival too. It is the leading industrial power with more than 30% of all global manufacturing.[2] It is pursuing military bases around the world and in the Western hemisphere. It is also the first U.S. competitor to surpass 70% of U.S. GDP in a century.[3]

The PRC's preferred alternative for global order would be substantially different from the U.S.-led order that has prevailed since the end of the Cold War. It is discernable in speeches by senior PRC leaders. Politically, Beijing would project leadership over global governance and international institutions, split Western alliances, and advance autocratic norms at the

expense of liberal ones. Economically, it would weaken the financial advantages that underwrite U.S. hegemony and seize the commanding heights of the "fourth industrial revolution" from artificial intelligence to quantum computing, with the United States declining into a "deindustrialized, English-speaking version of a Latin American republic, specializing in commodities, real estate, tourism, and perhaps transnational tax evasion."[4] Militarily, the People's Liberation Army (PLA) would field a world-class force with bases around the world that could defend China's interests in most regions and even in new domains like space, the poles, and the deep sea. The fact that aspects of this vision are visible in high-level speeches is strong evidence that China's ambitions are not limited to Taiwan or to dominating the Indo-Pacific.

The PRC perceives the international system as providing opportunity for the PRC to achieve national rejuvenation. Since 2017, Xi has in many of the country's critical foreign policy addresses declared that the world is in the midst of "great changes unseen in a century" [百年未有之大变局]. The phrase captures the idea that the order is once again at stake because of unprecedented geopolitical and technological shifts, and that this requires strategic adjustment. For Xi, the origin of these shifts is China's growing power and what it saw as the West's apparent self-destruction. On June 23, 2016, the United Kingdom voted to leave the European Union. Then, a little more than three months later, a populist surge catapulted Donald Trump into office as president of the United States. From China's perspective—which is highly sensitive to changes in its perceptions of American power and threat—these two events were shocking. Beijing believed that the world's most powerful democracies were withdrawing from the international order they had helped erect abroad and were struggling to govern themselves at home. The West's subsequent response to the coronavirus pandemic in 2020, and then the storming of the U.S. Capitol by extremists in 2021, reinforced a sense that "time and momentum are on our side," as Xi Jinping put it shortly after those events.[5] China's leadership and foreign policy elite declared that a "period of historical opportunity" [历史机遇期] had emerged to expand the country's strategic focus from Asia to the wider globe and its governance systems.

Although the PRC poses a variety of challenges to the United States, this testimony focuses on two in particular relevant to this jurisdiction and that affect millions of Americans: (1) the threat posed by PRC cyber actors, particularly to U.S. critical infrastructure, and (2) the threat posed by PRC criminal actors, especially in production and money laundering related to Fentanyl.

We now turn to each respectively.

II. PRC Cyber Threats to Personal Data, Intellectual Property, Government Systems, and Critical Infrastructure

PRC cyber actors have compromised sensitive U.S. networks with multiple objectives.

First, the PRC seeks access to American personal data for intelligence purposes. In the last decade, the PRC has hacked the Office of Personnel Management, Equifax, Mariott, Anthem Health Insurance, and multiple airlines – compromising hundreds of millions of records.[6]

Second, the PRC seeks access to American intellectual property. The PRC has infiltrated American companies to steal what some estimate at over $1 trillion of U.S. intellectual property.[7] PRC cyber actors have compromised cloud providers that handle data for hundreds of companies.[8]

Third, the PRC seeks access to government systems. In the last two years, PRC actors compromised tens of thousands of emails from the State Department, Treasury Department, and other agencies. Notably, the PRC targeted Microsoft Exchange Online, which allowed it to compromise 60,000 State Department emails and compromising the account of U.S. Commerce Secretary Gina Raimondo, U.S. Ambassador to China Nicholas Burns, and others. It is still unknown how the PRC was able to do this, and the incursion was first detected by the State Department.

Fourth, and most concerning, the PRC is preparing the operational environment for wartime using cyber instruments. Government officials and private sector leaders have increasingly called attention to PRC activity in U.S. critical infrastructure that could pose a direct threat to homeland security. Earlier this year, CISA, NSA, FBI, and Five Eyes partners assessed that, "that People's Republic of China (PRC) state-sponsored cyber actors are seeking to pre-position themselves on IT networks for disruptive or destructive cyberattacks against U.S. critical infrastructure in the event of a major crisis or conflict with the United States," and that a PRC group called "Volt Typhoon" had comprised infrastructure providers in several sectors.[9] At the Munich Security Conference a few weeks later, Deputy National Security Adviser Anne Neuberger explained further that, "For a long time when we all in the industry talked about cyber security our key focus was theft of data...what has shifted as captured in the Volt Typhoon threat vector is countries pre-positioning in the critical infrastructure of another country." Neuberger explained that "we know it is not for espionage purposes, because when we look at the sectors like water sectors and civilian airport sectors, those have very little intelligence value." She continued, "That is a concern because a potential disruption of critical infrastructure could be used to put pressure on a government during a crisis or could be used to put pressure or try to message to a population during a crisis.[10] As Jen Easterly said to the Select Committee on the CCP, the PRC is ready to "launch destructive cyber-attacks in the event of a major crisis or conflict with the United States," including "the disruption of our gas pipelines; the pollution of our water facilities; the severing of our

telecommunications; the crippling of our transportation systems." These steps would be designed to "to incite chaos and panic across our country and deter our ability to marshal military might and citizen will."[11]

The private sector is aware of the problem. As Microsoft CEO Brad Smith explained, "we've seen from China in particular this prepositioning of so-called web shells. Think of it as tunnels into our water system, our electrical grid, into the air traffic control system, the kind of thing that you look at and you say, this is only useful for one thing and that's they have it in place in the event of a war or hostilities."[12] In an annual report last year, Microsoft noted it had been tracking some of the relevant threat actors focused on U.S. critical infrastructure for several years.

In general, the United States needs to shrink its attack surface while investing in offensive operations against the PRC to establish deterrence.

First, Congress should prohibit software companies that sell to the U.S. government from operating in China. Several U.S. technology companies that serve the U.S. government have provided the PRC government the source code of the systems that the U.S. government and most Americans rely on. In 2003, Microsoft allowed China to participate in its Government Security Program which it indicated "provides national governments with controlled access to Microsoft Windows source code."[13] More recently, in 2016, Microsoft launched a "Transparency Center" in China to provide "access to documents and source code" for "Windows, Windows Server, Office, Exchange Server, SQL Server, and SharePoint Server," services upon which the U.S. government also depends.[14] Similarly, in 2015 IBM decided to allow the Chinese government review its source code in a controlled environment.[15]

Second, Congress should prohibit cloud operators that support the U.S. government from operating in China. These companies almost certainly face conflicts given the PRC's regulatory environment. The PRC has introduced a National Intelligence Law, Counterespionage Law, Encryption Law, Data Security Law, and updates to its definition of state secrets in recent years. This regime gives the PRC the ability to demand PRC entities and individuals comply with requests from the intelligence services, provide access to encryption keys, insert personnel on site, or outright seize equipment and data. In that regime, the fact that U.S. cloud operators in China are required by the Chinese government to partner with a Chinese operator is concerning. Microsoft, for example, partners with 21 Vianet, to operate Microsoft's cloud services in China, including Azure; Amazon partners with Beijing Sinnet Technology Co., Ltd. (Sinnet) and Amazon Web Services Ningxia Region run by Ningxia Western Cloud Data Technology, Co., Ltd. (NWCD). Others, like Google and Oracle, do not offer services in China.[16] For those that do, the concern is whether their systems in China are adequately firewalled from systems in the United States, or whether compromise of cloud infrastructure in China could be used to compromise U.S. systems. Even with such firewalls, it is conceivable that PRC operating partners could gain important

insights into how their U.S. partners provide cloud services to clients in the United States, important information about network topology and architecture. More fundamentally, the fact that PRC operators may be operating a PRC cloud with encryption keys provided to the PRC government all under a regime that gives broad authority to PRC intelligence services to embed themselves in the operator suggests data stored in U.S. cloud systems in the PRC is not secure.

There are reasons to believe the PRC is focused on gaining advantages from these kinds of entanglements. For example, technology companies supporting the U.S. government may be forced to cooperate with China's cybersecurity legislation by providing information on zero-days that the PRC government appears to be promptly weaponizing. Microsoft has publicly accused the PRC of using the country's new vulnerability disclosure requirements to stockpile zero-day exploits. "China's vulnerability reporting regulation went into effect September 2021," it wrote in a 2022 report, "marking a first in the world for a government to require the reporting of vulnerabilities into a government authority for review prior to the vulnerability being shared with the product or service owner." Based on the data, Microsoft concludes that, "the increased use of zero days over the last year from China-based actors likely reflects the first full year of China's vulnerability disclosure requirements for the Chinese security community and a major step in the use of zero-day exploits as a state priority."[17]

What is particularly concerning is the possibility that the PRC may be learning more about systems on which the U.S. relies while reducing its own reliance on U.S. systems. Conversely, we may not be able to gain comparable information about PRC systems. Over time, this creates a structural asymmetric vulnerability. This is not a purely academic consideration. For example, even as Microsoft was increasing PRC visibility into its products, the PRC was reducing its reliance on Microsoft products and forcing public service providers and others to switch to the indigenous PRC HarmonyOS system. During the recent outage related to a CrowdStrike update, PRC public services – in contrast to U.S. services – experienced "minimal impact." PRC government employees boasted that this "proved that the country has made progress in achieving its goal of 'safe and controllable' computing systems." Accordingly, there are risks that the information shared with the PRC about U.S. technology systems could create asymmetric vulnerabilities. Similarly, although U.S. cloud providers do have some market share in China, they are small compared to Chinese cloud providers who have successfully increased their market share. As with consulting, the benefits from involvement in the PRC marketplace are likely falling while the risks are growing. As Microsoft CEO Brad Smith noted in recent testimony, China accounts for about 1.5% of Microsoft's revenue and is scaling down its engineering team. At the same time, the PRC is backing its own cloud providers in foreign markets, and the opportunity for U.S. providers in the market is shrinking while the risks continue to grow.[18]

Third, Congress should codify the Information Communication Technology and Services Supply Chain Executive Order and fund the office that administers it. This lets us prohibit certain PRC goods that connect to networks. The Biden Administration used this Trump-era tool keep out PRC connected vehicles. But that's just the start. Recently, DHS CISA has found backdoors in PRC-made medical devices.[19] The time for action is now.

Finally, the United States needs to go on the offensive. If the PRC has accesses on U.S. critical infrastructure, the United States reciprocally needs to maintain access on PRC critical infrastructure. That will take resourcing and staff. Presently, the PRC has invested in that kind of manpower, but the United States generally has not. Accordingly, this Committee's Cyber PIVOTT Act can help boost our workforce for defense and offense.[20] Related to all of this are better defensive measures. Notably, the United States needs common sense regulation of the private sector, which right now has little incentive to upgrade its cybersecurity.

III. PRC Transnational Criminal Activity, Fentanyl, and Money Laundering

Two-hundred Americans die every day due to Fentanyl overdoses.[21] According to the DEA, Fentanyl overdoses are the leading cause of death for Americans between 18 and 45 and are responsible for 70% of overdose deaths in the United States.[22] In 2020, the DEA released a report on the flow of Fentanyl which found that, "China remains the primary source of Fentanyl and Fentanyl-related substances trafficked through international mail and express consignment operations environment, as well as the main source for all Fentanyl-related substances trafficked into the United States."[23] The PRC is directly complicit in the flow of Fentanyl to the United States.

The PRC gives tax rebates and grants to Chinese chemical companies for manufacturing and exporting Fentanyl precursors.[24] The PRC not only provides state-sponsored support to these companies; the Select Committee on the CCP found that the party holds direct ownership interest in at least four companies with connections to illicit drug sales.[25] The PRC also allows these companies to advertise their goods openly on PRC websites.[26] Moreover, PRC underground banks help cartels launder Fentanyl profits. These banks take hard dollars from the cartels in America and provide them pesos in Mexico; they then sell those dollars to Chinese citizens who want their cash out of China and take renminbi in China as compensation.[27] These transactions do not require the actual flow of funds across borders.

The PRC has taken steps to address this issue only twice: in 2019 and more significantly in 2023, when they went after some companies, shut down websites, took down advertisements, went after some money launderers.[28] But these actions are still inadequate. Ultimately, the PRC has the power to stop the precursor flow. They can stop money laundering too, which occurs on apps like WeChat that the PRC government monitors for dissidents. But for now, the PRC has not done so. Beijing instead appears to prefer to keep the issue alive for leverage with Washington.

As for possible solutions, Congress needs to strengthen U.S. sanctions authorities against entities involved in the Fentanyl trade, including PRC financial institutions.[29] Relatedly, Congress can also link progress on Fentanyl to other PRC priorities, in consultation with the administration. To combat money laundering, Congress should pass the Corporate Transparency Act so law enforcement can track the beneficial owner of PRC shell companies and crack down on money laundering.[30] Finally, Congress should pass the HALT Fentanyl Act to place Fentanyl-related substances as a class into schedule I of the Controlled Substances Act.[31] By imposing stricter penalties on Fentanyl, the law could deter international trafficking from China and strengthen law enforcement efforts against international drug trafficking networks.

I'll end with this. The PRC poses many challenges to homeland security. The issues addressed in this testimony affect the lives of tens of millions of Americans. The China challenge is abstract, so it is important we link it to the lives of everyday Americans.

With that I thank you for your time and look forward to your questions.

---

[1] Rush Doshi, *The Long Game: China's Grand Strategy to Displace American Order* (Oxford University Press, 2021).

[2] Dave Evans, "China's Crossroads: Challenges & Opportunities For The World's Factory," *Forbes*, November 26, 2024, https://www.forbes.com/sites/daveevans/2024/11/26/chinas-crossroads-challenges--opportunities-for-the-worlds-factory/; China Power Team, "Measuring China's Manufacturing Might," China Power, Center for Strategic and International Studies, last updated December 18, 2024, https://chinapower.csis.org/tracker/china-manufacturing/.

[3] Micah McCartney, "How China's Economy Compares to the US's After Latest Results," *Newsweek*, July 16, 2024, https://www.newsweek.com/china-us-economies-compared-1925603.

[4] Michael Lind, "The China Question," *Tablet*, May 19, 2020, https://www.tabletmag.com/sections/news/articles/china-strategy-trade-lind.

[5] Xi Jinping [习近平], "Xi Jinping Delivered an Important Speech at the Opening Ceremony of the Seminar on Learning and Implementing the Spirit of the Fifth Plenary Session of the 19th Central Committee of the Party" [习近平在省部级主要领导干部学习贯彻党的十九届五中全会精神专题研讨班开班式上发表重要讲话], Xinhua [新华], January 11, 2021.

[6] "Cyber Operations Tracker," Council on Foreign Relations, https://www.cfr.org/cyber-operations/. See also, Ellen Nakashima, "Hacks of OPM databases compromised 22.1 million people, federal authorities say," *Washington Post*, July 9, 2015, https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/hack-of-security-clearance-system-affected-21-5-million-people-federal-authorities-say/; Katie Benner, "U.S. Charges Chinese Military Officers in 2017 Equifax Hacking," *New York Times*, February 10, 2020, https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html; David E. Sanger, Nicole Perlroth, Glenn Thrush, and Alan Rappeport, "Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing," *New York Times*, December 11, 2018, https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html.

[7] Estimates vary, but all align around roughly at least $1 trillion in losses is conservative. See, Commission on the Theft of American Intellectual Property, *Update to the IP Commission Report*, February 27, 2017, http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf; Nicole Sganga, "Chinese Hackers Took Trillions in Intellectual Property from About 30 Multinational Companies," *CBS News*, May 4, 2022,

https://www.cbsnews.com/news/chinese-hackers-took-trillions-in-intellectual-property-from-about-30-multinational-companies/.

[8] Jack Stubbs, Joseph Menn, and Christopher Bing, "Inside the West's failed fight against China's 'Cloud Hopper' hackers," *Reuters*, June 26, 2019, https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/.

[9] United States of America, Australian Government, Dominion of Canada, United Kingdom of Great Britain and Northern Ireland, New Zealand, *Joint Cybersecurity Advisory: PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, Cybersecurity & Infrastructure Security Agency (US), National Security Agency (US), Department of Justice (US), Department of Energy (US), Environmental Protection Agency (US), Transportation Security Administration (US), Signals Directorate (AUS), Cyber Security Centre (AUS), Communications Security Establishment (CAN), Centre for Cyber Security (CAN), National Cyber Security Centre (NZ), National Cyber Security Centre (UK), AA24-038A, February 7, 2024, https://www.cisa.gov/sites/default/files/2024-03/aa24-038a_csa_prc_state_sponsored_actors_compromise_us_critical_infrastructure_3.pdf.

[10] Anne Neuberger, "MCSC 2024: Fireside Chat: Anne Neuberger," Sicherheitsnetzwerk München, March 11, 2024, YouTube video, https://www.youtube.com/watch?v=WlvcT3aPb2k.

[11] Jen Easterly, "Opening Statement by CISA Director Jen Easterly," Blog, News, Cybersecurity& Infrastructure Security Agency, January 31, 2024, https://www.cisa.gov/news-events/news/opening-statement-cisa-director-jen-easterly.

[12] *A Cascade of Security Failures: Assessing Microsoft Corporation's Cybersecurity Shortfalls and the Implications for Homeland Security*, 118th Congress, 2nd session, 2024, (Statement of Brad Smith, Vice Chairman and President, Microsoft).

[13] "Microsoft and China Announce Government Security Program Agreement," Stories, Microsoft, February 28, 2003, https://news.microsoft.com/2003/02/28/microsoft-and-china-announce-government-security-program-agreement/; "China Information Technology Security Certification Center Source Code Review Lab Opened," Stories, Microsoft, September 26, 2003, https://news.microsoft.com/2003/09/26/china-information-technology-security-certification-center-source-code-review-lab-opened/; "Microsoft Gives Chinese Government Access to Windows Source Code," *People's Daily*, March 4, 2003, http://en.people.cn/200303/04/eng20030304_112657.shtml.

[14] Laramillermsft and MicrosoftGuyJFlo, "Transparency Centers," Articles, Microsoft Security, Microsoft, February 2, 2024, https://learn.microsoft.com/en-us/security/engineering/contenttransparencycenters.

[15] Eva Dou, "IBM Allows Chinese Government to Review Source Code," *Wall Street Journal*, October 16, 2015, https://www.wsj.com/articles/ibm-allows-chinese-government-to-review-source-code-1444989039.

[16] "Cloud Locations," Google, https://cloud.google.com/about/locations#asia-pacific; Public Cloud Region Locations, Oracle, https://www.oracle.com/cloud/public-cloud-regions/.

[17] Microsoft, *Microsoft Digital Defense Report*, Security Insider, Microsoft, 2022, 39-40, https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2022.

[18] Mark Montgomery and Eric Sayers, "Don't Let China Take Over the Cloud — US National Security Depends On It," *Hill*, November 13, 2023, https://thehill.com/opinion/national-security/4307002-dont-let-china-take-over-the-cloud-us-national-security-depends-on-it/.

[19] "Contec CMS8000 Contains a Backdoor | CISA," February 13, 2025, https://www.cisa.gov/resources-tools/resources/contec-cms8000-contains-backdoor.

[20] "Chairman Green Reintroduces 'Cyber PIVOTT Act,' Senator Rounds to Lead Companion Legislation – Committee on Homeland Security," February 5, 2025, https://homeland.house.gov/2025/02/05/chairman-green-reintroduces-cyber-pivott-act-senator-rounds-to-lead-companion-legislation/.

[21] USAFacts Team, "Are fentanyl overdose deaths rising in the US?" *USAFacts*, last updated September 27, 2023, https://usafacts.org/articles/are-fentanyl-overdose-deaths-rising-in-the-us/.

[22] "DEA Administrator on Record Fentanyl Overdose Deaths | Get Smart About Drugs," accessed March 3, 2025, https://www.getsmartaboutdrugs.gov/media/dea-administrator-record-fentanyl-overdose-deaths.
[23] "Fentanyl Flow to the United States," Drug Enforcement Agency Intelligence Report, DEA-DCT-DIR-008-20 (2020), https://www.dea.gov/sites/default/files/2020-03/DEA_GOV_DIR-008-20%20Fentanyl%20Flow%20in%20the%20United%20States_0.pdf.
[24] "Select Committee Unveils Findings into CCP's Role in American Fentanyl Epidemic," April 16, 2024, https://selectcommitteeontheccp.house.gov/media/reports/select-committee-investigates-ccps-role-fentanyl-crisis
[25] Ibid.
[26] Ibid.
[27] Joe Miller and James Kynge, "The New Money Laundering Network Fuelling the Fentanyl Crisis," *Financial Times*, June 27, 2024, https://www.ft.com/content/acaf6a57-4c3b-4f1c-89c4-c70d683a6619.
[28] Alex Willemyns, "Rubio Accuses China Of 'Reverse' Opium War Via Fentanyl," *Radio Free Asia*, February 27, 2025, https://www.rfa.org/english/china/2025/02/27/china-rubio-fentanyl-opium-war/.
[29] Congress.gov. "H.R.10447 - 118th Congress (2023-2024): CCP Fentanyl Sanctions Act." December 17, 2024. https://www.congress.gov/bill/118th-congress/house-bill/10447.
[30] Congress.gov. "H.R.2513 - 116th Congress (2019-2020): Corporate Transparency Act of 2019." October 23, 2019. https://www.congress.gov/bill/116th-congress/house-bill/2513.
[31] "Grassley, Cassidy, Heinrich Propose Permanent Scheduling Fix for Fentanyl-Related Substances | United States Senate Committee on the Judiciary," January 30, 2025, https://www.judiciary.senate.gov/press/rep/releases/grassley-cassidy-heinrich-propose-permanent-scheduling-fix-for-fentanyl-related-substances.

Mr. GUEST. Thank you. Members will now be recognized by order of seniority for their 5 minutes of questioning. An additional round of questioning may be called after all Members have been recognized.

I now recognize myself for 5 minutes of questioning.

Mr. Singleton, I want to begin with you. In your written testimony that you submitted, on page 3 of that testimony, you have there a graph, a chart, that is titled "Global Leadership of Select Strategic Technologies."

There are 10 technologies that you have listed there, and in each of those, you have identified a global leader. It is troubling to me that it appears that, of those global leaders, that the United States

is the leader in 3 of those categories, and then China is the leader in the other 7.

So 70 percent of those technologies we see that China has outperformed the United States in those areas and just wanted to see if you could talk about that very briefly.

Mr. SINGLETON. Sure, no, thank you for the question. I mean, it's no mistake that China leads in those sectors. For more than a decade—and we are in now 2025, and I think we all remember the China "Made in 2025" plan—they decided to put their money where their mouth is.

Through intense industrial policy, the theft of our own intellectual property and through aggressive nonmarket practices, they were able to invest and scale in some of the largest technology companies in the world.

Whether it's DJI drones or Hesai LiDAR here in the United States or CATL batteries, these are Chinese champions that report directly to the Chinese Communist Party.

I think ultimately what we have to start thinking about are some cyber quarantines for some of these high-risk technologies here in the United States, really treating these systems, these devices, and these companies as inherently risky.

We probably need to really restrict, I think, their use in critical infrastructure in particular, and that's an area where I think Congress can make a tremendous impact.

Mr. GUEST. Let me ask you—and then I'll ask other members—you talk about restricting Chinese access to information. Congress had passed a TikTok ban several months back.

We see that currently there has been a stay on that as there are on-going negotiations between the American and the Chinese Government over the ownership of TikTok, particularly by ByteDance, the Chinese company.

First, Mr. Singleton, do you have any thoughts on does the Chinese ownership of TikTok, does that pose a threat to homeland security, and is that relevant for the hearing that we are having here today?

Mr. SINGLETON. Absolutely. I mean, Chinese Communist Party Chairman Xi Jinping referred to data as the 21st Century oil, and I can't think of any more pernicious threat than the one posed by TikTok.

Mr. GUEST. Dr. Doshi, what are your thoughts?

Mr. DOSHI. Mr. Chairman, I would agree, and I would go further and say that one of the challenges that TikTok poses is 180 million Americans can use it to get information. I don't want the control of the algorithm that displays that information to be controlled by Beijing. So I think this is a 100 percent real security threat.

Mr. GUEST. Mr. Evanina, do you have an opinion on that?

Mr. EVANINA. I would concur with my colleagues and also say that from an intelligence perspective, I think TikTok is one of the greatest intelligence operations ever in the history of the world.

Its target is directly at America with 180 million people having a device, and their ability to control the algorithms, drive their intelligence to our diaspora is harmful at the minimal and potentially devastating in the long run.

Mr. GUEST. Then Dr. Pillsbury.

Mr. PILLSBURY. Well, I agree, but I think I would get back to my main message of the need to rank order of priorities of what we're going to do about China.

Breaking off the connection between the CCP and TikTok is important, but there's an awful lot of things more important than that that even have some sense of urgency.

So it seems to me there is a political warfare or information warfare space that needs more attention. This—TikTok is part of it. There are other spaces, however, that come under Homeland Security. I'm particularly worried about unregistered foreign agents of China.

The Department of Justice, in December, put out a revision of the Foreign Agents Registration Act that will make it much more difficult for people to take money from China and then lobby. It really tightened up the number of loopholes in the Foreign Agents Registration Act.

Mr. GUEST. Dr. Pillsbury, let me interrupt you real quick just because my time is running short. Two quick questions. No. 1, you mentioned that—about assistance that the United States is providing China.

Is there any reason that the United States should be providing China any financial support?

Mr. PILLSBURY. I'm talking about both private sector up to $2- or $3 trillion, according to Roger Robinson, of American investment in China, and then Government agencies that continue to carry out policy that was first set back in the 1970's, that, for example, the FAA in Shanghai helps Chinese airliner manufacturing to be more competitive.

The FAA's defense is, "Well, we're just making sure the airliners are safe." But, when you have something like 30 or 40 of these programs, the overall impact seems to me is worth paying attention to, that our Government is still officially helping China in many, many sectors.

You can get an idea of this by going to the U.S. Embassy in Beijing website where they list 50 Federal agencies that are present in the Embassy in Beijing, and then they hint about these are all helping China in various ways. That's what I'm concerned about.

Mr. GUEST. Thank you so much. At this time, my time has expired, and I recognize the Ranking Member for 5 minutes of questioning.

Mr. THOMPSON. Thank you so much, Mr. Chairman. Based on the testimony I've heard from all the witnesses this morning, there's no disagreement that China represents a clear and present danger to the national security of the United States.

[Nonverbal response.]

Mr. THOMPSON. Thank you.

Part of that risk associated with that danger is in the cyber field, and I'm—in my testimony, I talked about the fact that a lot of the agencies that are tasked with the responsibility of protecting the United States from China and other rogue nations, we're cutting people.

I want you to talk about whether or not we need to be improving the personnel or technology to protect ourselves. Dr. Doshi, we can start with you, and we can go down the line.

Mr. DOSHI. Well, thank you, Ranking Member Thompson, for the question. Excuse me. I'll say the following.

I am concerned that on, when it comes to staffing and manpower, the PRC is investing a lot more in offensive cyber activity and defensive cyber activity than we are. So I do worry—you noted a number of cuts, Congressman, in your testimony, in our opening statement, about cuts to DHS, CISA, cuts to Cybersecurity Review Board, cuts to the teams working on Salt Typhoon, 50 percent cuts in some of the staff—I worry that those cuts come at a time when the Chinese are investing more. That heightens our vulnerability.

So, if we have to—I would recommend stewarding those resources better for the sake of our national security.

Mr. THOMPSON. Thank you.

Dr. Pillsbury, you talked about the personnel in the embassies that China is investing in. Do you see the personnel issue a challenge for us?

Mr. PILLSBURY. Yes, I do, and one thing that really concerns me—I'm sorry if I advertise my age—but during the Cold War, beginning in 1947, the Congress and the President created new institutions to deal with the Soviet threat.

They created the NSC. They created the CIA. They created the U.S. Air Force. They created the Office of the Secretary of Defense. All of this was driven by the perception of a Soviet threat.

When you look to China today, despite all the talk, there's no new institution or organization at all that's been created to deal with the China threat.

Last night, there was a little mention of it by President Trump when he mentioned shipbuilding, and he wants to create kind-of a bureau of shipbuilding to catch up with the Chinese, who, by the way, one figure says they build 300 ships for every 1 that we build.

So, again, it's a Homeland Security kind of question. Does the Secretary of Homeland Security need a China unit reporting directly to her, and then what would it look like? How many people? This is the kind of thing I'm most worried about.

We're just doing nothing in terms of creating new institutions to deal with China.

Mr. THOMPSON. Sure. Mr. Evanina, your background in intelligence, what does that say to you about personnel and other things?

Mr. EVANINA. Yes, I would concur with my colleague's statements with respect to resources in the Government, but I would also proffer that we need just as many resources, if not more, in the private sector and academia to defend against what China's doing here.

When we have, you know, 20 of the top 30 companies in our country breached in the last year by the Communist Party of China, we have to allow and facilitate for those corporations, from Wall Street, to energy, to telecoms, to be able to best protect them against intelligence apparatuses of the Communist Party of China.

We can no longer say, "You have to get better and more efficient in the private sector." It's unrealistic to ask a company in the United States to compete and defend against a bona fide intelligence operation around the world.

Mr. THOMPSON. Mr. Singleton.

Mr. SINGLETON. I would agree. I mean, the old adage, "Personnel is policy" is true. I think there are just tremendous opportunity space for Congress to codify programs to build out that tech talent work force that we need for tomorrow.

But I also agree that enhanced private- and public-sector cooperation is essential here. The private sector is a tremendous force multiplier, particularly in the case of threat intelligence sharing.

Mr. THOMPSON. Thank you. I yield back, Mr. Chair.

Mr. GUEST. Thank you.

At this time, the Chair recognizes the gentleman from the great State of Texas, former Chairman of this committee and current Vice Chair, Michael McCaul.

Mr. MCCAUL. Thank you, Mr. Chairman. Let me first begin, Mr. Ranking Member, in saying my condolences for the passing of Sylvester Turner. I knew him well when he was mayor of Houston, and he just got elected to Congress. He and his family are in my thoughts and prayers.

Dr. Pillsbury, good to see you again. If y'all haven't read his book, "The Hundred-Year Marathon," I highly recommend it. It is the authority, I think, on China, Communist China.

You know, as you know, I prosecuted in 1997, the Johnny Chung case, which led us to China Aerospace and the Chinese intelligence apparatus putting money in his Hong Kong bank account to influence a Presidential election, that being President Clinton.

What they wanted was to get into the WTO and to get dual-use technologies, primarily aerospace and satellite technologies. Guess what? They got it, and they continue to get it today. They steal it, but we don't have to sell it to them.

Chairing the Foreign Affairs Committee, I put export controls on various things, including Nvidia chips in 2024. The problem was, in 2022, Nvidia had already sold these chips to China.

So that, along with open AI, all of a sudden DeepSeek pops up, and we realize that China now has AI technology.

In this great power competition, once again, they steal it, but then we sell it to them. I believe that that has to stop. I introduced—we saw this with the hypersonic, by the way, built on the backbone of American technology and many other apparatus of the PLA.

I introduced the ENFORCE Act to basically prohibit, through export controls, the sale of military-grade AI technology. I see no reason in the world how we could justify any company in the United States selling to China military-grade AI technology.

So, Dr. Pillsbury, in the time I have, can you respond to this? I'd like to give the bulk of time to you, but to the other 3, your opinion as to whether this is a good idea in terms of what we can legislate in the Congress, to prevent the sale of this kind of technology.

Mr. PILLSBURY. I've been focusing on what the Homeland Security Committee could do itself, very narrow picture, but there's a lot of things.

I always appreciate mentioning my book and also you alluding to the famous Parlor Maid case.

Now, this, when we talk about intelligence collection on China, one of the biggest hazards is the use of deception, double agents, against our own intelligence community.

This committee has got a wonderful website. You're putting up each of the cases like this on your website. So I just want to commend you. I don't know of other committees that are, in real time, putting up examples like this. So——

Mr. MCCAUL. When you say "Parlor Maid," that was by FBI agent, J.J. Smith, sleeping with a Chinese spy that he cultivated as an asset for 10 years who was reporting back to Beijing.

Mr. PILLSBURY. Intelligence collection is always vulnerable to deception, and in the case of China, I did a study of a lot of textbooks and books on grand strategy, how they see the world, how they see their own history. The word "deception" kept coming up over and over again.

So our problem with foreign intelligence collection, somebody can recruit a really wonderful source or place a wonderful device and get all kinds of intelligence, get promoted, get a bonus.

Then, oh, all of a sudden it turns out it's a compromised source.

In the case of Parlor Maid, what I call for in the book is the FBI should have put out a notice that the last, let's say, 25 reports by Parlor Maid probably were under the control of Chinese intelligence and were false. Xi was trying to mislead us, probably under orders from the president of China, who she claimed to be friends with.

So I'm always glad to hear you raise the Parlor Maid case. It's still with us, I think, in many ways.

Mr. MCCAUL. It's taught at Quantico with the FBI, you know.

Do you have any thoughts on the ENFORCE Act? I know it's a different committee, and I apologize for that, but this is the Congress as a whole. Would that be a smart thing for Congress to do?

Mr. PILLSBURY. Yes, I think so. But, before you came in—I hope you'll forgive me—I advocated that this committee visit China with a well-organized agenda of questions.

If the Chinese accept and give you the right people to see, you could go into the fentanyl issue. You could go into things that are in your jurisdiction, and hopefully the House Foreign Affairs Chairman would not block Homeland Security visiting China.

Mr. MCCAUL. I don't think so, but I've been sanctioned. That may be a problem for me personally.

Is it a good idea to block the sale of AI military-grade technology? Maybe just get a quick yes or no.

Mr. PILLSBURY. Yes.

Mr. DOSHI. Yes.

Mr. MCCAUL. Everyone agrees. OK. Thank you.

Mr. GUEST. All right.

The gentleman's time has expired.

The Chair now recognizes the gentleman from the great State of California, Mr. Correa.

Mr. CORREA. Thank you, Mr. Chairman.

I want to thank the witnesses here today. I really enjoyed your discussion and you brought up some very good points.

Mr. Pillsbury, Dr. Pillsbury, I love what you said about coming up with a measure of our success or what we want to do when it comes to China because I think what my colleagues have said today, you know, banning sales to China, other actions, we do this,

yet they seem to figure out how to get around these obstacles we put up all the time.

I would almost say, in football terms, they're flooding the zone, and we're chasing our own tail most of the time—not figuring it out. But actually the fact that we are chasing them is a major statement in and of itself.

So I'd love to have this Homeland Security come up with a, you know, lack of a better term, a subcommittee just to address the China issue and not just a hearing here and there.

I can't help to think that a lot of these challenges we have are self-inflicted.

Mr. Evanina, you're a former FBI agent. I would call you a patriot for all you've done. You probably could be making then, for 9/11, you could've been making more money in the private sector than you were in the FBI.

My concern is the recent firings of FBI and CIA agents. OK? A lot of you said that the issue here is personnel. They have more people dedicated to the mission than we do. Yet we just fired a bunch of people, which it sounds like they're going after them right now.

China and Russia are trying to recruit them to get them to turn over information. Not only is the issue with those personnel that we fired, but what about the Evaninas that are left in the agency? What effect does that have on their morale?

OK. You go into work not on an hourly basis. You go into work for the mission. If you think you're going to be fired, you're going to be a person who's going to be on the street tomorrow, Mr. Evanina, how would that affect your morale and your motivation to be the best?

Mr. EVANINA. Thank you, Congressman, for that question. I'm a big proponent of understanding and preventing the insider threat from being problematic, and whether it's in the Government or corporate world. From an intelligence perspective, the Communist Party of China, the Russian intelligence services, that's their job is to come over here and go around the world and recruit disenfranchised employees, whether from the Government or corporate world, and identify them as being vulnerable and recruit them to facilitate either intelligence collection, selling secrets, or selling—providing intellectual property and trade secrets on the private-sector side.

So, for me, this is a big issue because we have to be very conscious and effective as we're going to jettison Federal employees who have access to critical information, whether it be analytics or secrets, and provide them an off-ramp to identify what those signs might look like if you are solicited or approached by a foreign intelligence service and/or their proxy.

So I'm concerned about the insider threat moving forward, both in the Government and the corporate sector.

Mr. CORREA. I would argue that, even people that you fire, even if they're new to the job, these are tomorrow's experts on the subject matter. So they've gone through background checks, academic performances, some of their best—the best we have in the United States, you put them in and then you fire them?

How does that bode for us 5, 10 years down the road when we're trying to still come up with the understanding, as Mr. Pillsbury said, of the mission that we're supposed to accomplish?

Mr. EVANINA. Well, as we've seen in history, the Communist Party of China and Russia will continue to try and place individuals into our apparatuses, the intelligence community and with the Government. By doing that, they need the information, intelligence of how do we operate from our application system, our background investigations or polygraph; what does it look like in our training centers; what's the best and most effective way to get people placed in these organizations?

So all of those employees, whether they're probationary or whether they're new recruits or they're seasoned veterans, all have an impact on intelligence gathering of our adversaries.

Mr. CORREA. So, Mr. Chairman, I'm out of time, but——

Mr. MCCAUL [presiding]. Fifteen seconds.

Mr. CORREA [continuing]. The gentleman here came up with a great idea, which is to come up with a more focused approach on this issue moving forward as opposed to a hearing on this on a random basis, so to speak.

Mr. MCCAUL. Right. Good idea.

Mr. CORREA. Thank you, Mr. Chairman. Time is up. I yield.

Mr. MCCAUL. The gentleman's time has expired.

The Chair recognizes Mr. Pfluger.

Mr. PFLUGER. Thank you, Mr. Chairman.

I hope that, within this committee, we can agree that, if there's ways to more efficiently do business, that we can do that and look forward to having that conversation about the folks who are not going to be a part of these agencies anymore.

But, getting to the heart of this matter, we do have good people working inside the agencies, and this has been an important issue. Without relitigating the last 4 years, let's start fresh here.

I'll start with Mr. Singleton, talking about the Confucius Institutes. I've had a lot of legislation on this, done a lot of work on Confucius Institutes. Very worried still that the Chinese Communist Party uses Confucius Institutes and other entities to hijack our intellectual property, to steal technologies, to do a variety of things that are detrimental to us.

So what I'd like to ask you is, given the strategy of the military civil fusion, what steps do you think the United States should be taking to prevent them from exploiting academic universities and using the CI kind of strategies?

Mr. SINGLETON. Sure enough. Thank you, sir, and thank you for your leadership on this issue, as well as the RSC that I know is taking a close—a close look at this.

You know, Confucius Institutes used to number over about 120 across the United States. There are less than about 14 today, but they didn't actually go anywhere. They just rebranded and renamed themselves, and now they go by other names that are even harder to track.

What's worse is we see the proliferation of these Chinese-controlled outreach programs at the K through 12 level across the United States. Again, absolutely no coordination, control, or mandating requirement for any of these things.

Beyond the concerns about free speech encroachment, beyond some of the ideological reservations we should have about what's being taught in these classrooms and to our students, there are real research risks. Primarily, it's because when you open some of these or establish some of these research partnerships in the academic exchanges, they all come together.

So, as we looked at the foundation for defensive democracies at all of the Confucius Institute contracts, they mandate research partnerships in cutting-edge emerging fields typically between Chinese universities supporting China's military and our university system.

Beyond that, we have to be pretty concerned, I think, about free speech on campus. There's ample evidence from the FBI and others showing that Confucius Institutes are used to suppress free speech and to organize protests against speakers, including the Dalai Lama, who come to U.S. universities to speak about human rights in China.

Mr. PFLUGER. Thank you very much.

Mr. Evanina, I'll go to you on a similar topic, but on hybrid threats and the hybrid approach that the CCP takes to—where they're blending, you know, lawfare and legal and illicit activities together.

So what are the concrete steps from your perspective that we can take to counter those?

Mr. EVANINA. Thanks for the question, Congressman. I think we have to first educate and advise and make everyone aware what that looks like. Whether or not you're in a university or research institute or if you're a corporate world, you don't—they typically don't know what that hybrid set looks like—whether it's a joint venture or it's an opportunity to go in in a hybrid, inflect some cash into a start-up or a company in the Silicon Valley or Austin, Texas, there comes a talent to that.

I think we have to be more effective and efficient as a Government entity, both in the Executive branch and Congress, in educating and informing how does that look like; how does it manifest with you and your dollars to be able to educate first and then mitigate second?

Like the Confucius Institutes, universities out there are just now starting to learn a lot of these partnerships with institutes in China are problematic, and we're starting to see onesie-twosies breaking those relationships.

Mr. PFLUGER. So you mean they're taking advantage of our country, the Chinese Communist Party?

Mr. PILLSBURY. Let me count the ways——

Mr. EVANINA. Yes. Absolutely.

Mr. PFLUGER. We should be alert to the fact that they're——

Mr. EVANINA. I do think we have to, but I think the onus is on the Government to advise and inform universities and research institutions what that looks like and be more effective.

Mr. PFLUGER. Dr. Pillsbury, last 30 seconds to you. What keeps you up at night about the Chinese Communist Party taking advantage of our country?

Mr. PILLSBURY. Just to stick on this topic, the information collection from our universities is really quite dramatic. I first learned about this from FBI reports almost 15 years ago.

They go into MIT, or you name the high-tech university, to the individual professors or department chairmen and sign a right of first refusal: "I give you $3 million; you tell me when you find me"—the Chinese Communist Party—"you tell me when you find something useful in your laboratory, and you show me first."

Mr. PFLUGER. Wow.

Mr. PILLSBURY. These agreements were being signed by many universities. They did not know each—what it meant, and they didn't even consult with each other——

Mr. PFLUGER. Should Federal funding be restricted from universities that are signing agreements?

Mr. PILLSBURY. Absolutely.

Mr. PFLUGER. Thank you very much.

I yield back.

Mr. MCCAUL. The gentleman yields.

The Chair recognizes the Representative from New Jersey, Ms. Pou.

Ms. POU. Thank you, Mr. Chairman, and thank you to our Ranking Member Thompson for holding this important hearing.

Thank you to each and every one of our witnesses for your testimony and providing us with a broad array of national security threats that we certainly understand we're facing from CCP. I thank you for your candid testimony and information.

In my district in northern New Jersey, I'm proud to represent a large and vibrant community of Ukrainian Americans, one of the biggest in our country. Just last week, I met with members of this community. The pain in the voices and faces of our community members were palatable. They stressed that, in addition to being the right thing to do, U.S. support of Ukraine benefits our national security with Ukraine serving as a barrier from Russia's further advancement into Europe.

So I am deeply disturbed this week when I heard and saw that President Trump ended or wants to end critical military support to our allies in Ukraine. From weapons to satellite data, Ukraines rely on our support to continue their fight, and we can't turn our backs on them now.

So I'd like to begin, Mr. Doshi, if you would, please, when the United States retrieved—retreats from our partnership, how does that affect our ability to maintain relationships with other countries and a unified approach to countering China? How do we do that?

Mr. DOSHI. Well, thank you very much, Congresswoman. Let me start by saying that China is watching everything that we're doing on Ukraine very closely.

Ms. POU. Indeed.

Mr. DOSHI. They would be very happy if, in a fit of political dysfunction or capriciousness, we decided to cut aid to Ukraine because they think that means we won't aid Taiwan should that question be called. So our activity on this issue has implications for how China looks at the Taiwan challenge.

The second part of this I'd like to stress, Congresswoman, is also that the China challenge requires working with others. China is 35 percent of global manufacturing. We're less than 15 percent. They are 60 percent of global electric vehicle production, 75 percent of electric battery production, 50 percent of all robot installation, you know, in the world. So, for us to be able to achieve scale to compete with them, we have to do it together with others.

I do worry that some of our activity on Ukraine or some of our activities with Canada makes it harder for us to rally allies and partners to rise to the China challenge.

Ms. POU. Dr. Doshi, though, if you would also just talk about, if—you know, if you no longer view the United States as a reliable ally, how does that create opening for China to exert its influence in Ukraine and elsewhere, anywhere else?

Mr. DOSHI. Well, thank you for that question, Congresswoman.

I think that China has always been looking to split the United States and Europe. They understand and everybody in this committee and everybody testifying today also knows that China wants to displace the United States as the world's leading power, but they can't do that without breaking the United States of its allies and partners.

The top of the list is Europe, Japan, and Korea. So the more we have a wedge with our European friends—and we may have disagreements, but the stronger that wedge is, the more space there is for China, the easier it is for them to access European technology.

Take export controls. You know, we need the Dutch, the Germans and others to help us keep critical technology out of China. That is going to get harder and harder if the Europeans go their own way.

Ms. POU. Totally agree. Thank you so very much.

You know, again, Chinese President Xi and Russian President Putin reaffirmed it last week, that their partnership has, quote, "no limits."

So, Dr. Doshi, and to the rest of our members, if we have the ability to respond, how might that partnership play out in terms of China's involvement in the Russian-Ukrainian war, and how does that harm America's national security?

Mr. DOSHI. Congresswoman, this is a very important issue.

In all the talk of a deal on Ukraine, we have to consider China. There is no successful Russian war effort in Ukraine without China's support for the Russian defense industrial base and Chinese transfer of lethal material to Russia. So they are the arsenal of autocracy right now. The fact that they're reiterating their no-limits partnership at this moment is partially anxiety that we might pry them apart but also a doubling down on the Russian war machine.

Ms. POU. So I have 15 seconds. Mr. Singleton, did you wish to share your thoughts?

Mr. SINGLETON. Sure. I would agree with Russia—it's time to impose costs on the Chinese Communist Party for aiding the Ukrainian war effort. They've gotten away with far too much for the last 4 years, and I think it's time to turn the tide.

Ms. POU. Thank you. Thank you very much for that.

I yield back, Mr. Chairman.

Mr. MCCAUL. The gentlelady yields back.

The Chairman recognizes the gentleman from Oklahoma, Mr. Brecheen.

Mr. BRECHEEN. Thank you, Mr. Chairman.

Mr. Singleton, you had something that you highlighted—I thought it was extremely succinct in your introduction—that the Chinese Communist Party leader Xi Jinping talking about that the, quote, "main battlefield" is this innovation of technology.

Then, Mr. Doshi, you talked about just—you highlighted yet again that, as the United States is at 15 percent of global manufacturing, that China is at 35 percent; you said another statistic a minute ago. It was 30. So somewhere between 30 and 35 percent.

I really want to just move to—the President has implemented this tariff, and you all are talking about, you've got some strong specifics, Mr. Singleton, where you talked about breaking that down, doing more targeted things, sanctions, banning. I want to give you some time to build upon what the President is doing.

We all look at things that—you know, whether it's a tie or whether it's a coffee mug, and we're all shocked, made in China. The President, knowing that economic strength is our national security is trying to do a lot of things right now on the international front to change this.

In addition to what Mr. Pillsbury talked about—which I think is just genius—of Russ Vought at OMB, hopefully picking up that banner again and saying, what are we doing to help them, as if they have a 2 trillion gross domestic product—which they were, I guess, 20 and 30 years ago—and now they're clipping at 20 trillion gross domestic product, which somebody said is now 70 percent relative to our 29 percent—29 trillion gross domestic product, and the highest GDP relative to the United States in the world. But we've empowered them because of all these goods that we're consuming.

So how can we—I'll open this up to anybody. How can we take what the President has seen clearly, tariffs and sanctions—and there will be a cost, but because of the danger, when he's saying this is the battlefield—he wants to play this game. He wants to take our technology. He wants to have the ability through Salt Typhoon, Volt Typhoon, bring our electric grid down, bring our water systems down, military installation, ownership of farmland, how can—how can we build public sentiment to bolster our President for the American populace to say, "We may have to pay a price because this is a real, real threat"? Whoever wants to take that.

Mr. SINGLETON. I'll start, but welcome others as well. I mean, I think tariffs are really important tools of geopolitical leverage if used correctly.

In the case of China, amid economic slowdown, tariffs, unlike sanctions, they bite overnight. They cut deep. Right now China's economy is facing tremendous headwinds, reliant almost exclusively on overcapacity and its export model, which makes it ripe for sort-of sharp targeted vulnerability in terms of using tariffs.

I think we can use tariffs to actually change Chinese behavior beyond its nonmarket practices. Fentanyl is a great example. I think the President is employing tariffs in that way as a pressure tactic to achieve changes in Chinese behavior.

I think Bill mentioned it best. We need a whole-of-country sort-of approach of this, and part of that is building out different pillars to the economic statecraft, sanctions, outbound investment screening, sectoral export control bans to prevent the flow of these technologies into China's military and its defense sector. All of the sort-of pillars of American economic power working together toward a desired end-state, which I hope we would all believe is a change in Chinese behavior.

Mr. BRECHEEN. Can we do something to build upon more targeted tariff percentages? I mean, are there ways to be targeted in the way we're doing reprisal tariffs that could—I mean, this is a gross domestic product that has gained at a rapid pace in the last 20 years—ago. No one saw China coming like this 20 years ago. I see a lot of head-nodding on the panel.

Mr. DOSHI. Congressman, 2 quick thoughts. First, the administration is, frankly, considering what are called component tariffs that would make it harder for China to kind-of hide, you know, behind rules of origin. It would allow us to go after the fact that Chinese chips might be in something bigger that we buy from another country. It allows us to carve them out of supply chains.

The second point, Congressman, is actually a critical one. The Trump administration in the first term had something—an Executive Order, ICTS Executive Order, it's a regulatory barrier. It allows us to keep goods out with a regulatory ban on them. That tool should be expanded. That Executive Order could be codified by Congress.

It was something the Biden administration used, and we could keep using it.

Mr. EVANINA. Congressman, if I may, I just want to amplify both of those comments by saying a little bit different perspective about amplifying the message and the why matters.

I think, when we talk about tariffs and economic drivers, I think we have to message the American people why this all matters. Because, in our generation, we look at it culturally, the Russians, the Cold War, they were bad. We beat them in 1980 in the Olympics, right? We had the Ayatollah in 1979; the Iranians culturally were bad.

We have not had that with the Chinese Communist Party yet. So, culturally, across our country—and I'll proffer to you, in Oklahoma, our constituents don't see China in the same light as we saw Iran and Russia. I think we have to do a better job, more effective at driving the issues as why this stuff matters.

Mr. BRECHEEN. Thank you, Mr. Chairman. I yield.

Mr. MCCAUL. The gentleman's time has expired.

The Chair recognizes Ms. McIver.

Mrs. MCIVER. Thank you so much, Mr. Chairman, and to my Ranking Member, and thank you to our witnesses for joining us today.

Under the pretense of promoting efficiency, Elon Musk's DOGE team has acquired unmatched control over critical Government databases and technology systems. These systems house sensitive information, including private data on Federal employees, Government contracts, regulatory investigations, and even the personal information of everyday citizens.

Equally concerning are Musk's close ties with China and his boundless access to and influence over U.S. Government agencies and systems. These dynamics raise serious questions about national security, data privacy, and the integrity of our Federal operations.

I look forward to hearing from the witnesses today as we work to ensure transparency, accountability, and the protection of American interests. With that, I have one question for each witness.

The intelligence community's 2024 Worldwide Threat Assessment highlights China as the most active cyber threat. How might the Trump administration's reduction in CISA personnel affect the Nation's ability to defend against these threats? Mr. Doshi—Dr. Doshi, you can start.

Mr. DOSHI. Sure. Thank you, Congresswoman. It's an important question.

What I'll say is that—and as I mentioned, China invests heavily in personnel for offense and defense. That gives them significant advantage. They've got 1.4 billion people; we have 350 million. Labor does matter in this business.

What I'd like to see is us increase our Federal work force when it comes to cyber, both offense and defense. Right now I do worry that the cuts are coming at the wrong time. Right now we're learning about Salt Typhoon, Volt Typhoon, compromise of critical infrastructure, telecom. Every single day there's something new. We need to be scaling up, not scaling down. That's what I worry about.

Mrs. MCIVER. Thank you so much for that, Dr. Doshi.

Mr. Singleton.

Mr. SINGLETON. I think it's important that we have the right personnel in place. I'm not an expert on CISA or the reductions in staff in force there. But I actually think that we also need to be thinking about building up that tech talent work force in the private sector as well.

I think this is where Congress has a really important role to play, both to incentivize private companies to hire and invest and train their own talent work force, but to think about how we want to maybe not rely so much on the Federal Government to solve all these problems but look to the private sector to do the work for us.

Mrs. MCIVER. Thank you. Anyone else want to chime in?

Mr. EVANINA. I would amplify that in respect with—I don't—fidelity on the cuts, per se, or what you reference. But I do say that I put most emphasis on our ability or inability to protect the Communist Party of China in our private sector, in Wall Street, in telecommunications, in energy, academia. We need to be more effective and efficient how we drive protection measures out there, which is the main battlefield for Xi Jinping, versus being so concerned about personnel in the Government.

Mrs. MCIVER. Well, you can't do that without people.

Dr. Pillsbury.

Mr. PILLSBURY. I agree with you. The homeland security assessment you mentioned, I believe, from committee staff is manned by 800 people. I agree with you that there's actually 3 sentences in the assessment that say China is the greatest threat.

But the bulk of the work is not China. It's all kinds of other threats. So looking at personnel issues, I just wonder if the com-

mittee could write a letter to that unit and say, "Why do you have 800 people? How many are working on China, the main threat you say yourselves versus other things?"

The personnel is very, very important. That's why I was advocating we need some kind of new unit in our Government that keeps track of the competition with China. We don't have it now in any—in any department.

Mrs. MCIVER. Thank you so much for that. I agree.

With that, Mr. Chairman, I yield back.

Mr. MCCAUL. The gentlelady yields back. The gentlelady from South Carolina, Mrs. Biggs, is recognized.

Mrs. BIGGS. Thank you, Mr. Chairman, and thank you to our witnesses for being here today.

The digital age has illuminated our world with unprecedented connection fueling American prosperity and transforming our very way of life. This very connectedness has also cast long shadows. We're building vulnerabilities that our adversaries, most notably the People's Republic of China, are determined to exploit.

For too long, we have witnessed their calculated and often aggressive drive to seize control of critical technologies, especially within the vital arteries of our telecommunications sector. The insidious and encroaching influence of the Chinese state-owned telecom enterprise Huawei over global 5G infrastructure is not merely a business concern; it is a direct assault on our national sovereignty.

Their control over these networks creates the potential for digital back doors, a silent invasion of our communications networks, a potential weapon against the very fabric of our free society.

Furthermore, Huawei controls approximately 30 percent of the global telecommunications market and is the dominant telecommunications provider in many countries acting as an arm of the Chinese Communist Party. This market dominance creates a dangerous scenario where unchecked growth equates to increased opportunities for Chinese espionage.

Imagine a scenario where sensitive Government communications, critical infrastructure control systems, or even personal data are compromised through these digital back doors.

As we have learned today, represented by events like these outlined in our witnesses' testimonies, this threat is a stark reality. The potential for compromise is not merely theoretical but a documented capability, a chilling testament to the danger posed by unchecked access to our vital communications networks.

So my question is to Mr. Singleton. Is it fair to say that we are now in global arms race with China over control of telecommunications infrastructure?

Mr. SINGLETON. Thank you for the question. I absolutely believe we're in a global arms race with China as it relates to emerging technologies but particularly telecommunications.

As a result of the tremendous work done by this committee, the Biden administration, and the Trump administration, Huawei is down, but it's certainly not out. I think even just last week the CEO of Huawei sat front and center in a meeting with Chairman Xi Jinping in Beijing to talk about China's role in emerging technologies. I think that right alone is a signal of positional power for

Huawei and the important role Huawei plays in China's industrial policies.

I think, to borrow a phrase from the Biden administration, I think there's both promote opportunities and protect opportunities here. We really need to be thinking about Western coalitions of telecommunications companies that can provide alternative telecommunications gear and systems to both countries here but abroad, but also enhance export controls, particularly through acts like the ENFORCE Act, to cut off Huawei from advanced semiconductors AI equipment. I think that dual approach is actually what's going to be needed here to protect communication systems going forward.

Mrs. BIGGS. Do you agree that the United States has a national security interest in ensuring that the global telecommunications core infrastructure is not controlled by a hostile state actor like Huawei?

Mr. SINGLETON. I think it's probably the defining challenge of the 21st Century. It's going to be figuring out who controls the means of communication, whether it's TikTok, whether it's telecommunications networks, whether it's basic standards for emerging technologies.

That will probably be the defining challenge, and whoever wins will control the drivers of the 21st Century industrial revolution.

Mrs. BIGGS. Just one more thing. So, with your—in your professional opinion, what do you think the new Trump administration—what could we do about that?

Mr. SINGLETON. Rush mentioned codifying OICTS. I think that's a tremendous move. The America First investment policy that the White House released about 2 weeks ago was a tremendous road map and offered so much opportunity for Congress to be thinking through codifying through law steps, whether it's outbound investment screening, enhanced export controls, severing China's ability to make greenfield investments in the United States to purchase farmland.

I think it was the road map that Congress could follow, and I think there would be tremendous bipartisan support for nearly every single one of the measures in that policy.

Mrs. BIGGS. Thank you very much, and I yield back.

Mr. MCCAUL. The gentlelady yields back.

The Chair recognizes the gentleman from Michigan, Mr. Thanedar. I hope I got that right.

Mr. THANEDAR. You did great. Thank you, Chairman.

Thank you, Ranking Member, and thank you for our distinguished panel here for coming and expressing your views and opinions.

So the CCP has been seeking to exploit American openness in order to steal economic secrets and undermine our national security. I'm particularly concerned about the access currently President Trump and Elon Musk have given to DOGE, unfettered access to sensitive information systems containing information about the inner workings of the Federal Government and millions of Americans, a lot of privacy, data of many Americans they have access to. I believe they are young 19-, 20-year-old who have not been vetted or has gotten any kind of security or screening.

So it is unclear whether or how this information that is given to DOGE is being safeguarded, and how would we ensure that such information doesn't fall into the hands of our adversaries like China, which is particularly troubling given Elon Musk's close ties with China, his many business ventures in China?

How—what kind of firewall there is to protect the information that's been freely flowing to the DOGE; and, specifically, I think I want to ask Dr. Doshi, can you explain how China's access to this sensitive information, information about American citizens—you know, I've been talking—having town halls in Michigan, talking to, you know, hundreds of my constituents, and they're very concerned about their private data, their Social Security numbers, their buying habits, whatever information that they have falling into the wrong hands. You know, they're already concerned about that information being freely given to DOGE. Now we don't know where else it's going.

So how would that impact our, you know, U.S. security from your viewpoint?

Mr. DOSHI. Well, thank you, Congressman, for the question.

I'll start by saying this. China is the most formidable cyber actor the United States faces, bar none. It's the most formidable. It has mounted a multi-decade campaign to steal our personal data for counterintelligence purposes successfully, our intellectual property, as we've discussed, again, quite successfully—they're still doing it—and to penetrate our critical infrastructure to cause us harm.

So, when we think about the situation we're in now, the U.S. Government has already been compromised multiple times. I do worry, though, that, you know, if we move fast and break things in some of these systems, it's possible we're giving adversaries additional vectors to compromise additional information. I think Americans understand the China challenge in abstract as Members of this committee know well. It's also useful to make it concrete to them.

The concrete risk here is that cyber actors will have their personal data and use it potentially down the road, especially if they're members of law enforcement or members of government, Federal Government, for blackmail purposes. That's something we want to avoid.

Mr. THANEDAR. Well, what can we do—and this is for anybody on the panel. What can we do to use technology to safeguard this data that we have? I know blockchain technology has been used in the crypto markets. But that technology has wide applications outside of the crypto industry.

Can such a technology be used to safeguard some of the data?

Mr. DOSHI. I'll start really quickly with just one or two ideas. I think technology is partly the solution to the problem that we have. Regulation is some of it. Personnel some of it. Tech is part of it, too, in 3 dimensions.

First, we should use better encrypted communications at the Federal level. We are not really up to speed on that. Second, we should make sure that the vendors we rely on, like Microsoft and Amazon, are not doing business in China in ways that undermine the security or the products that the Federal Government uses.

Then I think, third of all, we have to seriously consider moving certain communications to Classified spaces.

Mr. THANEDAR. Thank you so much. My time is almost up, so I yield.

Mr. MCCAUL. The gentleman yields.

The gentleman from Pennsylvania, Mr. Mackenzie, is recognized.

Mr. MACKENZIE. Thank you, Mr. Chairman, and thank you to all of our panelists today, an incredibly important topic that we're discussing, the threat posed by Chinese Communist Party to the United States and our national security.

We've talked about a lot of important issues, the cyber intrusions into critical infrastructure, the pernicious use of social media, and also the work that a party—the Communist Party of China is doing to embed themselves into America's education system.

One thing that I would like to talk about and focus on that I don't think we've maybe hit on enough here today is the defense industry for America and what the Chinese Communist Party is potentially doing to target our contractors and those in the defense industry.

We heard a little bit earlier about the theft of intellectual property, but what I have seen is that the Communist Party of China is investing in certain companies that seem to me to be strategic investments and sometimes parent companies where then the subsidiaries or part companies of those larger entities are actually providing defense investment and equipment and technology for our U.S. military.

So I would like to hear from any of the panelists if they have seen this kind of activity and what their thoughts are on what we should be doing to address it.

Mr. EVANINA. Congressman, thanks for that question. I think that's a very deep and introspective question about the commonplace and the tactics the Communist Party have used, not only in the corporate sector but the defense industrial base.

I think the way you laid out that scenario is commonplace. I think if you see one example of that, whether it be a subsidiary—a supply chain vendor, you're going to see that a thousand times across the—it's true to their form how they do it, how they penetrate, how they facilitate. They get access, whether it be architectural plans or just access to an IT system. It's commonplace.

I think, with respect to understanding how that works, how does it manifest, we have to be more effective and efficient with their defense industrial base, big companies, and have them force similar cyber hygiene practices all the way down through their supply chain, be able to prevent that from happening again and again.

We just saw recently some cases in the news where you had the small vendors who are supplying critical technologies to defense industrial base who were being owned and operated by a Communist Party of China personnel. That's simple due diligence we could be more effective and efficient at defeating.

Mr. PILLSBURY. I'll try to get to you, Congressman Mackenzie, a couple of things. One is a copy of President Trump's book in 2015 when he laid out the sophistication that he had observed with Chinese companies. They don't always give their real names when they come shopping for things in our country.

Second, there's a young scholar at SIIS here in town, just finished a book. I heard the briefing on it. The Chinese often have 5 or 6 layers of institutions, legal entities. It could be in the Bahamas, or it could be in Malta. When they do cyber espionage or when they buy and sell American companies, they can hide behind these 5 or 6 layers.

So this young scholar is trying to see how many of these layers can be detected through our own cyber operations. But the issue in—he wasn't President then, but the issue in his book, "Great Again," was just how sophisticated the Chinese are. He tells stories of his own efforts to have Trump company products made in China. He doesn't say it, but I think he lost money, and he doesn't like that kind of thing.

Mr. SINGLETON. I would just add that sometimes people are the problem. It's pretty concerning that there's a lack of post-employment restrictions on DOD and IC officials. They can go work for Chinese companies and maintain their security clearances after employment. They can lobby on behalf of Chinese companies or companies that have major investments in China. That's totally permissible and allowed today.

I would argue this is probably an opportunity for legislation to come up with post-employment restrictions, a real review on security clearances, and maybe you shouldn't be able to hold a security clearance and then benefit from that security clearance while you represent or advance a Chinese company's interests.

Mr. DOSHI. Congressman, I would just add, if I may, maybe 3 quick things. First, beneficial ownership. Knowledge is important for law enforcement. There's—Corporate Transparency Act could help us get at their shell companies that are acquiring parts of our defense industrial base.

Second, on the cyber side, there's a lot more that we need to hold our companies to do in contracting. Finally, you know, CFIUS is a tool that we need to expand for this purpose, particularly with venture.

Mr. MACKENZIE. Great. Well, I want to thank all of the panelists for that information and suggestions that they offered because, again, I have seen this myself in several instances, and I find it very concerning.

So I think that we should be doing more to address this across the entire spectrum of America's economy, but particularly when it comes to the defense industry.

So I just want to thank all of you again for joining us today and for your responses.

I yield back to the Chairman.

Mr. MCCAUL. The gentleman yields.

Chair recognizes the gentleman from Rhode Island, Mr. Magaziner.

Mr. MAGAZINER. Thank you, Chairman McCaul and Ranking Member Thompson.

Before I begin, I just want to recognize the empty chair on the dais and offer my condolences to the family, the friends, and the constituents of Congressman Turner. Although we were only colleagues here on the committee for a short time, I know that he left a legacy of a lifetime of public service and impact in his home city

of Houston. Our thoughts and prayers are with him and his family today.

On the topic of today's hearing, the Chinese authoritarian government continues to launch aggressive attacks against the United States, including but not limited to offensive cyber operations, targeting critical infrastructure, transnational repression, industrial espionage, and more. The CCP has worked to infiltrate our most sensitive sectors, including the energy grid in our communications networks, creating high-risk vulnerabilities in a time of crisis.

These cyber attacks against the United States also include the illegal pursuit and theft of American intellectual property. The theft of trade secrets through industrial espionage, coercion, or joint ventures poses a serious threat to the U.S. economy, erodes our competitiveness, and most importantly, costs Americans jobs.

China's theft of our intellectual property has been allowed to undercut American businesses, impacting our work force, and undermining our national defense. The Chinese government also continues to suppress dissent outside of its borders through a range of coercive tactics, including surveillance, harassment, and even violence.

The CCP's long arm of repression has real implications for the fundamental freedoms and human rights that we uphold as a Nation.

Unfortunately, the Trump administration continues to strengthen China by insulting our allies, undermining NATO, launching expensive trade wars against Mexico and Canada and now other American allies, and surrendering the developing world to China by shutting down USAID. Donald Trump and Elon Musk's destructive elimination of USAID is not only creating a series of humanitarian crises; it plays right into the hands of the CCP, driving strategically important countries away from the United States and into the waiting arms of China's Belt and Road Initiative.

Similarly, Trump and Musk's shameful cuts to our national security and cybersecurity agencies makes us less safe. They have made reckless personnel cuts and pressured public servants to resign at CISA, the Central Intelligence Agency, the FBI, and the Defense Department. All of these agencies and departments are critical for protecting Americans against CCP aggression, preventing cyber attacks and attacks on our infrastructure, and holding Chinese agents in the United States accountable.

Dr. Doshi, can you comment on the importance of Americans' soft power and the importance of maintaining relationships, particularly in the developing world, in this global contest that we have with the CCP and the dangers that come from repelling those nations away from the United States and into the waiting arms of the Belt and Road Initiative?

Mr. DOSHI. Well, thank you for the question, Congressman.

I'll answer in 2 respects. First, I'll talk about, I think, the Global South, if you will, and then maybe the rest of our allies and partners. On the Global South portion, you know, China has learned from the first trade war. What they're trying to do now is do better in the second potential coming trade war by relying more on exports of developing countries than to the United States and the

West. So they're relying more on Latin America, Africa, Southeast Asia, and other parts of the world to import their goods.

Now, that's a challenge for us because if we want to be able to really bring leverage to bear, we don't want them to be able to find market share elsewhere around the world. So how do we stop that?

Well, we have to be players in the developing world. We have to either bring aid or tie that aid sometimes to vendors implicitly. We have to make sure that we're active. It is possible that some of these cuts in some of these places can undermine some of those efforts.

Mr. MAGAZINER. If I could, just because I don't have a lot of time left, I want to give an example just to illustrate this for my colleagues here and for anyone who is listening.

I have a factory in my district that makes a peanut paste called Plumpy'Nut. It's used to save the lives of children who are starving. It's a high-protein paste.

They received a stop work order from DOGE, from Elon Musk. Their contracts were canceled. A month later, finally, as children were dying around the world, their contract was restored, but they still have not been paid yet. They are owed millions of dollars.

Meanwhile, we are relying on the developing world for critical minerals, for intelligence gathering, for trade, in competition with China, and we are letting their kids starve because some kid behind a computer screen here in Washington is cutting off life-saving aid, shooting ourselves in the foot, and strengthening our adversary China.

I yield back.

Mr. MCCAUL. The gentleman yields.

The Chair recognizes the gentleman from Tennessee, Mr. Ogles.

Mr. OGLES. Thank you, Mr. Chairman. Just take a moment to offer condolences and thoughts and prayers to the Turner family. Again, briefly our colleague, but a gentle soul and a kind man, and he will be missed.

Mr. Pillsbury, you coedited the Heritage Foundation's report, "Winning the New Cold War: A Plan for Countering China." It notes that there is growing evidence that Beijing is co-opting divisive ESG and DEI initiatives to undermine U.S. competitiveness.

What do you believe are the implications of those efforts?

Mr. PILLSBURY. Well, they're very scary. If they succeed, we lose our global primacy. We lose all of the benefits of being the world leader, and I doubt that we can get it back.

Mr. OGLES. Well, you hit on an important point. I think sometimes we get distracted with the media cycle and perhaps what's going on in the European Continent, which is important, of course. But, when we look at the existential threats to the United States and our supremacy globally, whether that's militarily or economically speaking, would it be fair to say—or at least it's my assessment that China would be the adversary that we should be most concerned about. Your thoughts?

Mr. PILLSBURY. Yes, I think so. The good news I've just learned in the past hour at this hearing is that, having lost the election, the Democrats now seem to have a new theme, which I had not heard before. We Democrats are tougher on China than you Republicans. There's a defense, I'm sure, but the fact that this is an issue

to attack Republicans really shows we have some hope for our country, that we're going to have a bipartisan approach.

Mr. OGLES. It's now a bipartisan issue, right? I mean—but, again, I want to focus on this issue. You know, we talked about—you hear about the Belt and Road Initiative on investment in foreign countries and how China is, quite frankly, coopting governments around the world with their Belt and Road Initiative.

Yet, some of the foreign aid that is being griped about that is being cut is for gender fluidity in some far-flung crap hole country that nobody cares about, and, quite frankly, they're offended that we're there.

So as we start to prioritize where we're spending our money, I think we think about homeland security. We think about our lethality. We think about our dominance in the economic and military sectors.

So—but I want to get back to China and DEI. While the Chinese Communist Party delights in the spread of ideologies like DEI; they weaponize it against us, throws it in our faces. We can't forget how they opened their engagement with the last administration by grandstanding about the Black Lives Matter movement at a meeting with Secretary Blinken in Alaska.

Meanwhile, the CCP is literally cutting the organs out of the Falun Gong practitioners. They have concentration camps for the Uyghurs and other religious minorities. After they kidnap and abuse Uyghur men, they send CCP officials to their homes to rape their wives and make their children sit with them for dinner and call them dad. They demonically call this the Pair Up and Become a Family program. The CCP's wickedness is hard to fathom.

Mr. Pillsbury, your written testimony encourages us to expose China's corruption, censorship. You specifically mention a Bloomberg news article about the Xi Jinping's family's wealth. Why do you think the CCP is so sensitive about the wealth of its leadership?

Mr. PILLSBURY. What I advocate in my testimony has to do with the ruthless nature of power politics at the top in China. We know this from a lot of disclosures that happen after somebody gets killed, or, in one case, when Kissinger was making his second visit, October 1971, a large number of generals and senior officials had been executed or put in prison, and we did not know about it. This continually happens.

There's a book last year by a British diplomat named Roger Garside called "Coup"—coup d'état. He implies that the current Prime Minister of China could launch a coup against Xi Jinping, and he even opens the book with how that might happen. Now, the Prime Minister suddenly found himself out and dead of a heart attack, but high-level politics in Beijing, we have to keep track of it, and we have to know what is going on that affects our interests.

This is one of the things I advocate. I got this idea, frankly, from President Trump, who once raised the issue: Our politics is in the newspapers every day. Can someone tell me about what Xi Jinping is worried about?

It's very hard to do that. We need to spend more time on it.

Mr. OGLES. Yes, sir.

Mr. Chairman, I just want to say, as we look to our homeland, as we look to our initiatives abroad, we have to think in terms of what's in it for us. So, whether it's the minerals deal in Ukraine, whether it's deals and programs in Latin America or South and Central America or Africa, we've got to put America first. We need to support our President and put our country first.

Mr. Chairman, I yield back.

Mr. MCCAUL. The gentleman yields.

The Chair recognizes the gentleman from California, Mr. Swalwell.

Mr. SWALWELL. Thanks, Chair. Thanks for having this important hearing, and also thank you for acknowledging the loss of our colleague, Mayor and Representative Turner. We're going to miss him and his spirit.

On this topic, I actually don't disagree much with what my colleague from Tennessee just mentioned. I want to ask the witnesses here, as it relates to China, do you agree that, unlike almost any intelligence service in the world, including ours, that they task their intelligence service to steal intellectual property to benefit Chinese businesses? Is there anyone here that disagrees with that?

Mr. PILLSBURY. Sir, I would just add one thing.

Mr. SWALWELL. Yes.

Mr. PILLSBURY. I think they're almost unique in the world in tasking the MSS to do this. Most intelligence services in the world are spying on government secrets, not trying to build up the national champions.

So, in many ways, we can tip our hat that the Chinese intelligence service is working for the national champions, unlike the world's other intelligence services.

Mr. SWALWELL. But I don't think you're suggesting that the CIA should be stealing secrets to help Cisco?

Mr. PILLSBURY. I think they would resign.

Mr. SWALWELL. So does everyone here agree that our greatest economic foe in the world is China?

I think there's agreement here.

Just by a show of hands, who here would support defending Taiwan militarily if China militarily invaded Taiwan? So would I, and so would a lot of my colleagues on both sides of the aisle.

I raise that because my colleague from Tennessee also referenced Ukraine and the minerals deal there. What concerns me about the state of play in Ukraine on this very important topic is that, if you are Taiwan right now, you should be very worried about us possibly leaving our friends in the field in Ukraine.

If you're Taiwan, you're probably asking yourself, could the United States stitch together an alliance to actually defend us?

Because, if China were to militarily invade Taiwan, sure, it's in our interest to defend Taiwan. Maybe there's a couple other countries in the region who may have an interest. I don't know why Europe would want to get involved, unless it was strong American partnership and strength and allyship that persuaded them to do that.

So, to my Republican colleagues, I guess I just warn that we can't be tough on China but soft on Russia, because China won't believe us. They will actually think that we wouldn't really honor

our commitment to Taiwan and that the rest of the world wouldn't go with us because we would have a credibility deficit on that issue.

As it relates to Ukraine, I also just want to note that the return on investment is probably the greatest military return on investment the United States has ever spent. I don't want to discount how much money we have spent. It's a lot. But most of the money has gone to factories in Texas and Ohio that create American jobs benefiting American companies, and the number of soldiers lost is zero.

So you could say the return on investment is infinity because you cannot divide zero.

So these 2 issues are directly related, and I hope we don't separate them because I want to be tough on China and tough on Russia, and I'm afraid you can't be tough on one and soft on the other.

Mr. Doshi, what is the state of play right now as it relates to Chinese, whether it's state-sponsored or individuals that they harbor in their country as far as cyber attacks that are not just stealing intellectual theft, but also ransomware or phishing or denial of service attacks on U.S. companies?

Mr. DOSHI. Well, thank you, Congressman.

In the last decade, China has become the world's most capable cyber actor. I think you could argue, before that, it was Russia; now it's definitely China. When it comes to taking American personal data, intellectual property, or prepositioning for cyber attack with web shells or living-off-the-land techniques, they're the state-of-the-art, and they're investing more resources, more staff, and more personnel to be the best at it.

Mr. SWALWELL. Really quickly, Russia, obviously, has a lot of independent cyber actors who are just financially benefiting themselves.

What—inside China, would you have the temerity as an independent actor not associated with the Government to attack the United States? I don't hear much about, like, that environment.

Mr. DOSHI. Very quickly, China has a number of independent cyber actors, but they usually are contracted by the government. They don't usually go rogue on their own.

Mr. SWALWELL. Thank you.

I yield back, Mr. Chair. Thank you.

Mr. MCCAUL. The gentleman yields.

The Chair recognizes the gentleman from Colorado, Mr. Evans.

Mr. EVANS. Thank you, Mr. Chair, Ranking Member.

Thank you, of course, to the witnesses for taking your time to come and have this important conversation with us today.

I spent 22 years in the military and law enforcement, 12 years U.S. Army, another 10 years as a local police officer. The district that I represent is really an intersection of a lot of things that are critical both in that public safety space and that national defense space, particularly—and we'll start off the conversation with critical infrastructure like energy. I represent the fourth-highest energy producing county in the Nation: oil, gas, wind, solar, geothermal. We've got nuclear fuel rods in the district.

So the first question to Mr. Evanina is, we know that the CCP is engaged pretty heavily in cyber espionage and attacks on critical

infrastructure. Can you comment on how we're currently postured to be able to defend against those attacks and what the road map going forward looks like to be able to protect our critical infrastructure and energy production?

Mr. EVANINA. Congressman, thanks for the question. I concur with your assessment of Colorado.

Back in 2017 and 2018 when I was director of the National Counterintelligence Security Center, we identified Colorado as not necessarily phase line zero but a critical element, specifically the I–25 corridor, we saw—this is going to be a perfect example, a road map for how China is attacking our critical infrastructure from north to south in Colorado because of those critical entities you referenced. We said, because they're doing this here in Colorado, we are now going to map that across our Nation because what China does very well is mimic their successes.

Because they were successful in Colorado, we said, "Let's look at how they're doing this across the ecosystem whether it be in Austin, Texas, California, Boston," and we saw the same type of activities in critical infrastructure that we saw in Colorado.

Second part is I think we have to be more effective and efficient at making aware how this threat manifests in critical infrastructure. As you know, 85 to 90 percent of the critical infrastructure is owned and operated by the private sector. They don't get that top secret intelligence or critical intelligence. We need to be more effective in declassifying, getting known and collected intelligence from the CIA, NSA, and FBI to those people who own the critical infrastructure so they can create and mitigate some of the cyber activities they see in their networks.

Mr. EVANS. Thank you for that. Then, kind-of pivoting off of that topic, still around critical infrastructure, Mr. Singleton, we know that one of the key challenges that's facing us is just the ability to build that critical infrastructure, to have that manufacturing base and to have those supply chains protected with sources that are not controlled by the Chinese Communist Party.

So, again, for my district, being very energy-heavy, one of the big concerns that we have is, if we don't have the energy to actually be able to fuel and provide for American manufacturing and American infrastructure in the United States, well, we know that China does not have anywhere near the environmental regulations that we have, and they're bringing on just an incredible number of coal-fired plants using slave labor and outright terrible methods to be able to fuel their grid.

Can you just comment on what we need to be able to do in the United States, particularly in the energy generation space, to make sure that we have sufficient energy to be able to compete with the Chinese Communist Party and their absolute disregard for the environment and how they fuel their grid?

Mr. SINGLETON. Absolutely. Thank you for that question.

I mean, I don't think we can be our own worst enemy here. I think that we've, unfortunately, taken a number of steps to make it very difficult to even mine or certainly process rare earth materials here in the United States. Until we work through some of those regulations, I would say we're fighting our—with one hand tied behind our back.

Mineral stockpiling may be a solution there, but I think there's a lot of work to be done in Congress to get there. I think, ultimately, we're going to have to be incentivizing and thinking about select investments in new energy systems and structures and companies to help scale them and working with partners and allies.

I think we've all mentioned here that the Japanese, the Koreans, the Australians, certainly companies here in the United States, all want to work together to build out this safe, secure ecosystem of energy systems and structures. We should be incentivizing that. I think we can lead there. It's an area where we can actually diffuse some of the costs amongst our closest allies, or we can actually share some of the sensitive information that goes into those types of systems.

Mr. EVANS. In my remaining 30 seconds, just around batteries, we have an incredible reliance on batteries and the battery supply—you know, the battery supply chains.

Can you comment on how we can better protect our battery production and storage systems here in the United States?

Mr. SINGLETON. China is a champion in battery energy storage solutions. These companies, particularly CATL, are mainlined into our electrical grid today across the United States, and the number of partnerships between CATL and U.S. utilities is only increasing. This is insanity, not just because CATL is ostensibly private but responsible to reporting to the Chinese government, but, because as we've talked about today, they serve as vectors into our critical infrastructure and supply chains for cyber attacks and espionage.

Mr. EVANS. Thank you. I yield back.

Mr. MCCAUL. The gentleman yields.

The Chair recognizes the gentleman from New York, Mr. Goldman.

Mr. GOLDMAN. Thank you, Mr. Chairman.

Again, I'm very glad we are having this hearing. Once again, I note the complete disconnect between this hearing and its purpose and what the Trump administration is doing.

Absolutely, we need to address China and do it on all fronts, cyber, economic, military, diplomatic, in all ways. But, when the CIA sends an unclassified email to the White House listing names of employees hired over the last 2 years, including a number of China-focused analysts, whose identities, of course, are heavily guarded from Chinese hacks, that compromises significantly our ability to conduct intelligence, gather intelligence, and push back against China.

Mr. Evanina, I know you were the director of the National Counterintelligence—NCSC—I forget what it's called—but the notion that probationary employees are somehow disposable seems to me at least to fly in the face of how our intelligence community works. Because am I correct that, in those early years, you often have extensive language training and extensive additional training to prepare you to go out in the field and successfully execute your job? Is that a fair assessment?

Mr. EVANINA. Yes, Congressman.

Mr. GOLDMAN. You know, I know Director Burns recently, when he took over at the agency, really tried to beef up hires related to China and those who speak some of the Chinese languages. He ac-

tually increased the agency's budget from 9 percent devoted to China-related analysis and espionage to what it is today, which is closer to 20 percent.

So, am I correct, Mr. Evanina, that, if an unclassified document is sent to the White House that includes the actual names of CIA employees, that significantly jeopardizes their ability to continue to do the clandestine intelligence work that they are charged with doing? Is that accurate?

Mr. EVANINA. Congressman, I'm not familiar with the fidelity of that issue, but if it's an unclassified report of individuals who are under cover, who have cover on them, and it's provided in the wrong hands at the White House, those who don't need to know, it could potentially cause problems, yes.

Mr. GOLDMAN. Right. Of course, we know, and I think you said in your opening statement, that China's hacking of Americans' personal data is wide-spread and extensive. I believe you said there are 50 percent of Americans have had personal data stolen by the CCP.

So what does that mean for the possibility that unvetted, non-Government officials can get access to every single American's personal identification information through the Treasury Department or the Social Security Administration, and potentially place it on unclassified servers?

Does that expose Americans' personal identification information to China's hacking and cyber-warfare efforts?

Mr. EVANINA. Obviously, in that situation, but I would proffer, Congressman, as I referenced, almost every American has had all their personally identifiable information already taken by the Chinese.

I think the concern you reference is hypothetically, if those is merged with individuals who are potentially under cover and matching person A with that data.

Mr. GOLDMAN. Right. I think that's incredibly important. So the notion that we're having this hearing and talking about beefing up our efforts to address China, to countering threats posed by the CCP—and I want to be clear, when we say "China," we mean the CCP—to our national security, and yet what the Trump administration, what Elon Musk are doing is undermining those efforts.

In fact, there's reporting even that some of the people who have been fired with security clearances or probationary employees are now being recruited by Russia and China to be agents themselves.

We know about Elon Musk's significant conflicts of interest in China with his own businesses, part of which influence—maybe have influenced his opposition to the budget bill that we agreed, in a bipartisan way to pass, in December.

So, Mr. Chairman, I would just urge you and your colleagues on the other side of the aisle to take this focus and this concern and bring it to the administration so that they can join you in bolstering these efforts, rather than undermining them.

I yield back.

Mr. MCCAUL. The gentleman yields. That concludes this hearing, and I'd like to enter into the record the closing statement by Chairman Mark Green, who is sick today. We hope he gets better.

[The statement of Chairman Green follows:]

STATEMENT OF CHAIRMAN MARK E. GREEN, MD

MARCH 5, 2025

Before I close, I want to express my sadness on hearing of the tragic passing of Mr. Turner. His family and loved ones are in our thoughts.

I want to thank our witnesses for sharing their insights with the committee in today's hearing. The first step in dealing with a threat is understanding the nature of that threat.

The threat from the CCP is comprehensive in its scope, extending throughout our society, our businesses, our universities, and our cyber networks.

The CCP's goal is nothing less than replacing the United States as the leading geopolitical and economic power in the world. Its approach emphasizes infiltration and influence within critical sectors of business, infrastructure, and academia to obtain long-term advantages.

The extent to which our adversary has managed to extend its reach and capabilities is disturbing and unacceptable.

Intellectual property theft in the past decade has stolen American research and innovation for the benefit of the CCP's technological ambitions.

Critical infrastructure has emerged as a major target of the CCP's efforts to exploit American vulnerabilities right here in the United States.

In recent years we have experienced large-scale cyber attacks such as Salt Typhoon and Volt Typhoon that targeted critical telecommunications networks.

We also continue to see the CCP and its associated corporate entities seek to embed within physical infrastructure such as transportation and supply chain networks, giving the CCP a route to engage in surveillance or potential disruption of such networks.

In times of heightened geopolitical tensions with the PRC, such vulnerabilities could be ripe for exploitation. This isn't simply about data theft—it is strategic positioning.

Leaders in the Federal Government, the private sector, and higher education need to be vigilant and proactive in countering the threat of the CCP's malign influence.

We cannot afford to be complacent in our competition with the CCP.

Today's hearing shows us that the threat within the homeland is much more extensive than many realize.

It touches on supply chains and critical infrastructure networks that we rely on every day, and it threatens to erode America's advantages in technological advancement and innovation.

Here in the Committee on Homeland Security, we will work on increasing our ability to understand, assess, and mitigate the wide range of CCP activities within the homeland that undermine our national security.

Today's hearing is only the start to our work over the next 2 years to counter the threat of the CCP.

This threat is one of the most critical strategic challenges that the United States faces in the twenty-first century. I appreciate our witnesses for their thoughtful and informative engagement with us throughout today's hearing.

Mr. MCCAUL. I just want to give a few closing remarks, but if the Ranking Member has——

Mr. THOMPSON. Yes.

Mr. MCCAUL. Let me recognize the Ranking Member.

Mr. THOMPSON. Let me thank our witnesses for their excellent testimony, and obviously you will probably see some of it in written form shared other places, but for all the right reasons, we have to protect our country.

I don't think there's any real difference on the committee as to who the real enemy is. I think there's some question there as to how we should protect it, but I'm convinced that we'll do that.

Mr. Chair, I want to enter into the record part of what Mr. Goldman was saying, a story sharing that Russia and China both are attempting to recruit disgruntled Federal employees for their own benefit.

Mr. MCCAUL. Without objection, so ordered.

[The information follows:]

EXCLUSIVE: U.S. INTEL SHOWS RUSSIA AND CHINA ARE ATTEMPTING TO RECRUIT DISGRUNTLED FEDERAL EMPLOYEES, SOURCES SAY

By Natasha Bertrand, Katie Bo Lillis, and Zachary Cohen, CNN

Updated 9:36 AM EST, Sat March 1, 2025

CNN.—Foreign adversaries including Russia and China have recently directed their intelligence services to ramp up recruiting of US Federal employees working in national security, targeting those who have been fired or feel they could be soon, according to four people familiar with recent US intelligence on the issue and a document reviewed by CNN.

The intelligence indicates that foreign adversaries are eager to exploit the Trump administration's efforts to conduct mass layoffs across the Federal workforce—a plan laid out by the Office of Personnel Management earlier this week.

Russia and China are focusing their efforts on recently fired employees with security clearances and probationary employees at risk of being terminated, who may have valuable information about US critical infrastructure and vital government bureaucracy, two of the sources said. At least two countries have already set up recruitment websites and begun aggressively targeting Federal employees on LinkedIn, two of the sources said.

A document produced by the Naval Criminal Investigative Service said the intelligence community assessed with "high confidence" that foreign adversaries were trying to recruit Federal employees and "capitalize" on the Trump administration's plans for mass layoffs, according to a partly redacted copy reviewed by CNN.

It added that foreign intelligence officers were being directed to look for potential sources on LinkedIn, TikTok, RedNote and Reddit.

At least one foreign intelligence officer directed an asset to create a company profile on Linkedin and post a job advertisement, and to actively pursue Federal employees who indicate they are "open to work," the NCIS document says.

The adversaries think the employees "are at their most vulnerable right now," another of the sources said. "Out of a job, bitter about being fired, etc."

"It doesn't take a lot of imagination to see that these cast aside Federal workers with a wealth of institutional knowledge represent staggeringly attractive targets to the intelligence services of our competitors and adversaries," a third source familiar with the recent US assessments told CNN.

The intelligence seems to confirm what was previously a hypothetical fear for current and US officials: that the mass firings could offer a rich recruitment opportunity for foreign intelligence services that might seek to exploit financially vulnerable or resentful former employees. The Justice Department has charged multiple former military and intelligence officials for providing US intelligence to China in recent years.

"China has always been committed to developing relations with the United States on the basis of mutual respect and non-interference in each other's internal affairs," said Chinese embassy spokesperson Liu Pengyu. "We oppose groundless speculation on China without factual basis."

CNN has reached out to the Office of the Director of National Intelligence as well as the embassy of Russia in Washington for comment.

Officials have been discussing the risk

Career officials at the CIA have been quietly discussing that risk and how to mitigate it in the recent weeks, current and former intelligence officials previously told CNN. Director of National Intelligence Tulsi Gabbard earlier this week suggested that those discussions represented a "threat" made by disloyal government employees—rather than a clinical warning of the potential risks posed by President Donald Trump's aggressive cost-cutting strategy—and that those involved should be penalized.

"I am curious about how they think this is a good tactic to keep their job," Gabbard told Fox News' Jesse Watters on Tuesday. "They're exposing themselves essentially by making this indirect threat using their propaganda arm through CNN that they've used over and over and over again to reveal their hand, that their loyalty is not at all to America. It is not to the American people or the Constitution. It is to themselves.

"And these are exactly the kind of people that we need to root out, get rid of so that the patriots who do work in this area, who are committed to our core mission can actually focus on that," she said.

Multiple current officials across national security agencies who spoke to CNN on the condition of anonymity expressed frustration at the administration's response to what they see as very real warnings—not partisan swiping.

"Employees that feel they have been mistreated by an employer have historically been much more likely to disclose sensitive information," said Holden Triplett, who served as director of counterintelligence at the National Security Council in the first Trump administration and is a former FBI attaché at the US embassies in Moscow and Beijing. "We may be creating, albeit somewhat unintentionally, the perfect recruitment environment."

"This isn't reality TV"

"This isn't reality TV," said another former intelligence official. "There are consequences."

The CIA and Defense Department are weighing significant staff cuts. The Pentagon said in a memo last week that over 5,000 probationary employees, who in most cases have been in their job a year or less, could be fired in the short term. And the CIA has already fired more than 20 officers for their work on diversity issues, many of whom are now challenging their dismissal in court.

The CIA also aggressively seeks to recruit disaffected government employees in adversarial countries "all the time," noted a former intelligence official—using similar tactics. The agency has released a series of public recruitment videos aimed at persuading disgruntled Russian government employees to spy for the United States, videos that detailed ways to securely contact the agency.

"'Domestic political turbulence in your country? Sign up with us to help us help your country!'" the former official paraphrased the US efforts, adding that those efforts deeply aggravate foreign governments.

The CIA may have already inadvertently put some American secrets within the grasp of foreign spies and hackers. In an effort to comply with the executive order to downsize the Federal workforce, the CIA earlier this month sent the White House an extraordinarily unusual email listing all new hires that have been with the agency for 2 years or less—a list that included CIA officers who were preparing to operate under cover—over an unclassified email server.

Some of those officers, who have had access to classified information about the agency's operations and tradecraft, may now be terminated as part of the layoffs.

This story has been updated with new reporting.

CNN's Sean Lyngaas contributed reporting.

Mr. THOMPSON. In addition to that, I want to enter into the record the fact that an unclassified email with names of some employees in the Trump administration was sent to the White House.

Mr. MCCAUL. Without objection, so ordered.

[The information follows:]

C.I.A. SENT AN UNCLASSIFIED EMAIL WITH NAMES OF SOME EMPLOYEES TO TRUMP ADMINISTRATION

The list of partial names was provided in an effort to comply with an executive order to trim the Federal work force.

By David E. Sanger and Julian E. Barnes, New York Times

Feb. 5, 2025

The C.I.A. sent an unclassified email listing all employees hired by the spy agency over the last 2 years to comply with an executive order from President Trump to shrink the Federal work force, in a move that former officials say risked the list leaking to adversaries.

The list included first names and the first initial of the last name of the new hires, who are still on probation—and thus easy to dismiss. It included a large crop of young analysts and operatives who were hired specifically to focus on China, and whose identities are usually closely guarded because Chinese hackers are constantly seeking to identify them.

The agency normally would prefer not to put these names in an unclassified system. Some former officials said they worried that the list could be passed on to a team of newly hired young software experts working with Elon Musk and his government efficiency team. If that happened, the names of the employees might be more easily targeted by China, Russia or other foreign intelligence services.

One former agency officer called the reporting of the names in an unclassified email a "counterintelligence disaster."

Current officials confirmed that the C.I.A. had sent the names of employees to the Office of Personnel Management, complying with an executive order signed by Mr. Trump. But the officials downplayed security concerns. By sending just the first

names and initials of the probationary employees, one U.S. official said, they hoped the information would be protected.

But former officials scoffed at the explanation, saying that the names and initials could be combined with other information—from driver's license and car registration systems, social media accounts and publicly available data from universities that the agency uses as recruiting grounds—to piece together a more complete list.

Senator Mark Warner of Virginia, the top Democrat on the Intelligence Committee, wrote in a social media post that the sharing of the officers' names was "a disastrous national security development."

"Exposing the identities of officials who do extremely sensitive work would put a direct target on their backs for China," Mr. Warner wrote.

The number of officers involved remains classified, but it could be significant. In 2024, the C.I.A. had its best recruiting drive since the aftermath of the Sept. 11 attacks. C.I.A. officers, because of their intense training, have a long probationary period, up to 4 years. However, the White House required only the names of people who had served 2 years or fewer.

Under William J. Burns, the former C.I.A. director, the agency put a new emphasis on trying to recruit a diverse group of officers, arguing that overseas spying operations required people with an array of language skills and cultural knowledge. He focused particularly on expanding the agency's coverage of China, creating a China center at the headquarters that included analysts, operatives and others. When Mr. Burns arrived at the agency in 2021, about 9 percent of the agency's budget was devoted to China-related analysis and espionage; today it is closer to 20 percent.

So any large-scale culling of more recent hires could have a disparate impact on Mandarin speakers and technology experts, along with the agency's minority work force. But current officials said the C.I.A.'s new director, John Ratcliffe, was prioritizing China and did not want to see any mass exodus of people with expertise in that area.

The Trump administration has made quick work of diversity programs, ordering them shut down and scrubbed from websites.

The White House-ordered review of probationary hires comes as Mr. Ratcliffe has begun an effort to push long-tenured agency officers to retire early. Mr. Ratcliffe, officials said, hopes to clear a path to leadership jobs for midcareer officers.

The C.I.A. is offering its employees what it is calling "deferred resignation," an option to quit but continue to be paid through September, as part of the efforts led by Mr. Musk to shrink the size of the Federal work force, officials said.

National-security-related agencies had originally been exempted, at least partially, from the government-wide "fork in the road" offer to leave their jobs that was extended last week. But Mr. Ratcliffe pushed to have a version of the offer extended to his work force.

Under the C.I.A.'s program, the agency will retain some say over the timing of when anyone leaves to ensure that critical areas have enough officers.

Otherwise, however, the offer is structured in much the same way as what Mr. Musk's team pushed out across the Federal Government.

In an email sent on Tuesday, agency officers were extended an offer to leave the agency effective Sept. 30 but continue to be paid. An aide to Mr. Ratcliffe said it was "effectively giving them a buyout and a runway to the private sector."

The offer was reported earlier by The Wall Street Journal.

The aide to Mr. Ratcliffe, who spoke on the condition of anonymity under agency protocol, said the effort was meant to encourage some of the large group of officers who joined after the Sept. 11 terrorist attacks to retire early.

"These moves are part of a holistic strategy to infuse the agency with renewed energy, provide opportunities for rising leaders to emerge and better position the C.I.A. to deliver on its mission," according to a statement released by a C.I.A. spokeswoman.

The spokeswoman said the offer would ensure that the agency's work force was responsive to the Trump administration's "national security priorities."

A correction was made on Feb. 5, 2025: An earlier version of this article misstated where the C.I.A. sent a list of employees. It went to the Office of Personnel Management, not to the Office of Management and Budget.

When we learn of a mistake, we acknowledge it with a correction. If you spot an error, please let us know at nytnews@nytimes.com.

David E. Sanger covers the Trump administration and a range of national security issues. He has been a Times journalist for more than four decades and has written four books on foreign policy and national security challenges.

Julian E. Barnes covers the U.S. intelligence agencies and international security matters for The Times. He has written about security issues for more than two decades.

A version of this article appears in print on Feb. 6, 2025, Section A, Page 17 of the New York edition with the headline: C.I.A. Sends White House Unclassified Email Listing Employee Names.

Mr. THOMPSON. What we heard today is that China's ambition to shift international order and their capability to do it is real.

While Acting Chairman Guest recognized that countering threats from the CCP will also take economic and diplomatic investment, the administration's actions run counter to that statement.

Just today, in response to the Trump administration's recent actions, the Chinese Embassy in the United States tweeted: "If war is what the U.S. wants—be it a tariff war, a trade war, or any other type of war—we are ready to fight till the end."

In a war, our Nation needs allies and assets. This administration is sidelining our friends, NATO, as well as Ukraine, while appeasing Russia.

The administration is cutting the cyber work force that protects our networks, undermining our intelligence capabilities, and weakening our relations around the world.

The administration's approach does not make sense. The administration is leading us into a fight with China with a misguided foreign policy, a misguided trade policy, and a misguided cyber policy, a misguided intelligence policy, and a misguided economic policy.

Instead, we must maintain our tried-and-true alliances and posture the United States to defend against threats both foreign and domestic.

I urge our Republican colleagues to step up and hold the Trump administration accountable.

I thank, again, the witnesses for their testimony and yield back.

Mr. MCCAUL. The Ranking Member yields.

Let me, in closing, say it's been a great hearing. I think, as Dr. Pillsbury said, this is a bipartisan issue. It's a threat to the United States, and as Americans, we unite as Republicans and Democrats.

I also just want to make a few comments on the threat landscape as I see it. As both the Chairman Emeritus of this committee and Foreign Affairs, the threat after the fall of Afghanistan, the invasion of Ukraine, then the Ayatollah rearing his ugly head in the Middle East, but the unholy alliance between Putin and Chairman Xi at the Beijing Olympics, prior to the invasion of Ukraine is, I find, deeply disturbing.

I think as Dr. Doshi mentioned, that the Chinese have completely revitalized the Russian military. Iran has sent drones that Russia uses to kill Ukrainians, you know, the same drones that they use to fire into Israel.

However, I do see normalization in the Middle East. Being the eternal optimist, I do see the conflict in Eastern Europe, I hope, being resolved.

It's the threat to the Indo-Pacific that I find the most serious within the context of the great power competition, but also as someone who's traveled to Taiwan and been surrounded on the island by war games, exercises conducted by the CCP, in a direct shot across the bow, not only to me but to the recently inaugurated President Lai, as someone who flew over the South China Sea, seeing China, Chinese warships invading Philippine waters with

water cannons, hitting vessels in the Philippines, warning us that we are invading Chinese sovereign territory.

It's getting very aggressive, which is why I passed the AUKUS bill to the alliance of United States, Australia, and the United Kingdom, to further not only submarine wars—warfare, but also pillar No. 2, which is AI quantum innovation when it comes to weapon systems, which is why I think, again, going back to this export-control issue on chips is important.

I think an invasion of Taiwan would be catastrophic. Either China would own or break TSMC, which I have traveled to and have seen. You mentioned ASML's machines, very important that they not sell those to China.

But the result there, as I was told by TSMC, would be a complete shutdown of 90 percent of the advanced global manufacturing, which is precisely why I introduced the CHIPS Act, under the guidance of Mike Pompeo, then-Secretary of State under President Trump, so there's no confusion about this program, which was designed to pull supply chain out of Taiwan and invest it in the United States.

TSMC just announced a $100 billion investment in the United States, which is a good thing, and we've had $650 billion reinvested for the purpose of manufacturing this critical asset here in the United States.

I want to leave you with 2 other thoughts that have not come up, and that is, I have visited with Merrick Garland, being in the brotherhood of the DOJ, and talked to him about the China Task Force being shut down, even though espionage has not.

This united front, someone who worked in this area many years ago, concerns me, as a 501(c)(3) political arm of the CCP in the United States.

Also something was brought to my attention by Palmer Luckey who runs Anduril, that does a lot of great innovation like the Ghost Shark, which will be used extensively in the Pacific. Talked about our patent system being open to the public and how China, for them, it's a treasure trove of documents that they can look at, on a daily basis, and steal patents from the United States.

Finally, capital flows. You know, I introduced a bill last Congress. I know the administration has come out with their own guidance and Executive Order on restriction of capital flows that then basically go into arming the PLA's war machine.

So I leave you with those thoughts in conclusion. I invite you to provide further testimony on those points.

Finally, to the point that Dr. Pillsbury raised, and that is the role of this committee, when you have all those employees over there at the Department of Homeland, how many are really working on China?

In my view, it should be the highest priority. So any guidance you have to this committee in terms of what the Ranking Member and the Chairman and the committee can do to strengthen our resiliency against what I consider to be the great power competition, the biggest threat to the United States, looking to the next generation, and that is Communist China.

So, with that, I know I have some closing remarks that have to do with the written statements will be allowed and so forth, but

I want to thank the witnesses for being here today, and I look forward to seeing your addendum, your further testimony in writing to the issues I just raised.

With that, this committee stands adjourned.

[Whereupon, at 12:19 p.m., the committee was adjourned.]

APPENDIX

QUESTIONS FROM CHAIRMAN MARK E. GREEN, MD FOR MICHAEL PILLSBURY

Question 1. In 2018, you testified before the House Intelligence Committee and your opening statement referred to how the United States has made progress in its new strategy toward the CCP, but as a Nation we may still be underestimating the CCP problem and China's resistance to change. Seven years and 2 administrations later, do you feel that we are positioned better to combat CCP threats? If so, how exactly? If not, how come?

Answer. Response was not received at the time of publication.

Question 2. You have examined the United States' strategic competition with China. We even have a bipartisan select committee in the House dedicated to these efforts. In your view, how do you think we should balance the need for a certain degree of pragmatic engagement with the CCP, while maintaining a strong deterrent in military and economic spheres?

Answer. Response was not received at the time of publication.

Question 3. One of the Trump administration's main initiatives is to hold China responsible for being a silent partner with the distribution of poisonous fentanyl into our homeland—a critical issue for our committee. How significant is the CCP's involvement in fentanyl distribution and deaths in the United States?

Answer. Response was not received at the time of publication.

Question 4. In your opinion, how can our Government be more effective in addressing the CCP's role in fentanyl trafficking?

Answer. Response was not received at the time of publication.

Question 5. Dr. Pillsbury, you have had a front row seat to the rise of China's economy—which owes much to American generosity from the 1970's to the present time. The United States has helped China gain access to world markets, notably support for China's acceptance into the World Trade Organization in 2001. In return, they promised transparency in its laws and regulations, intellectual property protections, and tariff cuts on imported goods. Do you think China has been a reliable partner in this relationship?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN MARK E. GREEN, MD FOR WILLIAM R. EVANINA

Question 1. You have mentioned before in your appearances before Congress the need for our Nation and Government to take a "modern view and reimagination" of counterintelligence. Can you explain why this is important in addressing our adversaries such as the CCP?

Answer. Response was not received at the time of publication.

Question 2. What specific changes or innovations do you believe are necessary within our current counterintelligence framework to effectively have this modern view of counterintelligence?

Answer. Response was not received at the time of publication.

Question 3. The insider threat and malign influence is a constant vulnerability used by the CCP that has not only affected local and State governments across our Nation, but academia and the private sector as well. Can you speak on effective ways to identify and prevent insider threats from the CCP?

Answer. Response was not received at the time of publication.

Question 4. You wrote an article last year for the National Defense Magazine titled, "Spectrum Shortage Threatens U.S. National Security." You stated that the spectrum, which is the invisible airwaves which makes wireless communications possible, has vulnerabilities that makes attacks possible from Chinese actors and threatens our national security. Can you speak about the importance of addressing this issue?

Answer. Response was not received at the time of publication.

Question 5. Last month, this committee released our updated China Threat Snapshot which detailed more than 60 cases of espionage conducted by the CCP on U.S. soil. These cases included but were not limited to transmission of sensitive military information and stealing of trade secrets. Can you speak to the methods that CCP uses for espionage activities?

Answer. Response was not received at the time of publication.

Question 6. It was recently reported in open-source news that the CEO of S&L Aerospace Metals LLC, Jerry Wang, is listed as an official for several CCP influence and intelligence groups. His company has received tens of millions of dollars in DOD contracts for parts for fighter jets, helicopters, and guided missile launchers. How vulnerable do you believe our Nation's supply chain is to the CCP and its affiliates?

Answer. Response was not received at the time of publication.

Question 7. In March 2023 you appeared before this committee and stated that economic security is national security. You stated that in 2020 alone, the estimated economic loss from theft of intellectual property and trade secrets from CCP was billions of dollars. This is a staggering amount; how can we mitigate this specific threat?

Answer. Response was not received at the time of publication.

Question 8. During the last administration, Chinese illegal aliens flooded across the border at unprecedented levels. Do you think it's possible that there may be CCP operatives who have crossed the borders, either detected or undetected, that are here in the United States for nefarious reasons?

Answer. Response was not received at the time of publication.

Question 9. On February 4, 2025: Leon Ding, a Chinese national, was indicted for allegedly stealing AI secrets from Google. According to the superseding indictment, he allegedly uploaded over 1,000 files containing confidential company information into his personal Google Cloud account from May 2022 through May 2023. Could you briefly walk us through the significance of this case?

Answer. Response was not received at the time of publication.

Question 10. On March 9, 2023: you testified before the committee that China "continues to utilize "non-traditional" collectors to conduct a plurality of their nefarious efforts here in the United States due to their successful ability to hide in plain sight. The non-traditional collectors, serving as engineers, businesspersons, academics, and students are shrouded in legitimate work and research, and oftentimes become unwitting tools for the CCP and its intelligence apparatus." Has your assessment changed in any way? How exactly?

Answer. Response was not received at the time of publication.

Question 11a. Under the first Trump administration, you served as the first Senate-confirmed director of the National Counterintelligence and Security Center (NCSC). The NCSC leads and supports the U.S. Government's counterintelligence and security activities critical to protecting America. Can you please expand on your prior work for this center?

Answer. Response was not received at the time of publication.

Question 11b. The NCSC provides outreach to the private sector at risk of foreign intelligence penetration. Can you please expand on the level of threats and efforts to mitigate such threats?

Answer. Response was not received at the time of publication.

QUESTIONS FROM CHAIRMAN MARK E. GREEN, MD FOR CRAIG SINGLETON

Question 1a. Your article titled "Safeguarding U.S. Interests in the Face of China's 'New Productive Forces' Strategy", highlights China's efforts to spur economic growth by asserting dominance in several key emerging technology sectors. Given the recent advancements we have seen with DeepSeek, I am interested in hearing more about the impact of China's "new productive forces" strategy on U.S. technology development and security.

If China successfully implements its "new productive forces" strategy, what cybersecurity risks will China introduce into the global technology ecosystem? How can the United States protect against these risks?

Answer. Response was not received at the time of publication.

Question 1b. Follow-up: My bill, the China Technology Transfer Control Act, would strengthen export controls to China for any covered technologies or IP. Given cyber space has no borders, what policy solutions can we pursue concurrently with export controls to strengthen our cyber defenses against China?

Answer. Response was not received at the time of publication.

Question 2a. China is sitting in critical infrastructure that Americans depend on every day. For at least 5 years, Volt Typhoon has been waiting and ready to shut

down our infrastructure in the event of a conflict between the United States and China over Taiwan.

The Trump administration often speaks about going on the offense. How can we leverage the U.S. toolkit to tell China that intruding into our critical infrastructure is unacceptable?

Answer. Response was not received at the time of publication.

Question 2b. Follow-up: How prepared is Taiwan to protect their networks and infrastructure against a cyber attack from China?

Answer. Response was not received at the time of publication.

Question 2c. Follow up: What should cybersecurity cooperation look like with Taiwan?

Answer. Response was not received at the time of publication.

Question 3. You recently wrote an article titled, "Laser Focus: Countering China's Lidar Threat to U.S. Critical Infrastructure and Military Systems." In the article, you explained how Lidar, which is a remote sensing technology with both military and civilian applications, stands at the middle of the CCP's bid for technological superiority. Could you please briefly expand on what you mean by this assertion and why it should matter to the American people?

Answer. Response was not received at the time of publication.

Question 4. On December 18, 2024: Chen Jinping, a resident of New York City, pleaded guilty to conspiring to act as an illegal agent for the People's Republic of China (PRC), in connection with opening and operating an undeclared overseas police station in lower Manhattan for the PRC's Ministry of Public Security. According to court filings, Jinping and co-defendant "Harry" Lu Jianwang also allegedly obstructed justice by destroying evidence of their communication with the PRC's government. Could you briefly explain the significance of this case?

Answer. Response was not received at the time of publication.

Question 5. On December 11, 2024: Yinpiao Zhou, a PRC citizen and lawful permanent resident of California, was arrested for allegedly flying a drone over and taking photographs of Vandenberg Space Force Base. He was arrested at San Francisco International Airport before attempting to board a flight to the PRC. According to court filings, a drone detection system identified the drone flying over the base. The drone systems identified that the drone flew for about 1 hour, flew to an altitude of nearly 1 mile above ground level, and came from Ocean Park, a public space adjacent to the base. Could you briefly explain the significance of this case?

Answer. Response was not received at the time of publication.

Question 6. Considering the CCP's National Intelligence Law, which can compel Chinese citizens to assist in intelligence gathering, how are U.S. border authorities assessing the potential long-term security risks posed by the influx of Chinese nationals, particularly in relation to critical infrastructure and sensitive technology sectors?

Answer. Response was not received at the time of publication.

Question 7a. Would you agree that a dedicated working group at DHS to tackle acts of transnational repression by the CCP against American citizens and dissidents on U.S. soil would help keep the homeland safe?

Answer. Response was not received at the time of publication.

Question 7b. Follow-up: On November 18, 2024: Texas Governor Greg Abbott issued an executive order (Executive Order No. GA–47) that enabled law enforcement agencies throughout the State to investigate and charge individuals who commit acts of transnational repression on behalf of the PRC and the CCP. Do you think that other States should consider taking similar actions?

Answer. Response was not received at the time of publication.

Question 8. In your testimony you stated that we are in a global arms race with the People's Republic of China (PRC), especially as it pertains to telecommunications. Could you please expand on how much of a cyber risk Huawei poses to U.S. companies and U.S. national security?

Answer. Response was not received at the time of publication.

Question 9. Is Huawei an integral part of the PRC's military-civil fusion strategy?

Answer. Response was not received at the time of publication.

Question 10. Does Huawei act in a manner counter to the interests of a free, fair, and competitive market to further the interests of the PRC's government?

Answer. Response was not received at the time of publication.

Question 11a. Barring any outright prohibition or ban of Huawei by U.S. allies and partners, how can American companies effectively compete against the PRC-state-backed company?

Answer. Response was not received at the time of publication.

Question 11b. What American companies, if any, currently have the capacity to effectively compete with Huawei across the full stack?

Answer. Response was not received at the time of publication.

Question 11c. Where do these companies stack up against their European competitors?

Answer. Response was not received at the time of publication.

Question 11d. Do any currently existing companies outside of the PRC have a competitive position versus a PRC-state-backed company like Huawei?

Answer. Response was not received at the time of publication.

