S. HRG. 117–315

BEIJING'S LONG ARM: THREATS TO U.S. NATIONAL SECURITY

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE

OF THE

UNITED STATES SENATE

ONE HUNDRED SEVENTEENTH CONGRESS

FIRST SESSION

AUGUST 4, 2021

Printed for the use of the Select Committee on Intelligence

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

U.S. GOVERNMENT PUBLISHING OFFICE
45–491 PDF WASHINGTON : 2023

SELECT COMMITTEE ON INTELLIGENCE

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

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

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

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

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

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

C O N T E N T S

AUGUST 4, 2021

OPENING STATEMENTS

WITNESSES

BEIJING'S LONG ARM: THREATS TO U.S. NATIONAL SECURITY

WEDNESDAY, AUGUST 4, 2021

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

The Committee met, pursuant to notice, at 2:45 p.m., in Room SH–216 in the Hart Senate Office Building, Hon. Mark R. Warner (Chairman of the Committee) presiding.

Present: Senators Warner, Rubio, Wyden, Heinrich, King, Bennet, Casey, Gillibrand, Burr, and Cornyn.

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

Chairman WARNER. Good afternoon. I call this hearing to order. And welcome to our witnesses, one of them a good, good friend of the Committee: The Honorable Bill Evanina, former Director of the National Counterintelligence and Security Center. He is the founder and CEO of The Evanina Group. And in many ways, a lot of what we're going to be talking about today, he's worked on with the Members of this Committee for many, many years.

Anna Puglisi, Senior Fellow at the Center for Security and Emerging Technology, or CSET, at Georgetown University.

And on WebEx, Matt Pottinger, the Distinguished Visiting Fellow at The Hoover Institution and former Deputy National Security Adviser at the White House.

Today, the Committee will examine the counterintelligence threats posed by the People's Republic of China and the Chinese Communist Party. We will look at the PRC's activities within the United States as it works to acquire critical U.S. technologies and intellectual property, hack into the U.S. cyber networks, and conduct influence operations to shape narratives to be more favorable to the PRC and the CCP. I hope the witnesses will also discuss their recommendations for better countering the CCP's efforts in the United States.

Now, the Intelligence Committee, as Senator Burr often reminded us, doesn't normally hold open hearings, but Vice Chairman Rubio and I believe this story needs to get out to the American public.

Several years ago, the Committee, in a bipartisan way thanks in part to Senators Rubio, Burr, Cornyn, and Collins, convened a series of classified sessions with leaders from the Intelligence Community and leaders from the private sector—tech, finance, venture capital, academia—to brief them on efforts by the CCP to target

their industries. I've wanted for some time to take those briefings and move them into an open hearing so that the U.S. public, including the private sector, our academic institutions, our media outlets, and others, can better understand these threats and how we as a society can counter them. Because the truth is the government cannot counter the CCP's actions all by itself.

One of the most important areas that I hope the witnesses will address is how China is focusing on targeting key U.S. technologies for both acquisition and development. These include aerospace, advanced manufacturing, AI, biotech, data analytics, semiconductors, renewables—all in order to ensure PRC's future dominance in these areas. We saw this play out in many ways. And again, I think this Committee was one of the first to notice the CCP's efforts in their pursuit of 5G technology, backing Huawei. And I'm proud of this Committee's work in sounding the alarm on the threat of what would happen if networks all around were reliant on a sole-source Chinese provider in 5G. That would threaten both our national security and our allies' security. I hope the witnesses will also address how the CCP is using a variety of methods to acquire these capabilities, including cyber and traditional espionage, but also using a lot of the tools of business, joint ventures, acquisitions, mergers, and increasingly strategic investments by firms that, at the end of the day, are answerable to the Communist Party leadership in Beijing.

They're also creating a series of partnerships with universities, in many ways, oftentimes luring some of those universities into trips or sinecures that sometime put that academic research at risk.

We also know, increasingly, we're seeing their malign influence efforts to affect policy decisions that we in the Congress make. Matter-of-fact, the FBI has estimated that China's theft of simply American intellectual property, not worldwide, just American intellectual property runs from between $300 billion to $600 billion a year. According to the DOJ, 80 percent of all economic espionage prosecutions brought by the DOJ alleged conduct that would benefit the Chinese state, and 60 percent of all trade secret theft cases have some nexus to China.

FBI Director Wray told this Committee in April that the Bureau has more than 2,000 operations going on, investigations, that tie back to the Chinese government. And this is one of the most stunning facts he laid out. He opens up a new investigation into Chinese espionage every 10 hours. The Director also attested that no other country represents more of a threat to the United States, to economic security, and to democratic ideals than China. And that China's ability to influence American institutions is "deep, wide, and persistent." Ceding leadership across these technology sectors would have major repercussions for U.S. economic and national security.

Let's not forget that, in most ways, since World War II, the United States has led in both scientific research and the development of transformational technologies. It's this leadership that has translated into decades of economic success for U.S. companies and our military capabilities. As part of our technological leadership, the U.S. or like-minded democracies also set the global standards

and protocols for new technology. Many times, we can implant in those standards, in those protocols, our values: democracy, transparency, diversity of opinion, and respect for human rights. And that is a long-term value to our country that I don't think is often factored in. I've been frustrated though by the frequency by which U.S. companies and their desire for market access in China have frankly given up sometimes on those values, and sometimes facilitated and enabled the PRC to acquire sensitive U.S. technologies. The idea they can't miss the Chinese market means they make sacrifices going into that market they would make in no other nation in the world. China, in turn, uses these technologies to advance its own illiberal vision to surveil and control its population, stifle the free flow of information, and repress foreign influence campaigns worldwide. These technologies enable the PRC to suppress dissidents and restrict religious groups. We see that whether it's in Xinjiang or in Hong Kong.

As we think through what the CCP is doing in the United States, I want to make crystal clear though, my concerns lie squarely with the President of China, Xi Jinping, and the Chinese Communist Party leaders, not the people of China, and certainly not with Chinese-Americans or other Asian-Americans who've contributed so much to our society.

Our answer to these challenges cannot be to keep talented folks out of the United States. In fact, we've seen in my State of Virginia, Northern Virginia particularly, a technology hotbed, literally, 40 percent of all the startups are started by first-generation Americans. So, it is in our national interest to welcome these talented Chinese academics, entrepreneurs, and technologists and in fact make it more attractive for them to use their talent to bolster our economy rather than simply going back to China. This is, again, where our values come into play. And Americans should also be aware that the PRC's pressures and coercion efforts don't stop with the diaspora or Chinese nationals living in the United States.

As Senator Rubio pointed out, increasingly the CCP is focused on pressuring U.S. citizens, entities, and businesses across industries to, again, shape a narrative that advances their goals. Even for this hearing, a number of potential witnesses declined to participate in an open format for fear of retribution to themselves or their families. From the PRC's pursuit of critical and sensitive technology to its repression at home and coercion abroad, and its focus on trying to win the technology battle in the 21st-century, it's clear that I think our country is facing a new Sputnik moment where we must take steps to remain competitive, especially in technology, and find better ways to strengthen our defenses against the CCP's myriad, intelligence, tech acquisition, and foreign influence operations. Because we're back into this kind of semi-hybrid system today, for today's meeting, we will be asking questions by order of seniority, and as Senator King has made clear, with the five minute rule applying.

Thank you. I now turn to the Vice Chairman.

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

Vice Chairman RUBIO. Thank you, Mr. Chairman, for holding this hearing.

I think you started out by talking about how unusual it is we have these open hearings, and there's a reason for it. The Members of this Committee on a regular basis review some of the most sensitive intelligence, both intelligence and the products that come from them, that this government has available to it. So, I think it should send a powerful message when you see that on issue after issue relating to China, issues that some would argue are outside the purview of what this Committee has traditionally looked at—technology, academia, influence operations, global diplomacy, industrial policy—that it is Members of this Committee that you see in the lead on so many issues relating to China. Because of the role the Members on the Committee play, they have a very unique insight into this horror show that's playing out before our eyes in the 21st century.

The title of this hearing is "The Long Arm of China." The long arm of China is not some futuristic threat. It's already here. China stealing between $300 billion and $600 billion a year—$300 billion and $600 billion a year—of American technology and intellectual property. They hack into networks, and they take it. They use venture capital funds to buy promising technology startups. They hide their ownership that way. They partner with universities on research, and then they steal that research, often research whose seed funding came from the U.S. taxpayer. They force American companies doing business in China to give the technology over to them.

And I think the other thing most people don't realize is China already, already, has tremendous influence and control over what Americans are allowed to say or hear about them or many of the other issues in the world. Hollywood is so desperate, for example, to have their movies shown in China that Hollywood won't make a movie that the China communist censors don't approve. The U.S. corporations are so desperate to have access to the Chinese market that they'll lead costly boycotts of a state, an American state, that passes a law that they don't like. But they don't dare say a word about the fact that as we speak, genocide is taking place against Uyghur Muslims. American companies have actually fired Americans who live in America for saying or writing something that China doesn't like. There are some examples here that are pretty stunning.

In 2019, China suspended business ties with the NBA because the general manager of the Houston Rockets expressed support for Hong Kong democracy protests.

In 2019, Apple removed an app that enabled protesters in Hong Kong to organize, following CCP pressure.

In 2019, an American company, Activision Blizzard, suspended a gamer and took away his prize money for voicing support for Hong Kong protesters.

In 2018, Marriott fired an employee that ran a social media account, because he liked a Twitter post from a Twitter account ap-

plauding Marriott for listing Tibet as a country rather than as part of China, and he was fired after that.

In 2018, Gap made a shirt with a map of China, and it didn't include Taiwan. They apologized for it, and they removed the shirt from its stores. Well, maybe you think that shirt thing is trivial. I don't think people getting fired is trivial, apps getting removed is trivial. These are just one of a handful of many. And this is already happening.

So, in conclusion, I'd say two things. The first is the Chairman is absolutely right. This is not about the Chinese people or especially not about Chinese-Americans, okay? My parents came from Cuba. I live in a community filled with Cuban-Americans. It would be unfair to blame Cuban-Americans for the atrocities of the Cuban regime, and it would most certainly be unfair to blame the Cuban people for the horrifying actions of the regime that controls that enslaved island. Likewise, the biggest opponents of the Chinese Communist Party on the planet happen to be Chinese. Many live here, many in other parts of the world, and many under their oppressive thumb. So, this is not about the Chinese people. It is about a Communist Party, and it is time to wake up.

Today, China is already carrying out the biggest illegal wealth transfer from one nation to another in the history of mankind.

Today, the Chinese Communist Party has more control over what Americans can say, what we can hear, what we can read, what we can watch than any foreign government has ever had in our history.

And they have weaponized our openness. They have weaponized our decency, and they have weaponized our corporate lust for profits against us. And if we don't wake up and we don't address this now, the America our children are going to inherit very soon could very well be one where the sanctimonious preachings, as someone once said, the sanctimonious preachings of a genocidal communist tyranny will be the only thing that Americans will be allowed to hear or say about China.

So, I'm glad we're having this hearing. And, Mr. Chairman, just as a point of privilege here, one of our longtime staffers, today is his last hearing with us, Paul Matulic. He's been with the Committee for 16 years. Worked with Senators Hatch, Chambliss, Burr, and Cornyn, and now, here with us, and so he's retiring. And we hope, as all retirees should, he's moving to Florida. We don't know. But that's what Americans do. We want to thank him for his service to the Committee, and we hope our last hearing will be a memorable one. Thank you for your service.

[Applause.]

Chairman WARNER. Well, let me echo that, and this was a subject of quite a bit of the focus yesterday in our closed hearing where we went into some of Paul's behavior and linguistic abilities. Luckily, that will stay classified, but we all very much value Paul's work and, again, want to commend him, in particular, for him and the whole team with their relentless pursuit of the truth in the Russia investigation.

With that, we turn to our witnesses, and I'm not sure—Anna, Bill, or Matt on WebEx—who's going to go first but the floor is yours.

STATEMENT OF BILL EVANINA, FOUNDER AND CEO, THE EVANINA GROUP; FORMER DIRECTOR FOR THE NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER (NCSC)

Mr. EVANINA. Good afternoon, Chairman Warner, Vice Chairman Rubio, Members of the Committee. It's an honor to be here before you today. I've humbly briefed this Committee on a regular basis for more than a decade as the Director of National Counterintelligence and Security Center, and as a senior executive of the FBI and CIA. I was tremendously honored last year to be the first Senate-confirmed director of NCSC, leading our Nation's counterintelligence efforts. And I want to specifically thank this Committee for your support.

I'm here today before you as a private citizen.

Today's topic, the holistic and comprehensive threat to the United States posed by the Communist Party of China is an existential threat, and it is the most complex, pernicious, aggressive, and strategic threat our Nation has ever faced. I proffer that the U.S. private sector and academia have become the geopolitical battle space for China. Xi Jinping has one goal: to be the geopolitical, military, and economic leader in the world. Period. He, along with China's Ministry of State Security, People's Liberation Army, and United Front Work Department, 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 the Communist Party. It drives their every decision. So, why does it matter? Because economic security is national security. Our economic global supremacy, stability, and long-term vitality is at risk and squarely in the crosshairs of Xi Jinping and the communist regime. It is estimated that 80 percent of American adults have had all of their personal data stolen by the Communist Party of China. The other 20 percent? Just some of the data.

As the Chairman and Vice Chairman already referenced, the estimated economic loss last year from the country of China just from known intellectual property and trade secrets loss is between $300 billion and $600 billion a year. It's a big number. What that means it's between $4,000 and $6,000 per American family of four after taxes.

Competition is great and necessary, and it is what made America the global leader we are today. However, I would proffer China's economic growth the past decade via any and all means is considerably less than fair competition. My question is, are we really competing?

If we do not alter how we compete with awareness of China's malign methodology and one-sided practices, we will not sustain our global position as the world leaders from tomorrow's emerging technology down to our creative ideations. We must create a robust public-private partnership with real intelligence sharing while at the same time staying true to the values, morals, and rule of law which made America the greatest country in the world.

This will take a whole-of-nation approach with the mutual fund-analogous, long-term commitment. Such an approach must start with a contextual awareness campaign, reaching a broad audience from every level of government to university campuses, and from

boardrooms to business schools. The "why" matters. As an example, Huawei is a national security threat to the United States. This Committee is aware of that. But we do not officially explain to America why. U.S. boards of directors and investment leaders must begin to look beyond the next fiscal quarterly earnings call and begin to think strategically about how their investment decisions and unawareness to the long-term threat can impact their businesses and industries, as well as America's economic and national security.

From a cybersecurity perspective, China possesses persistent and unending resources to penetrate our systems and exfiltrate our data, or sit dormant and wait, or plant malware on a critical infrastructure for future hostilities. At the same time, the insider threat epidemic originating from the Communist Party of China has been nothing short of devastating to the United States corporate world.

Additionally, the Communist Party of China strategically conducts malign influence campaigns at the state and local level of the United States with precision. These efforts must be exposed and mitigated. To effectively defend against China and compete effectively, we must put the same effort into this threat as we did to combat terrorism the past 20 years. I would suggest the threat posed by the Communist Party of China is much more dangerous to our economic and military viability as a Nation.

In conclusion, I'd like to say for the record, as the Chairman and Vice Chairman mentioned, the significant national security threat we face from the Communist Party of China is not a threat posed by the Chinese people or as individuals. Chinese nationals or any Chinese person or Chinese ethnicity here in the United States or around the world are not a threat. They should not be racially targeted in any manner whatsoever. This is a threat pertaining to a draconian communist country with an autocratic dictator who is committed to human rights violations and stopping at nothing to achieve its geopolitical goals. Thank you for this opportunity to be here with you today, and I look forward to dialog with my colleagues. Thank you.

Chairman WARNER. Thank you, Bill. Anna?

[The prepared statement of Mr. Evanina follows:]

STATEMENT OF WILLIAM R. EVANINA
CEO, THE EVANINA GROUP

BEFORE THE SENATE SELECT COMMITTEE ON INTELLIGECE

AT A HEARING CONCERNING THE COMPREHENSIVE THREAT TO AMERICA POSED BY THE COMMUNIST PARTY OF CHINA (CCP)

AUGUST 4, 2021

Chairman Warner, Vice Chairman Rubio, and Members of the Committee — it's an honor to appear before you today. I have been honored to brief this Committee on a regular basis over the past decade as the Director of the National Counterintelligence and Security Center, and as a senior counterintelligence executive in the CIA, and FBI. I was tremendously honored to be the first Senate Confirmed Director of NCSC in May of 2020. I am here before you today a private citizen, and CEO of The Evanina Group, LLC. In this role I work closely with CEOs and Boards of Directors to advise on the issues we are about to discuss and develop strategic mitigation efforts to ensure effective defenses, as well as brand protection.

Today's topic, the holistic and comprehensive threat to the U.S. posed by the Communist Party of China (CCP) is as critical of a topic, and threat, as we face today as a nation.

I have spent 32 years of my adulthood working the U.S. Government. Twenty-four of which with the FBI, CIA, and NCSC.

Our nation faces a diverse, complex, and sophisticated threats by nation state actors, cyber criminals, and terrorist organizations.

Russia poses an increased, and significant intelligence and cyber threat to the US, in both the public, and private sectors. Vladimir Putin, with his aggressive intelligence services along with loyal, highly resourced oligarchs, continue to push boundaries in numerous geopolitical and cyber arenas. Putin's goal to destabilize the U.S. and degrade our Democracy in evident every day, especially in illicit cyber activity and extensive social media malign influence campaigns.

Iran and North Korea continue to pose a challenge to the U.S. particularly from a cyber perspective.

However, the existential threat our nation faces from the Communist Party of China (CCP) is the most complex, pernicious, strategic, and aggressive our nation has ever faced.

I proffer that the U.S private sector has become the geopolitical battlespace for China as a baseline for this comprehensive and nefarious behavior.

Xi Jinping has one goal. To be THE Geopolitical, Military, and economic leader in the world. XI, along with the China's Ministry of State Security, People's Liberation Army, and the United Front Work Department, drive a comprehensive and whole of country approach to their efforts to invest, leverage, infiltrate, influence and steal from every corner of U.S. success.

Economic security is national security. Our economic global supremacy, stability, and long-term vitality is not only at risk, but squarely in the cross hairs of Xi Jinping and the communist regime. It is estimated that 80% of American adults have had all of their personal data stolen by the CCP, and the other 20 percent most of their personal data. This is a generational battle for XI and the CCP, it drives their every decision, particularly geopolitically. How to counter and push past the U.S. is goal number one for the CCP.

Intelligence Services, Science & Technology Investments, Academic Collaboration, Research Partnerships, Joint Ventures, Front Companies, Mergers and Acquisitions, and outright theft via insiders and cyber intrusions, begin the comprehensive and strategic framework for how China implements their strategy.

China utilizes non-traditional collectors to conduct a plurality of their nefarious efforts here in the U.S. 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.

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. Joint ventures, creative investments into our federal, state and local pension programs, collaborative academic engagements, Sister City Programs, Confucius Institutes on Campus, 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. The threat from China pertaining to academia is both wide, and deep. My colleague Anna Puglisi will discuss this more thoroughly today. However, the past three years of indictments and prosecutions have really highlighted the insidiousness of China's approach to obtaining early and advanced research as well

as understanding the complexity of gifts and funding at U.S. colleges and universities, particularly when tied to federal grants.

China's priorities for obtaining U.S. based technology and know-how, pursuant to their publicly available 25 Year Plan are Aerospace, Deep Sea Technology, Biotechnology, Information Technology, Manufacturing, Clean Energy, Electric Battery Technology, and DNA/Genomics. Any CEO or Board of Directors leading in any of these critical industries must become aware of the threat posed to them and work with their security team and outside experts to identify risk-based mitigation strategies.

The proverbial salt in the wound of all this nefarious activity is when the CCP steals our thoughts, ideas, patents, and technology, and manufactures that same technology in China, and the sells it back to American companies and around the world. One needs to look no further than the American Supercomputer Corporation for just a glimpse of the long-term impact to economic espionage. Then one must factor in all the manufacturing plants which were not built, and the tens of thousands of jobs which were not created because China, via its theft, beat the U.S. to the global market and is selling the same product and a significant reduction in real costs.

Boards of Directors and investment leaders must begin to look beyond the next fiscal quarterly earnings call and begin to think strategically with respect to how their decisions and unawareness of the long-term threat impact their businesses and industries, which is woven with our national security, economic stability, and endurance of our republic.

In 2017, the Communist Party of China issued new state laws to facilitate the perniciousness of their efforts to obtain data, from everywhere. Three specific portions of those laws should be understood, and be an enduring reminder to CEOs, General Counsels, Chief Data Officers, CIOs, 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.

Hence, 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. This includes third party data as well. The analogy is

a U.S. company enters into a business deal or partnership with a company from another country. The U.S. company must provide all relevant and requested data from their company, as well as the partner company, to the NSA, CIA and FBI.

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

To further the Communist Party of China's unleveled 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.

American business leaders, and Americans in general, must understand that China is a Communist Country run by an authoritarian "President" for life. Unlike in the U.S. and Western Democracies, and like Putin's Russia, there is no bifurcation between the government, industry, and or criminal organizations.

Hence, for a prospective business deal with a company in the U.S., the Chinese company can partner with China's intelligence services to assist in negotiations, vulnerabilities, and utilization of any already acquired data from said U.S. company. Again, this is akin to a U.S. based company calling he CIA and NSA for assistance on preparing a bid to merge with a company outside the U.S. and use all types of classified collection to form a proposal or use during negotiations.

The willingness of China, and its intelligence services, to illegally, and legally obtain DATA to drive artificial intelligence, research and development programs, and to facilitate their military and economic goals without doing the hard work to independently develop on their own, drives at the heart of China's unfair practices.

From genomics and DNA to third party financial data stored in cloud services providers, to fertility to Internet of Things technology, the effort du jour is accumulation of data, and lots of it.

China continues to surprise the world by aggressively stifling their citizens via laws, regulations, unparalleled domestic surveillance, and a debilitating Social Credit Score for every citizen. And a conversation about what is occurring the Uyghurs is for another hearing.

China's efforts to prohibit and violate free speech inside the U.S. must be identified, exposed and mitigated. China conducts such activities on Chinese nationals and on American citizens. Similarly, the CCP utilizes a suite of capabilities to silence critics here in the U.S. when the activity is exposed. The utilization of the United Front Work Department to drive false narratives in social media and within mainstream print and television media is consistent and

enduring. There are numerous examples of such, however I want to reference just a few recent examples. The first is the Chinese Embassy in Washington DC pressuring Nobel scientists to censor their speeches at the 2021 Noble Prize Summit. The prize winners were bullied by the Government of China to disinvite the Dalai Lama for the award ceremony. The second example is Zoom executive charged for working with the Chinese intelligence services to disrupt Zoom calls in the U.S. commemorating Tiananmen Square. The third example is American actor John Cena apologizing, in Mandarin, because of the pressure Chinese officials placed on him, and Hollywood, because he referenced Taiwan as a country. The pressure being placed by China on Hollywood has grown to a credibility questioning level and impacts just about every decision they make with respect to scripts and potential villains. This is referred to as "apology diplomacy" and has been publicly visible for many years when CEOs and company executives must apologize to Xi or the China for indiscretions with respect to referring to Taiwan as an independent country.

The last example, I feel is the most disturbing effort by the CCP here on American soil. Operation Fox Hunt is an international effort by the CCP to identify, locate and attempt to bring back Chinese dissidents who have left China and are causing President XI and the Communist Party discontent. For almost a decade Chinese intelligence services have been building teams to conduct surveillance in the U.S., oftentimes falsely enter relationships with local law enforcement to garner information on who China claims are fugitives, and attempt to bring them back to China.

The willingness, ability, and success of the Communist Party of China to conduct such aggressive activity within the confines of America's boarders is disturbing and unacceptable.

From a cyber perspective, China has significant and unending resources to penetrate systems and obtain data, or sit dormant and wait, or to plant malware for future hostilities.

Just last week, the FBI unveiled details for the first time on a 2011-2013 Chinese state-sponsored cyber campaign against U.S. oil and natural gas pipeline companies that was designed to hold U.S. pipeline infrastructure at risk.

Additionally, in July 2021, DOJ unsealed an indictment charging four individuals working with China's MSS for a global cyber intrusion campaign targeting intellectual property and confidential business information, including infectious disease research. Targeted industries around the world included aviation, defense, education, government, health care, biopharmaceutical and maritime.

And lastly, in July 2021, NSA, FBI, CISA publicly released more than 50 cyber tactics and tools used by Chinese state-sponsored hackers against the U.S. as well as mitigation steps for US companies.

Over the past decade we have seen CCP cyber and insider threat breaches and criminality to such a level I fear we are becoming numb when it is identified. One such event was the Equifax breach in May of 2017. As former head of U.S. Intelligence, I consider this to be one of the CCP's greatest intelligence collection successes. More than 145 million Americans had all their financial data, nicely aggregated, to the CCP along with Equifax's trade secrets on how they acquired such data. That is every American adult. Anthem lost 80 million medical records in 2015, Marriott lost 500 million guest's records in 2014, and in 2015 OPM lost 21 million records to China's cyber theft. I would be remiss if I left out China's breach of multiple cloud service providers in which China obtained access to over 150 companies' data.

The Insider Threat epidemic originating from the CCP has been nothing short of devastating to the U.S. corporate world. Anyone can go to Department of Justice's web site and search economic espionage. The result is hard to swallow. And those listed cases are just what was identified, reported by a U.S. company, and then prosecuted. I will touch on the impact of economic espionage a bit later. Just this past April 2021, a former scientist at Coca-Cola and Eastman Chemical was convicted of economic espionage & theft of trade secrets, on behalf of the CCP. The scientist stole trade secrets related to formulations for bisphenol-A-free (BPA-free) coatings for the inside of beverage cans. The scientist was working with a corporate partner inside China to monetize the stolen data utilizing the new company in China. The CCP had invested millions in the shadow new company in China. The stolen trade secrets cost US companies approximately $120 million to develop per open-source reporting. This is one example from the dozens identified in the past five years.

When you combine the persistence of intent and capability for the CCP's cyber intrusion programs, with the onslaught of Insiders being arrested, indicted and convicted by the FBI and DOJ over the past decade, it creates a formidable mosaic of insurmountable levels. But it is not. With a comprehensive whole of government and whole of society approach of defending against China with awareness, strategy, enhanced defenses, practical mitigation programs, and a patriotic value-based return to great competition, the U.S. can begin change the course of history as I see it now.

So, what is current and next in the targeted view scope by the CCP? Look no further than President Biden's economic growth agenda and proposed congressional legislation detailing our strategic movement in the next few years. Electric vehicles, battery technology, bio agriculture, precision medicine and sustainable green energy. China manufactures, produces, and delivers 80 percent to the anti-biotics sold and utilized in the U.S. We cannot afford to continue to

allow China to control and/or manipulate our supply chain and potentially hold us hostage in the future.

I would be remiss if I did not reference the strategic and aggressive nature in which the CCP conducts malign foreign influence in the U.S. Unlike Russia's persistent attempts to undermine our democracy and sew discord, mostly at the federal level and within the U.S. Congress, the CCP strategically, and with precision, conducts nefarious influence campaigns at the state and local level.

I have referenced the influence success in Hollywood and the self-censoring which occurs to not offend China to ensure sales of their product to the Chinese markets. When it comes to Taiwan, the CCP becomes the most aggressive. Oftentimes state and local officials agree to travel to Taiwan to identify or negotiate economic investment opportunities. The CCP will undoubtedly apply holistic pressure to the local officials, from overt threats to subtle promises of economic infusion at the city or town level. There is most likely a company or business located inside an official's town which is heavily influenced or leveraged by prior investment by the CCP. China will apply pressure to that U.S. company and threaten to slow down production or manufacturing in China if the company officials do not apply their respective influence on the elected leader to not travel to Taiwan. This state or local official, or even U.S. Congressperson, may have no knowledge of China's intent beneath the surface. At the same time, and not coincidently, an op-ed or article will appear in the local newspaper downplaying economic investment opportunities in Taiwan and championing alternative efforts in China.

WHY IT ALL MATTERS:

In 2020, 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). To make it more relevant to Americans reading this, it is approximately $4,000 to $6,000 per American family of four…after taxes.

Additionally, in 2010 China had one company in the top ten of Forbes' Global 2000 list. In 2020 they had five. That is a 500 percent increase in one decade. Competition is great and necessary and is what made America the global leader we are today. However, I would proffer China's growth through any and all means is much less than fair competition. To reiterate, competition is always good, and necessary in any aspect. My question is…are we really competing? If we do not alter how we compete on the global ecosystem with awareness of China's methodology and practices, we will not be able to sustain or global position as the world leaders in technology, manufacturing, education, science, medicine, research, development, and thoughts and ideas. We must aggressively enhance our willingness to not only understand these threats and unfair practices

but be willing to create a robust public private partnership with intelligence sharing to combat the CCP while at the same time staying true to the values, morals, and rule of laws made America the greatest country in the world.

The Senate's recent passage of a bill to bolster competition and provide the much-needed resources to do so is a great start down this long road. However, we must also protect the fruits of this legislative labor from being stolen and siphoned out of the U.S. by the same techniques China successfully utilizes today. Otherwise, we will continue to conduct research and development which the CCP will obtain, legally, and illegally, to bolster their economic, geopolitical and military goals of global dominance well into the future.

In closing, I would like to thank this committee, and the Senate writ large, for acknowledging the significant threat posed by China, not only by holding this hearing, but with all the recent legislative actions the past year on combatting this threat as well as driving enhanced competition. Continuing to combat the threat posed by the CCP will take a whole of nation approach with a mutual fund analogous long-term commitment. Such an approach must start with robust and contextual awareness campaigns. The WHY matters. Regarding these awareness campaigns, we must be specific and reach a broad audience, from every level of government to university campuses, from board rooms to business schools, educating on how China's actions impair our competitive spirit by obtaining our research and development, trade secrets and intellectual property, and degrading our ability to maintain our role as economic global leaders. I have provided some recommendations for this committee, the IC, the administration, academia, research and development, as well as CEOs and board of directors in our holistic efforts to detect and deter these threats, as well as educate, inform, and compete. 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 the global dominance.

Lastly, 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. Chinese Nationals, or any person of Chinese ethnicity here in the U.S., or around the world, are not a threat and should NOT be racially targeted in any manner whatsoever. This is an issue pertaining to a communist country, with an autocratic dictator who is committed to human rights violations and stopping 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 much more dangerous to our viability as a nation.

Recommendations:

The holistic, and existential threat posed by the CCP is one of the few bipartisan agreements in the US Congress today. We must take this opportunity to expeditiously advise, inform, and detail the threat to every fabric of our society, and why it matters. We must, as a nation, compete at the highest level possible while at the same time understand why we are doing so, and what is at stake.

1. Enhanced and aggressive real time and actionable threat sharing 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. The analogy would be the Financial Services ISAC. This intelligence delivery mechanism should include the Intelligence Community, FBI, and CISA and have at is core constituency 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. The Senate must ensure the Intelligence Community is leaning aggressively forward in providing collected intelligence 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 to the private sector. Enhanced declassification of collected intelligence 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. Implementation of the legislatively proposed Malign Foreign Influence Center. Ensure the private sector will be a constituent of the intelligence derived.

4. Bipartisan congressionally led "China Threat Road Shows" to advice and inform of the threat to CEOs, Governors, and Boards of Directors in critical economic, research and manufacturing sectors.
5. Close governance and oversight of proposed China Competition legislation with measurable outcomes and effectiveness reviews. Particularly in the research and development space.

6. Create a panel of CEOs who can conversely advise and inform Congress, the IC, and U.S. Government entities on perspectives, challenges, and obstacles in the investment arena and private sector. Currently, there is no such venue existing. I would recommend a *Business Round Table* type of framework. Membership should be diverse and include but not limited to the following sectors: Financial Services, Telecommunications, Energy, Bio Pharmaceutical, Manufacturing, Aerospace, Transportation, Private Equity and Venture Capital. Select key government participants and encourage actionable outcomes. This entity should be co-chaired by a CEO form this group.

7. Create a domestic version of the State Department's Global Engagement Center. The IC, and U.S. government needs a "sales and marketing" capability which can partner with U.S. business and academia to guide new and emerging threat intelligence, answer pertinent questions, and construct awareness campaigns against the threat from the CCP and other similar issues.

8. Establish an over-the-horizon panel to discuss, in a public forum, emerging threats posed 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, as well as the Federal Thrift Savings Plan.

9. Immediately create a Supply Chain Intelligence function which can sit both in the Intelligence Community as well as outside to facilitate real time intelligence sharing. This entity should include members of the private sector skilled in understanding our supply chain and who can expedite reacting to emerging threats. This entity will also be able to provide the U.S. Government cogent mitigation strategies and assistance with policy formulation to protect our vulnerable supply chain from persistent penetration and manipulation by China and Russia.

STATEMENT OF ANNA PUGLISI, SENIOR FELLOW, CENTER FOR SECURITY AND EMERGING TECHNOLOGY (CSET) AT GEORGETOWN UNIVERSITY

Ms. PUGLISI. Thank you. Chairman Warner, Ranking Member Rubio, Members of the Committee, thank you for the opportunity to testify today. The issues we are going to discuss will make us uncomfortable because they touch on the core beliefs and assumptions we make as Americans regarding democracy, opportunity, capitalism, open markets, and the importance and role of immigrants throughout the history of the U.S. My own grandparents were immigrants who came here to this country with little formal education, worked menial jobs, and made a new life for themselves.

My presence here today is a testament to the American dream. I want to start with saying that there's no room for xenophobia or ethnic profiling in the U.S. It goes against everything we have stood for as a Nation. And precisely because of these values, we need to find a principled way forward. The issues should not be seen as concerns of one Administration or the policies of one political party. But as the challenges created by a nation-state that is ever more authoritarian and that has a different system, a different regard for human rights, and a different view of competition and fairness.

Since you have my written testimony, I will focus my remarks on some of the highlights.

China is engaged in a strategic rivalry with the U.S. centered on economic power. China's management of its relationship with the U.S. has been designed to mask key aspects of this rivalry. This is why it's so difficult to have these conversations. Beijing, in many ways, understands the societal tensions, and its statecraft is directed at them—exploiting identity politics and promoting any changes to U.S. policy as ethnic profiling. Extreme positions such as closing our eyes or closing the doors only benefits China. So, now, let's take a moment and talk about what's at stake.

United States science and technology dominance since World War II has underpinned U.S. national strength and soft power. Losing our technological edge and the influence it entails will have far-reaching implications beyond scientific disciplines. This is not only about military technologies. Future strengths will be built on 5G, AI, and biotechnology. And our systems are fundamentally not the same. China's central government policies and the role of the State create this different system. These include talent programs that exploit its diaspora, S&T development programs with acquisition strategies built into them, and China's policy on civil-military fusion.

Let me be clear, China says it will use any knowledge or technology it acquires for its military. This is not conjuncture or profiling or analysis but China's stated position—and, I would add, for decades. We should believe them. Given the scope and scale of China's activities, a re-evaluation of our underlying assumptions and how we evaluate risk will be essential to counter these efforts.

Therefore, I have the following recommendations.

First, we really do need to improve ourselves. The U.S. and other liberal democracies must invest in the future. And we also have to realize that not all discovery has immediate commercial applica-

tion. We need to focus on things that provide the highest value to the Nation instead of just the lowest cost. We must build research security into future funding programs.

We also need to face the facts as a society. Beijing doesn't play by fair market rules. It does not respect foreign intellectual property. It is willing to act directly and indirectly to ensure its favored companies win in the market. The result of this is that our companies and our researchers are not competing on an equal and level playing field, but instead are up against the strategy—and, I would add, the power and the money—of a nation-state.

We must increase transparency. Existing policies and laws are insufficient to address the level of influence the Chinese Communist Party exerts in our society, especially in academia. We must increase reporting requirements for foreign money at our academic and research institutes, and university government labs and research institutions should have clear reporting requirements and rules on the participation of foreign talent programs. That part really needs to be country agnostic.

We need to ensure true reciprocity. This is about fairness and market access. We can no longer allow China to weaponize its market, connecting China's reciprocity and sharing of scientific data to its access to U.S. institutions and big science facilities as the leverage point. For too long, we have looked the other way when China has not followed through on the details of its agreements that it has entered into.

We also need to bolster cooperation and the communication of risk with our allies and partners. What also makes these conversations difficult, and as my colleague has alluded to, is that the reality that China is presenting is inconvenient to those that are benefiting in the short-term. This includes companies looking for short-term profits, academics that benefit personally from funding and cheap labor in the laboratories, and former government officials who cash in as lobbyists for China state-owned and state-supported companies.

We need to move beyond tactical solutions and have a comprehensive strategy for how we deal with China.

So, I would like to thank the Committee once again for continuing to discuss this issue. These are hard conversations that we, as a Nation, must have if we are going to protect and promote U.S. competitiveness, future developments, and our values. If we do not highlight and address China's policies that violate global norms and our values, we give credence to a system that undermines fairness, openness, and human rights.

The Chinese people deserve better, the U.S. people deserve better, and I think our future really depends on it. So, thank you.

Chairman WARNER. Thank you, Anna.

And now, I think we're going to hear from Matt Pottinger via WebEx.

[The prepared statement of Ms. Puglisi follows:]

Testimony before the SSCI

Anna B. Puglisi
Senior Fellow, Center for Security and Emerging Technology, Georgetown University
August 4, 2021

Chairman Warner, Ranking Member Rubio, members of the Committee: Thank you for the opportunity to testify. Perhaps no other issue is as controversial or challenging as the one we are discussing today. It is wrapped up in the fundamental feelings we have as Americans regarding democracy, opportunity, capitalism, open markets and the importance of immigrants throughout U.S. history.

My own grandparents were immigrants who came to this country with little formal education, worked menial jobs and made a new life for themselves. My presence here today is a testament to the American Dream. I want to start with saying that there is no room for xenophobia or ethnic profiling in the United States -- it goes against everything we have stood for as a nation.

And precisely because of these values, the issues we are discussing today will make us uncomfortable as we move forward to find principled ways to mitigate the policies of a nation-state that is ever more authoritarian, does not share our values and seeks to undermine the global norms of science and commerce. These challenges are not about the concerns of one administration or the policies of one political party, but the actions of a nation-state with a different system, different regard for human rights and different view of competition. The PRC has demonstrated a will to flaunt global norms to reach its strategic goals, and has put in place policies and programs that undermine the very values we hold dear: a fair and level playing field, transparency, reciprocity and market-driven competition.[i] These actions have far-reaching implications for the future of our nation and our ability to compete. On the committee's request, my testimony today will focus on China's use of non-traditional collectors, targeting of academia and theft of intellectual property, what is at stake and the long-term consequence of inaction. I will cover the following points:

- China is engaged in a strategic rivalry with the United States, centered on economic power. It has an all of-government strategy to target the foundation of that power—our technology and human capital.
- China's management of its relationship with the United States, despite implementing these policies, has been designed to mask key aspects of this rivalry. This is part of what makes these discussions so difficult.
- Beijing in many ways understands our societal tensions, which include race issues, and its statecraft is directed at them, exploiting identity politics by promoting any changes in U.S. policy as ethnic profiling, offering a narrative about being merely a proponent of "development" and science, in order to divert attention from its own questionable behavior. This is a well-funded effort.[ii]
- China has controlled the narrative despite violating the global norms of business and research, and as a result, many of the impacted groups do not recognize the growing challenge that this rivalry poses and often questions if there is actually a problem, despite the growing evidence that China is doubling down on its policies and programs.

- Beijing has made talent development and the exploitation of overseas students, universities, and government labs a central part of its technology acquisition strategy since the country's "opening" around 1978[iii]

- Regardless of their personal views, Chinese scientists, businesspeople and officials have to respond to the government or security services if they are asked for information or data. China intimidates and harshly silences its critics—this has only grown more so in the past few years.[iv]

- Our institutions were not designed to counter the threat to academic freedom and manipulation of public opinion that China's policies and actions pose.

- China's engagement with U.S. companies, universities and civic organizations has not led to a more open society in China or an equal playing field for Western companies in China. On the contrary, it has led to U.S. companies self-censoring themselves when it comes to human rights and issues of importance to the PRC—such as Taiwan—and U.S. universities accepting limits on academic freedom and freedom of speech. This is evidenced by those that criticize the Chinese government being denied visas and also more recently the harassment of foreign journalists. [v]

- Extreme propositions, such as closing our eyes (laissez faire) or closing our doors, only benefit China—the latter by discrediting en masse all efforts to address the problem and by depriving ourselves of the contributions of foreign-born scientists.

What is at stake: The importance of S&T

China's stated goal is to dominate in key technology areas. The United States' science and technology (S&T) dominance since World War II has underpinned U.S. national strength and soft power. Losing our technological edge and the influence it entails will have far-reaching implications beyond scientific disciplines. This is not to say that the United States needs to lead in every area, but that there are key economic and national security relevant areas and infrastructure that are at stake. Increasingly this is also not about military technologies, but dual-use technologies and commercial applications. Future strength will be built on 5G, AI and biotechnology. We have not lived in a world where the United States has been number two in foundational technology areas such as these.

- Beijing views technology—and the robust S&T infrastructure needed to develop it—as a national asset. The way it has structured its system to reach this goal is inherently at odds with key assumptions of globalization including open markets, reciprocity, transparency and findings being shared equally and unencumbered.[vi] China's leaders make no effort to hide their views of the importance of technological and commercial dominance, and how they view a robust S&T infrastructure as key to building a modern advanced economy, not necessarily an open market economy.

What is clear and well documented is that Beijing—especially Xi—looks at development as a zero sum game and that government support for key industries—the emerging technologies such as AI, next generation communications and biotechnology—gives China an advantage. Xi's statements include the following[vii]:

- "We should seize the commanding heights of technological innovation" May 2018

- "Artificial Intelligence is a vital driving force for a new round of technological revolution and industrial transformation. China must control artificial intelligence and ensure it is securely kept in our own hands." October 31, 2018. [viii]

- "Science and technology is a national weapon" and that "if China wants to be strong… it must have powerful science and technology." [ix]

- "In today's world, S&T innovation has become a critical support for increasing comprehensive national strength…whoever holds the key to S&T innovation makes an offensive move in the chess game of S&T innovation and will be able to preempt the rivals and win the advantages." [x] June 9. 2014.

Our Systems are not the Same

The current debate on how to deal with China as a strategic competitor rarely acknowledges the assumptions that have shaped how the United States and other economically developed nations forged ahead with engagement, commerce and scientific collaborations with China. Discussions about the benefits of globalization, decoupling, techno-nationalism and what it takes to be innovative are all shaped by this. These core beliefs have the following underlying assumptions: that you need democracy to be innovative and creative, that you need a market economy to be successful, and that we—especially the United States—will always out-innovate them. In practice, these beliefs play out in the following way:

- We are not a US business, we are a global one
- Innovation comes from the private sector, not government investments
- Everyone has the same driver—making money

However, the biggest assumption has been that China would change and acquiesce to the belief system of western capitalism and globalization. But China's actions tell a different story.

China's system is different because of the role of the state that permeates all aspects of society from Party cells in businesses-including western ones, a Party Secretary at universities that has more power than the university president and the social credit system that impacts daily life. Chinese students are sent overseas to learn with a purpose, and its business and S&T collaborations are designed to deliver maximum returns to the state[xi]. Although Beijing has not always been successful in this endeavor, its strategy illustrates a government with a plan and the political will to take a long-term view of development, invest in infrastructure and people and put in place the building blocks it needs to support China's economy and military modernization. It is masterful at setting the terms of those engagements to achieve long-term goals determined by the state.[xii]

What China has done with 5G is an example of how China pursues technologies that are critical foundational elements of the modern world. China uses its instruments of national power to position its companies in leading roles in critical technology niches, such as the next generation of communications infrastructure. China does this because it recognizes the many economic and security benefits these sectors will produce. This is what is at stake. [xiii]

Human Cost of China's Behavior: The Role of Non-Traditional Collectors

One of the biggest challenges to understanding the scale and scope of China's actions, and designing mitigation strategies is China's use of what are called "non-traditional collectors." These are the experts—scientists, students and business people—who work on particular research projects in different industries and target technology and technological information. This is a different methodology and is documented in Chinese language policy documents over the last several decades[xiv]. Our system—and I would add our institutions and the authorities we have granted them—is not designed to counter this kind of threat. Traditionally counterintelligence has focused on intelligence officers, military end-use and

illegal activities. I tell you today, if we only focus on trying to mitigate China's illegal actions, or those undertaken by intelligence officers or only are related to military technology, we will fail.

The Chinese government's explicit efforts to exploit its diaspora—and our innovation base—must be addressed and countered. China's exploitation of its diaspora is also a threat to the great majority of persons of Chinese ethnicity who play no part in this, but are tarnished and may be subject to unjustified criticism because of China's actions. This makes for a difficult balance. Our response must be two-handed—protect the rights of the people targeted by the Chinese Communist Party (CCP) while dealing with transgressions. Notable here is the fact that increasingly, the CCP targets non-ethnic Chinese, too, showing how this issue is not, in essence, one of ethnicity. Thus, the United States must continue to encourage academic exchange and an influx of scientific "talent" while at the same time find nuanced policy solutions, not only to stop the hemorrhaging of critical military and industrial technologies, but also, crucially, to "play offense" and continue to grow our national innovation base. This is also true for U.S. allies and like-minded countries worldwide.

The human cost of China's policies accrues in both directions, as Beijing disadvantages and tarnishes its own scientists who are trying honestly to work within global norms, because its domestic laws compel the disclosure of data/information. In this sense, the U.S. and other western countries are also culpable. By treating China as a neutral actor, and pretending that we operate within the same kind of system, we undercut those scientists and institutions in China trying to follow international norms. By not holding the Chinese government accountable, we give credence to a system that deprives China's educated elite from the dignity they aspire to and deserve. The Chinese people deserve better.

Policies That Create a Different System: Central Government S&T PLANS

Beijing's policies are dynamic and tailored to the changing landscape of technology development. The MLP, Made in China 2025, policies for Strategic Emerging Industries and the Five Year Plans are all policies that support China's S&T development.[xv] These are not isolated plans but a complementary web of development and industrial policies for emerging technologies to achieve its goal of technological leadership. The policies focus not only on specific technology areas but seek to create the environment to foster innovation and development, and most importantly build a national innovation base that will be the foundation for future economic growth and military modernization that Beijing controls.

- This is best illustrated by the "13th Five-year Plan for Military and Civil Fusion"[xvi] established in 2017 and focused on emerging technologies. The plan specifically calls for a "cross-pollination of military and civilian technology in areas not traditionally seen as 'national security issues,' such as quantum telecommunication and computing, neuroscience and brain-inspired research," and states that such projects will be supported by foreign outreach initiatives. In addition to these overarching projects, there are programs to develop specific high-tech areas such as biotechnology, integrated circuits, and "next-generation" artificial intelligence.
- Each of these programs highlights the role foreign "talent" is expected to play and how it is to fill key knowledge gaps. This is also reflected in earlier central government plans such as the Medium Long Term Plan for S&T development that explicitly calls out leveraging collaborations with universities and multinational corporations to gain key technology for China.

Civil-Military Fusion/Civil Military Integration

China says it will use any knowledge or technology it acquires for its military. This is not conjecture, profiling, or analysis, but China's stated position for decades. From early military-civilian integration (军民结合) policies to the more recent military-civilian fusion (军民融合), China takes a holistic approach to development, blurring what is civilian, what is military, what is private and what is public. This impacts the basis for entry of Chinese students and post-docs into U.S. labs because of China's ability to compel citizens to share information. It also challenges existing export and visa policies that build their restrictions around affiliations with a military end-user but make exceptions for civilian uses. To the Chinese leadership, every civilian use is also a potential military use.

Talent Programs[xvii]

The CCP and Chinese government continue to view Western education—and universities—as an entry point into the U.S. innovation base because it is an easier target. Xi has called human capital the "first resource" [xviii] and China's policies reflect this.

- Chinese government's National Medium and Long-term Talent Development Plan (2010–2020), stated that talent was core to the country's social and economic development and set detailed national talent targets. [xix]
- 2017: "Plan to Build a National Technology Transfer System." A comprehensive articulation of China's tech transfer system. The acquisition of "high-level overseas talent"—both ethnic Chinese scientists from abroad and other foreign scientists—is emphasized throughout.
- 2016: "Planning Guide for Manufacturing Talent Development." Joint plan to import (another) "1000" foreign experts able to make "breakthrough" improvements, via talent programs and other venues. Emphasizes recruiting from "famous overseas companies."
- CAST's "HOME Program" (or Haizhi Plan, 海智计划)," instituted in 2004 by the Chinese Association for Science and Technology to "Help Our Motherland through Elite Intellectual Resources from Overseas," and supported by China's central and local governments. Its 2019 slate includes 29 projects.[xx]

In addition to these overarching projects, as mentioned previously there are programs to develop specific high-tech areas such as biotechnology, integrated circuits, and "next-generation" artificial intelligence. Each such program highlights the role foreign "talent" is expected to play. [xxi]

What is at Stake: Non-Military Examples of China's Policies--Biotechnology and Renewable Energy

GMOs

Food security, throughout history, has been a major issue for Chinese leaders and related to ensuring regime stability. While other countries have similar goals, what is different is the role of the State in technology acquisition programs that target foreign technology and knowledge to meet this goal. China has made developing genetically modified crops a key part of its development strategy. They are not only highlighted in the general "biotechnology" area of the MLP and Five Year Plans, but are also called out as a mega-project, a Strategic Emerging Industry and mentioned in what was Made In China 2025. [xxii] To put in perspective what is at stake for U.S. farmers, the USDA estimates China's corn consumption will increase by 41% by 2023.

The case of Mo Hailong illustrates how China's policies lead to technology acquisition and the behaviors we are discussing today. Mo and his co-conspirators were found digging up test seed in an Iowa field in 2011[xxiii]. Mo operated a subsidiary of a state-supported Chinese company Da Bei Nong called

KingsNower and was sending these seeds to China. While Mo was arrested, spent time in prison and had to pay restitution, these seeds represent the most time and resource intensive portion of the development cycle for U.S. industry. China still acquired the technology. More seeds that a company in China sells—that were based on proprietary technology valued at millions of dollars—means fewer seeds that can be sold by U.S. companies. Given how China leverages and restricts its market, U.S. farmers may find themselves having to buy seeds from China's companies in order to sell their products in China.

Wind turbines

Another example of the impact of China's policies is wind turbines. This technology has been deemed a "Strategic Emerging Industry" in China, and is also highlighted in Made In China 2025. China has legitimate reasons for wanting renewable sources of energy, including some of the worst air pollution in the world. However, it has also stated that it wants to dominate in these areas, seeing increasing demand for renewables worldwide growing as more and more countries try to cut back on fossil fuels as a way to mitigate climate change. This is another area where China is willing to pursue its development in ways that are not bound by normative principles of global norms and include technology acquisition from other companies. In 2005, American Superconductor Corporation (AMSC) entered into a partnership with the Chinese company Sinovel that included wind turbine design and engineering services, including the software to regulate the flow of electricity between the turbines and the grid—which is the key piece of technology.

By 2011 Sinovel was the largest wind turbine manufacturer in China and the second-largest in the world. In March of 2011, an employee of AMSC received $15,000 to transfer AMSC's proprietary control software technology to Sinovel managers, and Sinovel severed its business relationship with AMSC. At this point in time AMSC was not aware that the business deal was severed, because Sinovel now had the key piece of technology and no longer needed AMSC. When AMSC announced publicly that it lost its business deal with Sinovel, its stock price dropped 40% in one day. Over the following two years, 500 of AMSC's 700 employees lost their jobs.

This is the real impact that China's actions have on U.S. workers. Academics and economists often debate whether what China does is "efficient" and argue that its system is not sustainable. However, even if this is true, the amount of damage that this behavior has, and will continue to have, on U.S. companies and citizens is far-reaching. What happened to AMSC illustrates the cost of doing nothing and allowing China's state run central policies to continue unabated.

Medical Research

Medical research is usually not associated with national security, but China has made dominating biotechnology and the global pharmaceutical industry a priority, and has adopted supporting policies such as Made in China 2025 and the Precision Medicine Initiative to reach this goal. These activities include targeting early developments of cutting edge research—often at universities or government labs—buying companies with key technology, and becoming a chokepoint for vital pharmaceutical ingredients, generic medicines and non-human primates.

China targets not only cutting-edge technologies, but also key resources on which the world is dependent. The last U.S. manufacturer of penicillin went out of business after China dumped chemicals at low prices for a four-year period. The Chinese government in this case actually filed a brief saying the companies had to set prices because of China's law. China has also said that it wants to make generic versions of 90% of blockbuster drugs with expired patents. How many other companies will go out of business because of these actions? The United States is reliant on China for penicillin, many of the ingredients that go into other medicines, and as we recently saw, key parts of the personal protective equipment supply chain. [xxiv]

China, as it has become more capable, targets early in the development cycle—the basic and applied research at universities and government and corporate labs. Recent cases at MD Anderson illustrate this. In this instance, grant proposals sent to U.S. based scientists to be peer-reviewed—which is supposed to be confidential—were instead sent to colleagues of the U.S.-based reviewer in China. This information was used to set up "shadow labs" in China that utilized the data and scientific knowledge of the U.S. grant proposals. The benefits of that research went to the Chinese institution and researchers not the U.S. institution and the U.S. taxpayers funding the work. This illustrates how stealing ideas gives China an advantage in new areas, as they have their own ideas to work with, as well as ours. It is naïve at best to believe that developments made by China will be shared equally, without restrictions or strings attached, because it is what is best for humankind. The current COVID-19 pandemic, and China's lack of transparency, demonstrate that this is not the case. What is at stake, according to Dr. Pisters, President of MD Anderson Cancer Center, is "the integrity of the peer review system" and the "intellectual property that is being created by U.S. based investigators."[xxv] This system is what has sustained U.S. competitiveness and innovation for decades.

CONCLUSIONS

China's strategy to target U.S. technology is coordinated, massive, comprehensive and effective. While its goal is technological self-sufficiency, China is not taking the path of free and fair market competition to achieve this goal. Instead, China uses a variety of methods to achieve a playing field tilted entirely in its favor. These methods include cooperative agreements that are leveraged and exploited to obtain technology above and beyond what is agreed upon, illicit front companies, end-user acquisition, and cyber and non-traditional collectors. Our companies and researchers are not competing on an equal and level playing field, but are instead up against the strategy—and power and money—of a nation-state that has the political will to see these efforts through over decades. These cases highlight the challenge that the United States and like-minded countries face in developing mitigation strategies to address the following:

- Clear policies and guidelines set forth by the Chinese government that incentivize all aspects of China's S&T infrastructure—including universities, companies and S&T Diplomats[xxvi]—to meet the nation's goals.
- Detailed technical requirements that come straight from the Chinese entity in need of specific technology or technological know-how.
- Support from Beijing that isn't focused on private wealth generation or efficiency in the short-term, but designed to build capacity and foundations for future industries and growth.

Given the scope and scale of this activity, and that fact that it is often focused on civilian technologies, a re-evaluation of our underlying assumptions and how we evaluate risk will be essential to counter these efforts. Therefore, I recommend the following:

Improve ourselves: The United States and other liberal democracies must invest in their futures. Not all discovery has immediate commercial applications—it took 30 years from discovery to development of the Lithium ion battery. We must accept that everything should not be only about the lowest cost, but instead focus on the highest value for the nation. We must build research security into future funding programs. What has been laid out here demonstrates the depth and breadth of China's efforts to target our technology, and the lengths it will go through to acquire it.

- The United States must encourage STEM education and create support networks for under-represented populations in the STEM fields. Many students leave STEM fields in the first year. If students are working their way through college, they may not have time for lab work or research

experiences. Funding should be provided for this, as we are leaving whole segments of our population behind.

Face the facts: Beijing doesn't play by free-market rules, it does not respect intellectual property, it is willing to act directly or indirectly to ensure its favored companies win in the market, and it doesn't share the same views on political openness the United States, Europe and other "like-minded" countries have long shared. Engagement with China has not made it more open, and it has not acquiesced to existing norms and rules. Acknowledging this reality complicates mitigation, because we are not negotiating on individual policies but against a different system. Moreover, the people who come here, however well-meaning they are personally, are to a greater or lesser extent beholden to China's system.

Increase Transparency: Existing policies and laws are insufficient to address the level of influence the Chinese Communist Party exerts in our society—especially in academia. The CCP exploits identity politics through United Front influence campaigns. This must be addressed and made public. By the same token, we must increase reporting requirements for foreign money at our academic and research institutes, as well as state and local governments to better identify these avenues of influence. Talent programs set up by the Chinese government, because of the restrictions and rules they place on the participants, present a conflict of commitment-where participants are often serving two different organizations which at best introduces conflicts of interest and in some cases fraud, and other illegal activity. Universities, government labs and research institutions should have clear reporting requirements and rules on participation.

Ensure True Reciprocity: Connecting China's reciprocity and sharing of scientific data to its access to U.S. institutions and big science facilities is a leverage point. For too long we have looked the other way when China has not followed through on the details of the agreements that it has entered into.

Bolster Cooperation and Alliances: Greater cooperation and integration with like minded countries of the European Union and Japan will not only foster the development of emerging tech industries, but also create alternative innovation hubs that mitigate China's unfair practices and continue to foster the global norms of science.

In closing, what will also make this difficult is that the reality that China is presenting is inconvenient to those benefiting in the short-term. This includes companies looking for short-term profits, not long-term sustainability of a particular industry, academics that benefit personally from funding or cheap labor in their labs, and former government officials who cash in as lobbyists for China's state-owned and state-supported companies. China is masterful at divide-and-conquer, identity politics, controlling the narrative and falsely presenting engagements as "win-win." In reality, China wins twice—both by gaining technology and controlling the narrative in such a way that its behavior, over time, gains legitimacy.

The United States has in many ways lost the PR war with China by not talking about the structural differences in our systems and instead focusing on individual instances of bad behavior that can seem anecdotal. This has essentially been a tactical approach—playing "whack a mole"—instead of a strategic one that presents a narrative painting the full picture of how China flaunts the values of globalization and increasingly promotes an alternative authoritarian system.

I want to thank the committee again for continuing to discuss this issue. These are hard conversations that we as a nation must have if we are to protect and promote U.S. competitiveness, future developments, and our values. If we do not highlight and address China's policies that violate global norms and our values we give credence to a system that undermines fairness, openness and human rights, and deprives China's educated elite of the dignity they aspire to and deserve. The Chinese people deserve better. The U.S. people deserve better. Our future depends on it.

[i] E.g., "The IP Commission Report." The Commission on the Theft of American Intellectual Property (May 2013). Hannas, Mulvenon and Puglisi, *Chinese Industrial Espionage*. (Routledge, 2013) hereafter "*CIE*." Michael Brown and Pavneet Singh, "China's Technology Transfer Strategy" (DIUX, February 2017). Section 301 *Report into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation*. Office of the United States Trade Representative (27 March 2018). U.S.-China Economic and Security Review Commission, "2019 Annual Report to Congress" (November 2019).

[ii] William C. Hannas and Didi Kirsten Tatlow, *Beyond Espionage: China's Quest for Foreign Technology* (Routledge 1st edition, September 2020); Alex Joske, "Hunting the Phoenix," Australian Strategic Policy Institute, 2020, https://www.aspi.org.au/report/hunting-phoenix ; Receipts of local UFWD paying overseas scientists available at: "The distribution list of provincial-level projects for the introduction of foreign intelligence special funds at the provincial level in 2018" [2018 **年省**级引进国外智利专项经费直项目分配明细表], https://web.archive.org/web/20201112190122/http://webcache.googleusercontent.com/search?q=cache%3AKAaZ3LpEe4oJ%3Arst.hunan.gov.cn%2Frst%2Fxxgk%2Ftzgg%2F201802%2F9516964%2Ffiles%2Fe1c7ddd51dda49f6b70a6ad5ae9b0490.xls+&cd=3&hl=en&ct=clnk&gl=us

[iii] IBID

[iv] **Roth, Kenneth "China's Global Threat to Human Rights", Global Report 2020**

[v] Mann, James "The China Fantasy: How Our Leaders Explain away Chinese Repressions" Viking 2007; Pomfret, John "What America didn't anticipate about China" The Atlantic, 16 October 2019.

[vi] Hannas et al., "Chinese Industrial Espionage: Technology Acquisition and Military Modernization". Routledge, 2013

[vii] **在中国科学院第十九次院士大会、中国工程院第十四次院士大会上的讲话 （2018 年 5 月 28 日）(http://www.xinhuanet.com/politics/leaders/2018-05/28/c_1122901308.htm). Xi used a slightly different formulation of this line at a June 9, 2014 speech at CAS and CAE: 习近平：在中国科学院第十七次院士大会、中国工程院第十二次院士大会上的讲话（2014 年 6 月 9 日）(http://cpc.people.com.cn/n/2014/0610/c64094-25125594.html); See also how Xinhua emphasized this particular line of the speech with the headline here: 习近平：把关键技术掌握在自己手里 (http://www.xinhuanet.com//politics/2014-06/09/c_1111056694.htm); 习近平：为建设世界科技强国而奋斗 (http://www.xinhuanet.com/politics/2016-05/31/c_1118965169.htm)**

[viii] 国务院关于印发"十三五"国家战略性新兴产业发展规划的通知. State Council, 2016

[ix] 国家科技创新基地优化整合方案. MOST, MOF, National Development and Reform Commission, 2017

[x] "十三五" 科技军民融合发展专项规划. MOST, CMC, 2017.

[xi] Hannas and Tatlow, "China's Quest for Foreign Technology: Beyond Espionage" Routledge, 2020

[xii] Hannas and Tatlow, "China's Quest for Foreign Technology: Beyond Espionage" Routledge, 2020.

[xiii] Alex Rubin, Alan Omar Loera Martinez, Jake Dow, and Anna Puglisi "The Huawei Moment" (Center for Security and Emerging Technology, July 2021). https://doi.org/10.51593/20200079

[xiv] These policies include "two bases formula", "short-term visits" and "serve in place. See Hannas et al., Routledge 2013 more a more in depth treatment of these policies.

[xv] Simon and CAO, "China's Emerging Technological Edge: Assessing the Role of High-End Talent". Cambridge University Press, 2009; **Cong CAO, Richard Suttmeier, and Denis Fred Simon. "China's 15-year Science and Technology Plan," Physics Today, December (2006), pp. 38-43;** Hannas et al., "Chinese Industrial Espionage: Technology Acquisition and Military Modernization" Routledge, 2013.

[xvi] Translation of "The 13th Five-Year Special Plan for S&T Military-Civil Fusion Development" ["十三五"科技军民融合发展专项规划], Center for Security and Emerging Technology; "Opinions on the In-Depth Development of Military-Civil Fusion" [军民融合深度发展的意见], General Office of the State Council on Promoting the National Defense Technology Industry [国务院办公厅关于推动国防科技工业], December 2017, https://perma.cc/4M58-X4C2; "'Military-to-civilian' and 'civilian-to-military' pace accelerates, the development of MCF continues to release new momentum" ["军转民""民参军"步伐加快军民融合发展持续释放新动能], China Financial News Network [中国金融新闻网], August 1, 2018, https://perma.cc/B4FH-H2SK

[xvii] Original CSET Data Visualization, "Chinese Talent Program Tracker," Center for Security and Emerging Technology, November 2020. https://doi.org/10.51593/20200066

[xviii] **"十三五" 生物技术创新专项规划 (*13th Five-year Plan for Biotechnology Innovation*). MOST, 2017**; 国家集成电路产业发展推进纲要 **(National Integrated Circuit Industry Development Plan). State Council, 2014;** 新一代人工智能发展规划. **(Next-Generation Artificial Intelligence Development Plan). State Council, 2017; "Why is Xi Jinping's 'First Resource' so important?" ["习近平眼里的"第一资源"为何如此**

重要"], ***People*** **[人民网], July 18, 2018, http://politics.people.com.cn/n1/2018/0718/c1001-30155931.html.; 国家技术转移体系建设方案. State Council, 2017; 制造业人才发展规划指南. MOE, MHRSS, MIIT, 2016.**

[xix] "十三五" 科技军民融合发展专项规划. MOST, CMC, 2017.

[xx] Hannas and Tatlow, "China's Quest for Foreign Technology: Beyond Espionage" Routledge, 2020.

[xxi] "十三五" 科技军民融合发展专项规划. MOST, CMC, 2017; "十三五" 生物技术创新专项规划 (*13th Five-year Plan for Biotechnology Innovation*). MOST, 2017; 国家集成电路产业发展推进纲要 (National Integrated Circuit Industry Development Plan). State Council, 2014; 新一代人工智能发展规划. (Next-Generation Artificial Intelligence Development Plan). State Council, 2017.

[xxii] Notice on Issuing "Made in China 2025" (State Council, Guo Fa 2015 No. 28, issued 8 May 2015; Decision on accelerating the Cultivation and Development of Strategic Emerging Industries (Guo Fa (2010) No. 32, issued 10 Oct 2010;

[xxiii] "The Saga of the Chinese spies and the stolen corn seeds, will it discourage economic espionage" LA Times, 31 October 16; Farm Journal Ag Web, "Mo Hailong Pleads Guity to Seed Theft Conspiracy", 28 Jan 16;

[xxiv] Gibson, Rosemary " China RX: Exposing the Risks of America's Dependence on China for Medicine". Prometheus Books, 2018.

[xxv] "MD Anderson Researchers Ousted as NIH and FBI Target Diversion of Intellectual Property", The Cancer Letter, 26 April 2019.

[xxvi] Ryan Fedasiuk, Emily Weinstein, and Anna Puglisi, "China's Foreign Technology Wish List" (Center for Security and Emerging Technology, May 2021). https://doi.org/10.51593/20210009

STATEMENT OF MATT POTTINGER, DISTINGUISHED VISITING FELLOW, THE HOOVER INSTITUTE; FORMER DEPUTY NATIONAL ADVISOR FOR THE WHITE HOUSE

Mr. POTTINGER (via WebEx). Chairman Warner and Vice Chairman Rubio, thank you and your fellow Committee Members for hosting a public hearing on this very important topic.

Many Americans were slow to realize it, but Beijing's enmity for the United States really began decades ago. Ever since the Chinese Communist Party, or the CCP, came into power in 1949, it's cast the United States as an antagonist. And then three decades ago at the end of the cold war, Beijing quietly revised its grand strategy to regard Washington as its primary external adversary, and it embarked on a quest for regional, followed by global, dominance.

The United States and other free societies have belatedly woken up to this contest, and there's a welcome spirit of bipartisanship that's emerged on Capitol Hill. But even with this new consensus, we failed to adequately appreciate, I think, one of the most threatening elements of the Chinese strategy, and that's the way that it seeks to influence and coerce Americans, including political, business, and scientific leaders, in the service of Beijing's ambitions. So, the CCP's methods are really a manifestation of political warfare, which is the term that George Kennan, the chief architect of our cold war strategy of containment, used in a 1948 memo to describe the employment of all of the means at a nation's command short of war to achieve its national objectives.

So, that's what China is doing.

And one of the most crucial elements of Beijing's political warfare is its so-called United Front Work. So, United Front Work is an immense range of activities with no analog in democracies. China's leaders call it a "magic weapon," and the CCP's 95 million members are all required to participate in the system, which has many different branches. The United Front Work Department alone, which is just one branch, has three times as many cadres as the U.S. State Department has Foreign Service officers. Except instead of practicing diplomacy, the United Front gathers intelligence about and works to influence private citizens, as well as government officials overseas with a focus on foreign elites and the organizations they run, including businesses that you and Senator Rubio just mentioned. Peter Mattis, who detailed how United Front Work is organized during his 2019 testimony before the House Permanent Select Committee on Intelligence, said, "Put simply, United Front Work is conducted wherever the party is present." And the party is quite present here in the United States. Assembling dossiers on people has always been a feature of Leninist regimes. But Beijing's penetration of digital networks worldwide, including using 5G networks that you referenced, Chairman Warner, has really taken this to a new level. The party now compiles dossiers on millions of foreign citizens around the world, using the material that it gathers to influence, and target, and intimidate, reward, blackmail, flatter, and humiliate, and, ultimately, divide and conquer.

Bill Evanina's written testimony today makes plain that Beijing has stolen sensitive data sufficient to build a dossier on every single American adult and on many of our children, too, who are fair game under Beijing's rules of political warfare.

Newer to the Communist Party's arsenal is the exploitation of U.S. social media platforms. Over the past few years, Beijing has flooded U.S. platforms with overt and covert propaganda, amplified by proxies and bots. And the propaganda is focused not only on promoting whitewashed narratives of Beijing's policies, but also increasingly on exacerbating social tensions within the United States and other target nations. The Chinese government and its online proxies, for example, have for months promoted content that questions the effectiveness and safety of our Western-made COVID–19 vaccines. There's been some recent research by the Soufan Center that also found indications that China-based influence operations online are now outpacing Russian efforts to amplify some conspiracy theories.

So what are some of the things that Washington can do to address Beijing's political warfare?

First, I think we should stop funding technologies in China that are used to advance the surveillance state and the military of Beijing. Beijing's turning facial recognition, 5G, data mining, machine learning technologies, and others, not only against their own citizens but, increasingly, against Americans here at home. The executive orders that were issued by the Trump and Biden administrations that prohibit the U.S. purchase of stocks and bonds in 59 main Chinese companies is a good start. But the Treasury Department really needs to expand that list by orders of magnitude in order to better encompass the galaxy of Chinese companies that are developing these so-called dual-use technologies.

Congress should also look at revising the Foreign Agents Registration Act, or FARA, to include more robust reporting requirements, steeper penalties for noncompliance, and a publicly accessible database of FARA registrants and their activities that's updated regularly.

The United States can also do more to expose and confront Beijing's information warfare through our social media platforms. Remember, these are platforms that are themselves banned inside of China's own borders. U.S. social media companies have the technological know-how and resources to take a leading role in exposing and tamping down shadowy influence operations online, and the U.S. Government should partner more closely with Silicon Valley companies in this work. Washington should also partner with U.S. technology giants to make it easier for the Chinese people to safely access and exchange news, opinions, history, films, and satire with their fellow citizens and other people who are outside of China's Great Firewall.

Finally, we should do more to protect Chinese students and other Chinese nationals living here in the United States. Many people of Chinese descent, including some U.S. permanent residents and even U.S. citizens, live in fear that their family members back in China will be detained or otherwise punished for what their American relatives say or do here in the United States. And this kind of coercion by Beijing, among other things, has silenced countless Chinese-language news outlets around the world. So much so that there's almost no private Chinese-language news outlet left in the United States or abroad that doesn't toe to the Communist Party line. The U.S. Government can help by offering grants to promising

private outlets and also reenergizing some of the federally funded media such as Radio Free Asia.

And U.S. universities, maybe with help from the U.S. Government, should also hand a second smartphone to every Chinese national who comes to study in our schools in the United States so that they have a smartphone that is free from Chinese apps such as WeChat, which monitor users' activities and censor their news feeds.

Thanks very much.

[The prepared statement of Mr. Pottinger follows:]

STATEMENT OF MATTHEW F. POTTINGER, DISTINGUISHED VISITING FELLOW AT THE HOOVER INSTITUTION AND CHAIRMAN OF THE CHINA PROGRAM AT THE FOUNDATION FOR DEFENSE OF DEMOCRACIES

BEFORE THE SENATE SELECT COMMITTEE ON INTELLIGENCE

"BEIJING'S LONG ARM: THREATS TO U.S. NATIONAL SECURITY"

4 AUGUST 2021

Chairman Warner, Vice Chairman Rubio, I'd like to thank you and your fellow committee members for hosting a public hearing on this important topic.

Many Americans were slow to realize it, but Beijing's enmity for the United States began decades ago. Ever since taking power in 1949, the ruling Chinese Communist Party (or "CCP") has cast the United States as an antagonist. Then, three decades ago, at the end of the Cold War, Beijing quietly revised its grand strategy to regard Washington as its primary external adversary and embarked on a quest for regional, followed by global, dominance.

The United States and other free societies have belatedly woken up to this contest, and a welcome spirit of bipartisanship has emerged on Capitol Hill. But even this new consensus has failed to adequately appreciate one of the most threatening elements of Chinese strategy: the way it seeks to influence and coerce Americans, including political, business, and scientific leaders, in the service of Beijing's ambitions.

The CCP's methods are manifestations of "political warfare," the term that George Kennan, the chief architect of our Cold War strategy of containment, used in a 1948 memo to describe "the employment of all the

means at a nation's command, short of war, to achieve its national objectives."

One of the most crucial elements of Beijing's political warfare is so-called "United Front" work. United Front work is an immense range of activities with no analogue in democracies. China's leaders call it a "magic weapon." And the CCP's 95 million members are all required to participate in the system, which has many branches. The United Front Work Department alone has three times as many cadres as the U.S. State Department has Foreign Service officers. Instead of practicing diplomacy, however, the United Front gathers intelligence about and works to influence private citizens and government officials overseas, with a focus on foreign elites and the organizations they run.

Peter Mattis, who detailed how United Front work is organized during his 2019 testimony before the House Permanent Select Committee on Intelligence, said "Put simply, United Front work is conducted wherever the party is present." And the Party is quite present here in the United States.

Assembling dossiers on people has always been a feature of Leninist regimes. But Beijing's penetration of digital networks worldwide has taken this to a new level. The party compiles dossiers on millions of foreign citizens around the world, using the material it gathers to influence and intimidate, reward and blackmail, flatter and humiliate, divide and conquer.

As Bill Evanina's written testimony today made plain, Beijing has stolen sensitive data sufficient to build a dossier on every American adult—and on many of our children, too, who are fair game under Beijing's rules of political warfare.

Newer to the party's arsenal is the exploitation of U.S. social media platforms. Over the past few years, Beijing has flooded U.S. platforms with overt and covert propaganda, amplified by proxies and bots. The propaganda is focused not only on promoting whitewashed narratives of Beijing's policies, but also on exacerbating social tensions within the United States and other target nations.

The Chinese government and its online proxies, for example, have for months promoted content that questions the effectiveness and safety of Western-made CoViD-19 vaccines. Research by the Soufan Center has also found indications that China-based influence operations online are outpacing Russian efforts to amplify some conspiracy theories.

So what are some things Washington should do to address Beijing's political warfare?

* First, we should stop funding technologies in China that are used to advance their surveillance state and their military. Beijing is turning facial recognition, data-mining and machine-learning technologies not only against Chinese citizens, but increasingly against Americans here at home.

Executive orders issued by the Trump and Biden administrations that prohibit the U.S. purchase of stocks and bonds in 59 named Chinese companies are a good start. But the Treasury Department needs to expand that list by orders of magnitude to better encompass the galaxy of Chinese companies developing so-called dual-use technologies.

* Congress should look at revising the Foreign Agent Registration Act (FARA) to include more robust reporting requirements, steeper penalties for non-compliance, and a publicly-accessible database of FARA registrants updated frequently.

* The United States can also do more to expose and confront Beijing's information warfare over U.S. social media platforms—platforms that are themselves banned inside China's own borders. U.S. social media companies have the technological know-how and resources to take a leading role in exposing and tamping down shadowy influence operations. The US government should partner more closely with Silicon Valley companies in this work. Washington should also partner with U.S. technology giants to make it easier for the Chinese people to safely access and exchange news, opinions, history, films, and satire with their fellow citizens and people outside China's so-called Great Firewall.

* Finally, we should also do more to protect Chinese students and other Chinese nationals living in the United States. Many people of Chinese descent, including some U.S. permanent residents and U.S. citizens, live in fear that family members in China will be detained or otherwise punished for what their American relatives say or do inside the United States.

Coercion by Beijing has silenced countless Chinese-language news outlets around the world—so much so that almost no private Chinese language news outlets exist in the United States or abroad that don't toe the Communist Party's line.

The U.S. government can help by offering grants to promising private outlets and reenergizing federally funded media such as Radio Free Asia. U.S. universities, perhaps with help from the US government, should also hand a second smartphone to every Chinese national who comes to study in the United States—one free from Chinese apps such as WeChat, which the Chinese security apparatus uses to monitor users' activity and censor their news feeds.

Thank you.

-end-

Chairman WARNER. Again, I want to thank all three of our witnesses today. And, again, for late-arriving Members, we're going to go by traditional seniority and five minute rounds.

I also very much appreciate all three of you making the point that our beef is with the CCP and its leadership and not the Chinese people and surely not the Chinese diaspora—Chinese-Americans—and that there is no place for racists or xenophobic targeting in our country. And that, in many ways, would simply play into the hands of the CCP.

Let me start with a question, a question different than I was originally going to start with. I'm going to start with something that is currently taking place. As we know, or maybe I'm not sure most Americans know, in roughly 2015–2016, China changed its, in a sense, corporate legal framework to make explicitly clear that any Chinese company's first obligation was not to its shareholders or even its employees, but its first obligation was to the Communist Party.

Coincident with that same time, we have seen an emergence, oftentimes driven, as Bill pointed out, by intellectual property theft—we've seen an emergence of Chinese social media, delivery, other companies that have had some of the biggest returns of any companies in the world over the last few years: the Alibabas, the Baidus, the Tencents. What I'm not sure most folks have realized is that those companies and many others—the vast majority of their investors are either American or Westerners. Something unique has happened, though, starting with Jack Ma and Ant when they tried to go public a number of months back, and the government intervened and stopped that enterprise from going public. A number of other Chinese tech companies have now been cracked down upon.

You know, is this an ability to try to get their large tech companies under control the same way we are having that active debate in this country?

Is it, in a sense, a warning shot across the bow for those companies that are potentially been trying to go public either here in the United States or on the Hong Kong exchange as opposed to inside the PRC?

Or is it even a possibility that this is an effort, since these companies are not going away, to wash out those Western and American investors? Because we've seen the values of these companies in some cases decreased by 50 percent literally over the last 60 to 90 days, and then to have them, in a sense, refinanced with Chinese funds themselves with more compliant tech leadership. And I throw that out to all three of the members of the panel for comments.

Mr. POTTINGER. Senator, I thank you very much for that question and those points. You know, I think you're exactly right that what you're seeing now is a deliberate obliteration of the line, certainly, a blurring, but ultimately an obliteration of the line between private companies on the one hand and state-owned companies on the other in China. An obliteration of the line separating civilian companies on the one hand and military companies and institutions on the other. And even a blurring of the line between foreign-invested companies, you know, multinational companies so to speak, and domestic Chinese-state champions. Beijing's goal is to

re-concentrate the authority of the party over all of the economic life of Beijing. And that's really what this is about, much more than just wanting to assert control over data, although that's one of the other reasons that Beijing has been taking these steps against Alibaba and DiDi, and many, many others to come. There are a number of laws that force those functions that you referenced. I'd be happy to provide an index of some of those laws that require companies in China, including foreign joint ventures to, first and foremost, serve the national security interests of the party, to serve the party's broader interests, and to work at the behest of the security apparatus to do that.

Corporate governance in China is not what is represented in public filings to the Securities and Exchange Commission. I've been waiting, turning purple, holding my breath, waiting for the Securities and Exchange Commission to begin asserting its authority to actually recognize that the risk factors are not even remotely adequately addressed in the public filings of Chinese companies here in the United States.

Chairman WARNER. Matt, could I cut you off there? I'm going to try to adhere to my time, and I want to see if Anna or Bill have another comment on this topic as well.

Mr. EVANINA. Senator, just two foot stomps from your point and maybe amplify what Matt had mentioned, specifically for corporate America, the three laws that China initiated, two new security laws and one cyber law, I think, are critical for CEOs and investment folks in the United States to understand. Most importantly is from a technological perspective that every CISO and CIO in China for a Chinese company in China or abroad is mandated to provide third-party data to the intelligence organizations in China. So, if you are a U.S. company and you're partnering with a company in China, you have to be aware that any and all of your data will be provided to the intelligence services in China. That's number one.

Secondly, to your point, 13 of the 15 largest companies in China are state-owned or operated. There are only two left. Alibaba is one of the two left, and we see what's happened to them now overseas in China with the draconian efforts that Xi is employing.

Ms. PUGLISI. I just want to foot stomp on the laws, and that's something that we can provide to the Committee. But in some ways, to take a lighter attempt, they've actually said the quiet part out loud in seeing what's happening to these companies, because this actually is a really good demonstration of how different the systems are.

Chairman WARNER. I would point out, and before we move to the Vice Chairman, we had 13 of what we call our classified roadshows. Every industry, virtually every major college and university in America, participated in one or more of those—with the exception of private equity. The very private equity that funded some of these Chinese tech companies that are now getting absolutely creamed as the Chinese government reasserts control. Maybe they would have been better to take advantage of our repeated offers to meet with private equity in a classified setting, so they understood perhaps better what they were getting themselves into. So, I'm not shedding a lot of tears for some of their losses, but I do hope, on a going-

forward basis, they and others will continue to make sure that they go in with eyes wide open in terms of dealing with the PRC.

With that, Senator Rubio.

Vice Chairman RUBIO. Thank you.

Mr. Pottinger, let me start with you. Did China try to manipulate public opinion in the United States and around the world during the early days of the COVID pandemic?

Mr. POTTINGER. Senator Rubio, certainly, we saw all sorts of activity by Beijing. Overt propaganda as well as what I would call more "shadowy schemes" to influence and amplify messages that in many cases are disguised to appear as though they are organic discourse between private citizens, but are really core, very carefully, and well-resourced campaigns orchestrated by Chinese propaganda officials. Now, you're referencing the time early in the COVID epidemic. Some of the ones I can just think of off the top of my head were efforts to create doubt about the origins of this pandemic, in fact, to claim that the pandemic originated from the U.S. military. We saw efforts to undermine, as I mentioned earlier, the credibility of our vaccines. Certainly, quite a lot of propaganda, both overt and covert, designed to create distrust and a lack of faith in democracy as a whole, and to amp up and elevate the idea of Leninist totalitarianism as a somehow superior model in spite of what the record has been over the decades that the Chinese Communist Party has been in power. I'm thinking of the tens of millions of deaths of its own citizens from mismanagement from their government. So, the short answer is Yes, sir.

Vice Chairman RUBIO. Thank you. Ms. Puglisi, the National Counterintelligence and Security Center warned, I think, in February that China is collecting the medical data, the DNA, and the genomic data of Americans. Why do they want the DNA and genomic information of Americans?

Ms. PUGLISI. China has amassed the largest genomic holdings of anywhere in the world. One of the most important questions in the next generation of both medicine and also biological research is the genotype to phenotype. So, understanding what genes do. And so access to that kind of data, both their own and from other places in the world, gives them an advantage in figuring out some of those problems. We know from their central government policies and programs they have emphasized the importance of next-generation medicine and that is a huge focus for them.

Vice Chairman RUBIO. Meaning the designing of precision medicine that allows curing specific conditions in people with specific genetic makeups?

Ms. PUGLISI. Yes.

Vice Chairman RUBIO. Mr. Evanina, in your opinion, how confident is China in their ability to get American banks, American investment firms, and American big business? How confident are they in their ability to get these to act as their lobbyists here in Washington?

Mr. EVANINA. Senator Rubio, there's no lack of confidence. I don't believe that the Communist Party of China has any reticence to believe they can't acquire whatever they want to acquire. And you see currently now with the new movement of the Communist Party of China investing into pension funds, both at the state and local

level, as well as into our thrift savings plan federally. They do it in a sublime manner, sometimes shrouded in U.S. business investment and shrouded with third-party front companies to be able to get and corner the market, so to speak, in our investment funds.

So, they have no lack of confidence in acquiring anything they need in our financial services sector.

Vice Chairman RUBIO. And that's for sure. But I think the question was how confident are they in their ability to get an American company, for example, or a finance sector or what have you, to use the lure of access to the Chinese marketplace to get them to come back to Washington and lobby policymakers here against or for decisions that China favors? In essence, they deputize them to come back and say, "Don't do this," or "Don't do that." Their ability to turn these American entities into lobbyists for their preferred policy outcome in our policies.

Mr. EVANINA. Again, there's no lack of confidence, and we've seen that occur in other parts of Chinese lobbying here in D.C., hiring former Members of Congress, former members of the Administration, former members of large banks to be able to come back and lobby and explain China's methodology and their narrative as to why their funding is more important than any funding here. And I will reiterate Senator Warner's point that some of my activities subsequent to retirement, the private equity venture capital folks are saying they're getting 30 percent ROI from investments in China.

Vice Chairman RUBIO. Yes. And so, just real quick, tied to that. Are they forward-thinking enough to look at a state legislator, a mayor, a commissioner at a local level and say, that person may one day be a member of Congress? Let's start working them now, get close to them, and have them adopt our favorite narrative of China so that in the future, when they wind up in that position, they'll be more favorable to our views?

Mr. EVANINA. Absolutely, and it's common practice.

Chairman WARNER. I want to note that Senator Cornyn and Senator Feinstein did some very good work that all of us on the Committee supported on trying to strengthen some of those restrictions on that foreign investment with the CFIUS Act.

Senator Wyden.

Senator WYDEN. Thank you very much, Mr. Chairman. Thanks to all our panelists. I'm of the view that data is one of the most underappreciated threats to America's national security, and that is especially true when you're talking about Americans' data being exported to our adversaries. And it's already the case with the Chinese government, or hackers based in China, have stolen the personal information of hundreds of millions of Americans.

As a result, I have been pushing hard to enact a law that would ensure that Americans' most private data cannot be sold off in bulk to countries that would use it against us.

So, I want to pick up on one of the earlier questions one of my colleagues just asked about with respect to genetic data and because of the importance of this issue.

Mr. Evanina, I know you've spent a lot of time on this. How does the Chinese government actually obtain the genetic information of

Americans? And tell us for the record why that's so dangerous to national security.

Mr. EVANINA. Thank you, Senator Wyden.

I think there's a couple of aspects to this question. First is to foot stomp your message of China's demand for data. When we look at what they've accumulated in the last decade, I'll point to Equifax: 150 million Americans, all their financial data has been taken by China. I would say that it's unnecessary for China to procure or buy our data when they can come in and take it for free, because our lack of cybersecurity defenses here provide an open door for them to take through spearfishing or other vectors to get into our systems and take our data.

With respect to DNA and genomics, they'll use front companies like BGI, which is a company around the world, to set up stations to collect COVID samples and do fertility clinics. And every single time you do that, you're giving away all your data to that node of that company, which as we said before, is now beholden to the Communist Party. So, as you provide genetics, blood typing, or any kind of COVID test, it's going to possibly go to the Chinese Communist Party, which is why we must protect what we do here on our soil from companies like Quest and other diagnostic companies, which are in every single town, from being procured by the Chinese government.

Senator WYDEN. I'm going to also hold the record open because I feel so strongly about this. For any additional information you can give us on exactly how they obtain the genetic information, because that's the threshold question. You know, when American companies are being purchased, there's the CFIUS process that addresses the purchase of American companies. But the purchasing and export of the data itself is totally unregulated, which is why I feel so strongly about this legislation. And so, if Mr. Evanina, in the next week or so, you could give us more information on how they actually go about doing it.

Question for you, Ms. Puglisi.

It's clear that the American government has been forcing the transfer of a number of valuable American innovations through legal acquisitions and illicit tactics. Another legislative initiative I'm pushing would require companies doing business in China to report on technology- and IP-transfers. In your view, wouldn't this requirement help the U.S. Government get a better sense of the problem and allow for our government as we try to put together an all-of-government response to come up with a better approach?

Ms. PUGLISI. So, I think that really gets at that transparency issue and understanding. I think, to step back from that as well, what's important is understanding what are the market conditions that are being set, because we know that China has used its market to force a technology transfer. And so, having a better understanding of, and also pushing back on that, will help both with that transparency piece and understanding the pressures that those U.S. companies are under.

Senator WYDEN. I'm over my time. I'm going to give you all a written question on hacking, which is sort of the other side of the coin.

Thank you, Mr. Chairman.

Chairman WARNER. Thank you, Senator Wyden. Senator Burr.

Senator BURR. Thank you, Mr. Chairman. Anna, I found your opening statement to be very clear and very diplomatic, I would say.

I'm going to read you a statement that I think encompasses the threat. You tell me what I've left out of it, if you will:

> The People's Republic of China is actively conducting multi-disciplined espionage operations against the United States. Further, the Chinese Communist Party is engaged in influence and intelligence operations inside the United States at an unprecedented scale, targeting numerous sectors of society, including the academic community, private sector, media platforms, and policymakers in order to advance its security and economic objectives and strengthen the CCP's hold on power. The CCP aims to acquire technology, conduct espionage, and shape narratives to align the CCP's ideology and objectives.

Is there anything you disagree with in that statement? Is there anything I've left out?

Ms. PUGLISI. The one thing I would like to highlight is that one of the challenges in dealing with how China targets our technology is they use a very different methodology. So, if we focus only on intelligence officers, things that have a direct military application, and things that are illegal, I believe we will fail. And so, it's looking at those gray areas and looking at how what started off as legitimate co-operations or collaborations or even business deals get moved into that gray area.

Senator BURR. Well, I think we would agree with you. Bill, the Department of Justice has used the name and shame program, the model of highlighting cases of Chinese espionage in the United States. And it currently makes the public more aware of CCP's nefarious activities within the U.S.

In your opinion, how effective is "name and shame," and what, if anything else, can be done to deter the Chinese?

Mr. EVANINA. Sir, I'm a big believer in the efficacy of name and shame. I think that when you look at Xi Jinping and his regime, what hurts him the most is any kind of negative consequence. And as we get the word out, not only around the globe—and as you know, in my previous role, I was head of counterintelligence for NATO. When I would speak to our NATO partners, they would be excited because of the naming and shaming, and the exploitation of criminal behavior by the Chinese communist regime. You have big cases—whether it be Huawei or any other kind of espionage investigation insiders of cyber—that get known around Europe and around South Asia and South America. So, it allows the U.S. Government, policymakers, intelligence services to garner support and build coalitions against China, whether it be Belt and Road or the economic proclivity in Europe. And I would proffer that the work the U.S. Government has done on Huawei, in calling out their nefarious behaviors, has done a whirlwind of efforts in Europe with the EU and NATO.

Senator BURR. Good.

Matt Pottinger, what technologies do you believe we must do a better job at protecting? And what's after 5G?

Mr. POTTINGER. Thank you, Senator. I think that we know from China's own strategy and from the actions in implementing that strategy that they've used semiconductor mastery—that is, all of

the elements including the fabrication of semiconductors—as the foundational technology upon which everything else that we're competing against China for in this century is resting on. So, whether we're talking about synthetic biology or 6G, 7G, advanced materials, and machine learning—all of this is built on advanced semiconductors; and Beijing is quite determined to make itself wholly independent of any other market for those semiconductors. And in ways that would also make us increasingly dependent on China so that they would have enormous coercive leverage over us.

So, I'm a free-market guy, but there's the one exception that I'm really making is that I believe that we do need to provide subsidies to bring back a certain amount of the manufacturing of semiconductors to the United States to remove that piece of leverage from China. So, semiconductors is number one.

In the area of 5G and the other generations of wireless and communications technology that are going to follow, we need to use our export controls more sharply than I think we've been using to date. We did some very important things in 2020: expanding the foreign direct-product rule, making it impossible essentially for heavily state-owned and state-subsidized companies like Huawei to obtain high-end semiconductors. We need to use those tools even more sharply now before we lose them. Again, we've got some companies in the United States that make great equipment for making semiconductors and they want to access the China market. In the long run, that's going to be very bad for us if we're giving China the means to create a coercive and wholly independent manufacturing capability. We want to bring some of that home, forgo some of those short-term, smaller profits now in order to grow a much larger pie after that.

Chairman WARNER. Thank you. And I just want to clear up one item, Bill. I think in your response to Senator Wyden, I believe your point was that we have to be careful about the Chinese, for example, acquiring certain American labs or other items. It's not the fact that if you get a COVID test right now, that data goes to China. So, just to be clear for the record.

Senator Heinrich.

Senator HEINRICH. Thank you, Chairman. I want to yield a little time to Senator King who has a pressing engagement.

Senator KING. I have a meeting that I have to go to, but I'll be submitting four questions for the record, and I hope you all will provide some of your good thinking on it. These are sort of thought questions based upon today's testimony.

Thank you all very much. Thank you, Mr. Chairman. Thank you.

Senator HEINRICH. You bet. You co-authored a recent report titled, "China's Foreign Technology Wish List," which looks at how China's science and tech diplomats working out of embassies and consulates across the world, act as brokers to acquire foreign technology. And the report notes that artificial intelligence, machine learning are sort of near the top of that wish list.

Can you discuss the role that these science and tech diplomats play in acquiring foreign technology? And what else are you seeing in the areas of AI and machine learning, in particular?

Ms. PUGLISI. Of course. So, I think the role of S&T diplomats, what it really highlights is the depth and breadth of China's tech

acquisition bureaucracy, as we laid out in this report. And this is based on Chinese-language documents that we have mined and acquired—these are all open-source material—that there's a demand signal. And so, the entity in China requests or highlights that they have a gap either in technology or knowledge that goes to a central database, and then it's actually farmed out across the world. And what's interesting about this is it really shows a nuanced understanding of where that technology is located and where to find that. And as you mentioned, the two things, the highest that showed up the most in our research, was both AI and machine learning and actually biotechnology. And one of the hubs of activity for that in the United States was the Houston consulate.

Senator HEINRICH. Very interesting. The CCP has leveraged individuals outside of government to pursue technology transfer, targeting foreign researchers and business leaders in order to transfer that technology back to the PRC. Can you walk us through any examples that are particularly illustrative, either in academia or in the private sector, just to give folks a sense for like how this tactic really plays out in real life?

Ms. PUGLISI. So, what I'll speak to is a specific methodology that we see and then—.

[Audio interruption.]

Is that better? Okay. Sorry about that. So, what is interesting in both as in my previous iteration working for—, we always get questions about, okay, what is the list, right? What are the technologies that are being sought? And we do have that in a very general sense. But what makes that so challenging is what we call the Chinese use of nontraditional collectors. And so, these are actually the experts that are working on a particular area, working on a particular project, that are the ones that are targeting the technologies.

What makes it so hard to counter a lot of times is initially, some of these relationships begin as legitimate, whether they be collaborations or individuals that either join universities or join companies. But China has a number of policies, and one of the ones that I think pertains to this particular type of targeting of technology is one called "serve in place." And it's something that we've seen reflected in Chinese policy documents since the early '90s. It articulates that they seek to leverage individuals who are not living in China, who don't have any intention to go back, and they reach out to those people to fill strategic gaps.

And increasingly even more so is the technological know-how. And so the how do you do things? How do you do quality control? How do you move technology out of the lab?

Senator HEINRICH. Wow.

Mr. Pottinger, could you talk a little bit more about semiconductor manufacturing and fabrication? And how would you rate our efforts so far at trying to start the process of bringing that back to domestic production? And what additional efforts would you recommend?

Mr. POTTINGER. Thanks, Senator.

So, the majority of the world's highest-end chips are actually made in Taiwan, by Taiwan's Semiconductor Manufacturing Corporation. China has put well over $100 billion in subsidies into try-

ing to replicate what Taiwan is able to do, and with very mixed results. In fact, they've not been able to replicate what Taiwan does. But what they are now trying to do, having recognized the fact they can't make chips at the bleeding, cutting edge the way that Taiwan makes them, China is trying to make chips that are a couple of generations older than the chips that Taiwan makes.

Now, older does not mean worse. Because, in fact, the device I'm talking to you on right now, or a personal smartphone is made up of ten chips, maybe only one of which is the really cutting-edge chip. The others, which control graphics and voice, and cameras, and things of that nature are older-technology chips, which make up a massive segment of the market. They're still extremely important and they can be leveraged in ways to make them greater than the sum of their parts, depending on how creatively you tie these things together. So, what we do in the United States—we don't make that many chips anymore. We have a couple of exceptions. There's a company called GlobalFoundries in upstate New York that makes chips that are a couple of generations older, but it turns out that our military, most of our equipment runs on chips that are a couple of generations or more older because those systems stayed in place for so long. So, it's been critical that we have a certain amount of manufacturing here at home.

Where we really lead is in the design of chips and also in equipment that's used in the fabrication of the chips. So, those are areas where we want to do a better job, more strategic job, of looking holistically at how we can deny China its very deliberate and clear objective of making itself completely independent and making us increasingly dependent on their supply for semiconductors, which until we have another technology, are absolutely essential to every area where we want to compete in the innovative economy.

Chairman WARNER. Thank you, Senator Heinrich. Senator Blunt.

Senator BLUNT. Thank you, Chairman. Ms. Puglisi, let's talk about campuses for a minute. Nothing creates more friends for the United States of America than time in the United States of America. And this research discussion is one discussion. Another discussion is there are lots of Chinese students on campuses that have fine business schools, that have good health programs of various kinds, and other programs that don't do a lot of research.

What are the dangers of us closing the door to smart, young, Chinese people who want to come here and spend a couple of years and how do we thread that needle?

Ms. PUGLISI. Senator, that's a really important point, and it's really important to distinguish between undergraduates, graduate students, graduate students that are studying things that we are concerned with. And I think it circles back to the remarks that I made about acknowledging how different our systems are. Because we can't possibly understand, I think my colleagues also spoke to this, the amount of pressure that some of those students can be under if their families are still in China. The most recent Global Human Rights Watch report that came out talks about surveillance happening on U.S. campuses of these Chinese students.

Senator BLUNT. Well, I think we have to be careful there, because just like we can't understand the pressure they're under, they can't understand what the United States is like in the same

way as if they were here. And, Chinese students, particularly undergraduate students in a non-research setting on campus, I think that's a different thing than people—technical research, calling back the results to the mock lab in China somewhere. I think we need to be really careful about this.

I'm going to go to Mr. Pottinger next.

It seems to me that there is a likely change in a mindset here. You know, we all know that China has a huge demographics problem, and I don't want to go down the demographics trail. The trail I want to go down is there are millions of young Chinese adults who in their whole life, they've had two parents who were totally focused on them. And four grandparents who had one grandchild also totally focused on them in a country that had more things to share, more ways to buy things for that one grandchild.

Are they going to have the same response to the increasingly repressive Chinese Communist Party the generation before have had? Are we seeing some likely pushback from young Chinese adults who've had basically all the attention you could possibly ask for their entire life and almost everything they wanted to have from parents and grandparents?

Mr. POTTINGER. Senator, there's been recent reporting, some interesting reports have been written about sort of this ennui that is afflicting the younger generation of Chinese young men and women. I think that the Communist Party systematically removed from Chinese culture so many of the elements that could enrich people's lives, including faith, including what had been in the late '90s into the early 2000s, a growing amount of free exchange and discourse. Those things are now going in reverse. You're seeing the systematic stamping out of civic life, whether it's secular or religious. The most extreme example is the genocide taking place against traditionally ethnic Muslim minorities in Northwest China, but also against Christians and others. And access to outside information is getting more restricted.

Senator BLUNT. Thank you. Let me see if I can add one quick question.

So, Bill Evanina, what of this more restricted society, in all ways you've looked at that, how is that coming generation going to react to that in a different way than their parents and grandparents have?

Mr. EVANINA. Senator, thanks for the question. I think your premise is correct. We are seeing that kind of slow change, but I would proffer that Xi Jinping is seeing that same change as well and he's becoming more draconian. They've become the most impressive surveillance state in the history of the world, not only domestically in China, but as well, as we heard, here in the U.S. Those 320,000 students who come to the U.S. are forced to have Chinese phones with WeChat so the Chinese can monitor them here.

So, when you are here, whether you're a student or researcher, and you get a call from the Ministry of Security asking you to do something for them and your grandmother is sick or your father needs a job, you are going to do whatever they ask you to do. So as much as we see a change in the want of the Chinese young peo-

ple to get Internet, the quicker we see that the quicker the Chinese Communist Party disallows them to have the Internet.

Senator BLUNT. Thank you. Thank you, Chairman.

Chairman WARNER. Thank you. Senator Bennet.

Senator BENNET. Mr. Chairman, I want to first start by thanking you for not just holding this hearing, but for the focus of the Intelligence Committee's attention on this subject for quite a while. I've been on the Committee now for three years and what I'm about to say, I didn't know before I had the benefit of the hearings that we have had, and that is that the Chinese Communist Party, the Chinese government, will use any means licit or illicit to pursue their China First policy. The question for us is whether we're willing or whether we're going to be collateral damage in all that.

And this isn't just a fight or a competition, let's use that language—a competition between two economies—it's a competition between democracy on the one hand and totalitarianism on the other. It doesn't have anything to do with, as you said, with the decision the Chinese people are making, but they are the decisions that the Chinese government has made, and increasingly, in the last decade, exported around the world. So we're facing the consequences of that all over the world. That creates a huge and heavy burden for us and for our democracy, I think. It calls into question some of the idiotic battles we've had around this place instead of our attention being focused where it ought to be focused.

It calls into question whether or not we've done enough to work with our allies and other democracies around the world and other economies around the world who share similar equities to ours with respect to China, which the good news is almost every other economy and every other democracy in the world. Not everyone, but almost everyone shares those equities. And that's why in the end, I'm optimistic. I think we can compete because I think we've got a much better system than they have—when it's working, properly when it's working well.

So, I actually, in all of that, have a question. Maybe I'll start with Mr. Pottinger just because he's not here and anybody else who would want to answer it. If you disagree with anything I said, please feel free to do that. This is America, you can do that and be happy to have it. But if you don't, I'd be curious what message you would like to send, to go back to the Chairman's initial question, to private equity firms in the United States, to their leadership, the leadership of venture capital firms, and other investment firms that are investing in Chinese technology. Imagining that somehow, it's not dual-use technology, imagining that somehow the Communist Party isn't going to be the beneficiary of this, and telling themselves that that ROI that Bill talked about, somehow, is worth whatever the risks are.

So why don't we start, Mr. Pottinger, with you?

Mr. POTTINGER. Thanks, Senator. I think that the argument on returns on investment is rapidly evaporating. We saw the obliteration of close to a trillion dollars in shareholder value just in the last several weeks as Chinese stocks were systematically rectified by regulators in Beijing. So that argument, I think, over time, is going to atrophy.

But what I would tell private equity investors, including venture capital investors, is that ultimately, many of the technologies that they're investing in, in fact, arguably almost every successful Chinese tech company that exists today, was seeded with Silicon Valley or other foreign venture capital money, as well as with Silicon Valley know-how. And we know that some of those companies have now applied their technology to some of the most nefarious human rights atrocities since the mid-20th century. So that is going to come back to haunt companies reputationally, in ways that I think a lot of companies aren't yet prepared for.

Senator BENNET. I have got 40 seconds left. I don't know if either of you would like to comment on that.

Mr. EVANINA. I would just like to amplify Matt's message. I would say, the most painful salt in the wound is when American investors invest in tech companies in China where that technology was stolen from the U.S. in the first place. And then we are forced to buy that technology as consumers at the end of the day. So, the fruits of our thoughts and our ideations in technology were stolen, and then they were forced to purchase them back from the Communist Party of China, is the painful salt in the wound.

Senator BENNET. Thank you, Mr. Chairman.

Chairman WARNER. Senator Cornyn.

Senator CORNYN. Well, in typical Washington fashion, let me start out with some acronyms: CFIUS, FIRRMA, ECRA, and FARA. I want to ask two questions about those topics.

One is in 2018, we did export control reforms. We reformed the Committee on Foreign Investment in the United States and gave the Treasury Department, which convenes the CFIUS, a lot more resources. And I'd like to get your analysis of what's changed and what needs to change, what hasn't changed.

And then, on FARA, we've done a lot of work, I know particularly in the Judiciary Committee, Senator Feinstein and Senator Grassley and me trying to get reforms of the Foreign Agents Registration Act. The Lobbying Disclosure Act, I think it's called, provides an out for foreign agents to register as lobbyists but not as foreign agents, and basically impeding the benefit of our knowing who's a foreign agent and who's not.

I think this is one of the biggest untold problems that we have dealing with foreign countries, including China, is we know other countries hire lobbyists and other agents. But if we don't know who they are and what their agenda is, it's pretty hard for us to put that in the proper context to protect ourselves. We're supposed to represent our constituents and Americans, not the interests of foreign countries, but if we don't know who's who, it's a real problem.

So I might ask the three of you, if you have something you could tell us about CFIUS and FIRRMA and export controls, and if you feel like we are where we need to be if there's more we need to do. And then, I think I heard Mr. Pottinger talk about FARA as I was walking in, but I would invite any one of the three of you to talk about that issue as well.

So maybe, Mr. Evanina, can we start with you?

Mr. EVANINA. Thank you, Senator.

Great question. And all three, CFIUS, FARA, and FIRRMA, are very important aspects of how the government deals with this epi-

demic. I do think that subsequent to legislation a few years ago, I think we still need to appropriate more resources to it. I think, yes, it was housed in Treasury, but there are multiple other agencies who can add value to that who did not increase resources to that effort. So, I do think it's the right vehicle. There are just not enough people in that vehicle to do that work. So, caution with that.

Secondarily, I think the premise of some of these is a little skewed because, as Anna talked about the nontraditional collectors who come here either wittingly or unwittingly working for the Communist Party of China, don't know their lobbyists and don't know they're here registering as a foreign agent. Most likely, they're not. And oftentimes, they can conduct high-level research at a ceramics lab or an institute and then get a phone call one day from someone back home. They don't know that they're an agent of a foreign power and they don't know that they're a lobbyist. So, I think, sometimes, the nomenclature and lexicon need to be shaped and formatted more toward the nontraditional collector.

Senator CORNYN. Ms. Puglisi, would you care to comment?

Ms. PUGLISI. So, it's encouraging, all of the hard work that everyone on the Committee has done, especially in these different areas. I think going forward, going back to my remarks, I think it's important to remember the multifaceted ways that China targets our technology and how different the systems are. I think one of the challenges, as we break this problem down into specific slices, we as a country, because we are a law-based society, because we are a rules-based society, try to get things narrow to a specific point. But when we're dealing with a non-rules-based adversary or entity, it makes those policies much more difficult to not only enforce but to have the desired outcome. And so I think as we move forward, we need to think about what is the desired outcome of the efforts across the board with technology acquisition and how do we mitigate some of these activities. And design policies and programs in addition to the ones that we already have that get at how do you deal with a non-rules-based entity.

Senator CORNYN. Mr. Pottinger, would you care to comment?

Mr. POTTINGER. Senator, thanks for your leadership on FIRRMA a few years back, which was a real improvement on CFIUS. I would say that where there's still a loophole is in the area of venture capital and private equity. Beijing benefits enormously just from having a seat on those funds. It gives it a sort of a panopticon to see all of the newly emerging companies and technologies that they want to then target for more in-depth scrutiny and investment and theft. On the FARA front, making it a searchable public database that's frequently updated so that it becomes much more public and much more comprehensive. All of that activity that you referring to, some of which is not currently captured but which needs to be. Thank you.

Chairman WARNER. Senator Casey.

Senator CASEY. Mr. Chairman, thanks for having this hearing and focusing our attention on these issues in this open setting.

I wanted to start by making reference to Mr. Evanina's background. He's a Lackawanna County, Pennsylvania native; a Valley View High School graduate; also a degree from Wilkes University.

So, I just hope after your career is over that you, at least, retire in Lackawanna County.

But we're grateful for your public service and for the work you continue to do, I will probably direct what I hope there would be two questions to Ms. Puglisi and Mr. Pottinger, but Bill, feel free to weigh in as well.

I wanted to start with an issue that Senator Cornyn and I worked on, especially in the lead-up to the most recent competition legislation. We introduced a bill called the National Critical Capabilities Defense Act. It would establish an interagency committee to review outbound transactions, not inbound, but outbound, by U.S. firms to nonmarket economies like China that would, in my judgment, the judgment that a lot of people result in the outsourcing of critical supply chains and create further U.S. dependence upon a nonmarket economy like China.

I guess my first question is to what extent is that kind of outbound investment by U.S. companies to nonmarket economies like China compromising our supply chain security and then subsequently our national security?

Ms. PUGLISI. Thank you, Senator. I am not familiar with the legislation that you put forward, but I will comment on the supply chain question, the latter part. I think it's very important. And we see just most recently with PPE and how unreliable some of those supplies were. A colleague of mine is doing a lot of research on medical supply chains, and especially as we discuss how do we have pandemic responsiveness when our supply chain, especially for APIs, especially for some basic drugs, are not located here. And so, I think, that gets back to the comment that I made in my prepared remarks about as we're examining the supply chains, we really need to look at what is the best value for the Nation as opposed to the lowest cost.

But that also gets at some of the market access issues as well, because we have seen cases—and I actually put in my written testimony—about cases where because of that market access, we have pharmaceutical companies that are sending or closing down those API, or can view more basic drugs manufacturing here, and actually manufacturing those in China. So, with the draw, then they'll be able to sell some of their more lucrative materials there.

Senator CASEY. Thank you. Mr. Pottinger, any thoughts you have?

Mr. POTTINGER. Thank you, Senator. I laud the goal that you're pursuing here with this legislation, which I haven't yet read. But look, the Department of Commerce has already declared six nations that are "adversaries" of the United States. China is at the top of the list, together with others that you might imagine—Russia and Iran and a few others. One of the reasons that Beijing may have felt so confident—and it really didn't bat an eye before destroying almost a trillion dollars in shareholder value in its publicly listed firms in the United States—was because it's getting tens of billions of dollars through other means from more passive sources in the United States. These are institutional investors who are passively tying their money in the form of bond purchases and stock purchases to indexes. These index providers are weighing Chinese companies much more heavily than they used to, even as China be-

comes less and less transparent of an ecosystem to invest in. Almost every American reporter is now being kicked out of China. We've no idea what's going on with Chinese companies. Yet, these index providers keep putting more prominent weighting on Chinese companies so that more and more passive investment, ultimately hundreds of billions of dollars, is going into Chinese stocks and bonds. That's a big problem. So, I think if we were to have sort of an outbound CFIUS mechanism, that's definitely worth exploring. The others look at Hong Kong as well. Hong Kong has now, unfortunately, been turned into a typical Chinese city, and we should be treating them the way that we treat mainland China when it comes to inbound and outbound investment.

Senator CASEY. Thanks very much. Mr. Chairman, I'll submit a question for the record on intellectual property—but we'll do that for the record.

Chairman WARNER. I think you're pursuing an interesting line of questioning, and I think what Mr. Pottinger just said there, it wasn't just the folks who went directly into some of these companies who lost all this value but, oftentimes, the passive investors. And the thing is these companies are not going to disappear. They may simply be replaced with more Chinese investors and a more compliant leadership in those firms.

Senator Gillibrand.

Senator GILLIBRAND. Thank you, Mr. Chairman.

Mr. Evanina, you were the head of the National Counterintelligence and Security Center. In 2018, DOJ required state-sponsored media outlets like Xinhua News and China Global Television Network to register as foreign agents. Yet, when Americans visit those websites, when Americans read or listen to watch those stories, there isn't even the most basic labeling information for the consumer that they're visiting a foreign agent registered news site.

This is true for Russia, too. Russian media outlets like Sputnik that run influence operations through radio shows in the U.S. are forced to register as foreign agents by DOJ, but no one notifies the Americans who are listening to the shows or who are reading their stories. And I think that's really irresponsible.

Why is the burden on the U.S. consumer to go to the DOJ website to hunt down FARA filing forms to know where they're getting their information?

Mr. EVANINA. Senator, thanks for the question. And I think you were getting at the heart of what I believe to be the new frontier, which is malign foreign influence. And I think we look at how countries like China and Russia facilitate their influence here. It starts with media, and it plagues social media, TV stations, newspaper print, and we are unable to see it. And I will proffer that the U.S. government's inability to look at media due to constitutional issues provides a vast, gaping hole for who should do that, right?

I think it's unfair, as you said, for constituents to understand—and they're not going to go to the DOJ website—but we don't have a reference. State Department has a Global Engagement Center. We don't have a domestic engagement center to help, advise, and inform Americans as to how to identify where that influence is and what might be true or what might not be true from that website. So, I do think we have a hole to fill with respect to understanding

malign foreign influence and to help Americans everyday living technology but also with elections in the future.

Senator GILLIBRAND. Where would you place that domestic engagement center, under what agency?

Mr. EVANINA. Well, I would have to think more on that, Senator, but off the top of my head, I would say it would have to be partly in the Intelligence Community where can garner the most real-time actionable intelligence from our collection. At the same time, it has to have a vehicle that could produce that intelligence unclassified to the consumers around America.

Senator GILLIBRAND. Right. Because shouldn't this basic foreign agent information be affirmatively provided to American consumers, so they can make informed decisions about where the foreign state-sponsored news is actually coming from?

Mr. EVANINA. Yes, and to that point, I think if you look at things from an agency perspective of the goals, responsibilities, and the agency's names, I would say Department of Homeland Security would be the right nomenclature for that kind of role.

Senator GILLIBRAND. So do you think that FARA needs to be strengthened or clarified in some of those loopholes that allow China and others to push their misinformation without any consumer protection notice?

Mr. EVANINA. Yes. I do think that any of these issues, whether it be FARA or FIRRMA or CFIUS, should be relooked at every year, because the technology moves and how we see it, our adversaries change their tactics based upon legislation we employ and our policies. We have to update year-by-year basis to understand how China or Russia or Iran has revectored their influence so we can act accordingly.

Senator GILLIBRAND. I think that also should apply in some respects to our platforms, our social media platforms, because especially in a current example like the debate about vaccinations, a lot of Chinese and Russians are actively trying to mislead Americans. And I think there has to be some responsibility to the purveyors of this information to have a way to know if they are foreign agents. Do you agree?

Mr. EVANINA. I completely agree. And I look back the last year or so, as Mr. Pottinger had referenced and as I went through the election, the ability to siphon through maligned foreign influence and messages that are factually not correct, is a very difficult venue. And we look at the abilities of our adversaries, Russia and China, to no longer cede information here, but to use our own information to amplify for other Americans takes on its own new weight of a really difficult obstacle to be able to do that.

Senator GILLIBRAND. Ms. Puglisi, obviously, foreign adversaries have tried to influence our country for a very long time. This is nothing new. Russia has attempted to steal our technology through investments, through exchange students, through cyber operations, attempted to recruit, tried to intimidate, stifle dissent, unflattering narratives, as does China. So, obviously, this is problematic and serious, but the question is what aspects of this threat are new, and is it simply a question of the scale and breadth of China's operations and theft of trade secrets that differentiate it? And how

should these distinctions shape our strategy and counter their efforts?

Ms. PUGLISI. Thank you, Senator, for that question. I would say the aspects that are new is that it's more and more in the civilian space. And I think if you raise the issue of the Soviet Union, we look back and that was very heavily military-focused. And some of my earlier comments about how our traditional structure of CI is focused on intelligence officers, on things that were completely illegal, things that have a direct military application. And the way China targets our technologies and the way it leverages its own diaspora, I think, is something that's very new. It's also the scale and scope, and the fact that these are central government programs that have been in place for decades, that focus on the influence piece, the civil technology piece, and really target the gray areas of our civil society. And you pair that with the largest crackdown on civil society that we're seeing in China under Xi, and it's a really toxic mix.

Senator GILLIBRAND. Thank you. Thank you, Mr. Chairman.

Chairman WARNER. Thank you, Senator Gillibrand.

I just have one more question, and I know we have a series of six votes started, and that's why some of my colleagues have, I think, gone back to the floor. One, I want to thank all three of you. I liked one of Matt's ideas a lot—about all these 360,000 down to 320,000 Chinese students—give every one of those students an American phone when they got here, so they are not surveilled constantly. But my sense of the Chinese economy, one of the challenges we have, frankly, for any American or for that matter, Western-based company—and I would point out that while this Committee, I think, got ahead of the game a little bit on spotting 5G, the first signs of warning about Huawei didn't actually come as much from the Intelligence Community. It came from places like Japan and South Korea and elsewhere. But it seems to me that the Chinese economy has allowed—I don't know if that's changing dramatically now as we see the leadership and some of the value taken out of some of the most successful tech companies in these last few months. But for the last five to ten years, China would allow a ferocious level of competition at least within the tax base. But that competition would be allowed until a national champion emerges, a la Huawei or ZTE. And in that space, no Western, no American, for that matter, any Western company could actually be on the competitive edge; they would never be allowed a Western American company to kind of win in one of these new technology areas. Matter of fact, as we know, with Facebook being excluded or Google trying for a while and then leaving on their own accord, and others. And the idea that that Chinese technology winner then suddenly, even if they're independent gets the full backing of the state—Huawei, we talked about a hundred billion dollars plus—is really an economic model, kind of an authoritarian capitalism model that I don't like, but it's had a pretty successful record recently. Because if you then combine that not only with the financial support but also with the Belt and Road Initiative, the Digital Silk Road, China's increasing power around the world, you suddenly had a series of maybe not satellite countries in the traditional mindset, at least countries that were dependent on China's forbear-

ance, because China happened to be also building a bridge or building a road in many of those countries. You know, I think that model is hard to compete against.

I think we've seen it as well, and I think this Committee spent a lot of time looking around this issue which I raised in my opening comments, around standards and rules of the game. Again, within technology, because I would argue that—I'll use the Sputnik as an example—but post-Sputnik, virtually every major technology innovation over the last 60 years, if it wasn't invented in America, we still got to set the rules and the standards and the protocols. And those rules, whether it was about transparency and respect for human rights, even in technology standards, you can embed some of your standards. It kind of crept up on us in 5G, and I say this is an old telecom guy, where suddenly China was flooding the zone on these international standards-setting bodies with engineers with power.

And they are I would argue in many ways on the 5G issue, they won the standard-setting component. And, unfortunately, we're seeing whether it's in AI or facial recognition or a host of areas where they have now had the audacity to lay out with a great deal of specificity where they hope to dominate, they are being fairly successful.

So, the question I have for all three of you, my last question is, I don't believe we can do this alone. I think some of our greatest strength has been our alliances—that there is a moment in time where not just Five Eyes or not just NATO, but democracies around the world. I would even argue that we may be entering in an era of post-World War II, that was an era of military alliances, NATO, SEATO, a series of other—. The 1960s and 1970s or last century sort of European Union being a classic example of economic alliances.

I think in 2021 and going forward we need to think about technology-based alliances, and those alliances ought to be based upon democracies who share those same sets of values and goals of democracy. And that needs to start in areas like standard setting. It is as where we have actually finally put our money where our mouth is in terms of recent legislation that virtually everybody on this Committee supported around support for semiconductors. And we did get a smaller slug in for 5G and O-RAN.

But I'd ask all three of you, and I'll start, Anna, with you, then go to Bill, and then let Matt close out. How should we think about this effort to get our allies better engaged with us as partners, not into this bifurcation choice, either going to be on our side or China's side, but do this in some level of collaboration around technology development, around standard-setting, around, again, promoting a very alternative model to the authoritarian communism model or authoritarian capitalism model that China has, frankly, practiced fairly well?

Ms. PUGLISI. Thank you, Senator.

You raised some really important points. I want to highlight the model that you described as one that China has laid out for its strategic emerging industries. It's winning the China market first, creating that national champion, and then having that go out and compete on the world stage. And talking about Huawei, I think, is

a great example of that. What it highlights are those areas and what are those characteristics of these different industries where profit margins, national security, in some ways, go in opposite directions, and how do we actually compete with that. Because those industrial policies of our like-minded are very, very different in scale, scope, and flavor than what we're seeing with China. Forming those tech alliances will be, in my opinion, very, very important.

We can't out-China China, let's face it. But we don't want to. We want to double down on the advantages of our own system. And that is working with our partners and allies in building those innovation hubs, finding those niche areas. Some countries will be set for tech alliances in certain areas, some in different technologies. But it's also, I think, it's part of that information sharing and risk calculation sharing that we should have those dialogs about what's at stake, and how we can use technology that are in line with our values and the values of our allies and partners.

Chairman WARNER. Thank you. Bill?

Mr. EVANINA. Senator, first, thanks for having this hearing. I think it's really important for the American public to understand the issues that you and the vice chair brought to the openness since we hadn't had any closed hearings for a few years. I think your premise is right on our need to cooperate and collaborate with our allies. However, I will proffer that we need to lead in that collaboration. I think, with respect to my colleague Anna's point, China is not going to change. And I think it was one thing in D.C. that we have bipartisan support on, is that China is going to be China and they're going to double down.

We have to make a decision in America. Do we want to change the way we operate? We're clearly bifurcated for the right reasons between the government and the private sector. I will proffer that it's time to change the way we look at that and really look at how we are willing to change the construct for partnering with private sector industry and technology to be able to build coalitions between our government first in the industry and then show that leadership to our allies in Europe and other places, so they can use that as a framework.

We won that argument with Huawei for the same reason. I think the next step with technology is to do the same methodology: find champions in the U.S. and have the government partner with so that we look at China as a competitor, not just as an enemy, and we can compete, because we can compete because we're America. And we will win if we may put our mind to it. Secondarily, as we deal with Huawei, other countries and allies will watch and learn and do the same methodology in their own country to do the same diplomatic and technological solutions. So, I do think we have an opportunity here with allies if we change the way we do business here in the U.S.

Chairman WARNER. Very good. Matt? And I recognize I've got to go run vote in a moment.

Mr. POTTINGER. You bet. Thanks, Senator. Very quickly, you know, I agree with you. I think your vision for these sorts of coalitions are around certain technologies—coalitions of the willing, if you like—is the way that we need to go, and there's precedent for

that. During the Cold War, we had what was called the coordinating committee where industry in Japan and the United States and other allied countries made sure that the Soviet Union didn't gain access to our most cutting-edge semiconductor technology.

Here we are again. It's the same technology: semiconductors. We've got to win that race. Commerce needs to be brought firmly into the fold. The Bureau of Industry and Security has to be really treated and think like a national security arm of the U.S. Government, not a trade promotion arm. If we're going to win on semiconductors, we've got to make peace with the Europeans on these privacy issues and these things that we're tied up with. Right now, the Europeans are very inconsistent in how they're viewing privacy. They're targeting American technology giants but they're not applying the same standards to Chinese companies, which are going to be truly harmful to the interests of Europeans and disrespectful of people's privacy, of their data, and so forth.

So that's an area where we need to break through. But, I think, I agree with you. With those kinds of coalitions, even if it's not one neat global approach, but one of different coalitions, I think we're unbeatable.

Chairman WARNER. Well, thank you all. Just two quick last comments.

One, to not just American industry, but all of the Western industry that is invested in China, I don't know if we can have—no problem with that as long as it's not at the price of your values. As long as you do not surrender to, as Senator Rubio pointed out, that you turn a blind eye to human rights abuses or you are willing to be co-opted into taking policies that you would not take, not only in the United States but, for that matter, any other country in the world. That we have to be constantly consistent on. And I think the business community needs to continue to hear these messages in these open settings and as appropriate in close settings as well so even further information can be shared.

And then last point, and again, very much appreciate all three of the witnesses that in your opening statements, you all hit on this point. And that is that this beef, our concern, our challenge, is with the Communist Party of China and its leadership. And any forces in this country that instead play into broad-based racist or xenophobic statements about the Chinese people, the Chinese diaspora, Chinese-Americans, Asian-Americans, frankly, do a disservice to our country and our values, but also play right into the CCP's agenda that the only place you will ever have a firm and permanent home is back in China. And I think we, and I say this here for speaking on behalf of all the Senators on this dais who are here today, need to redouble our efforts to make that distinction and to make sure that, particularly law enforcement—and I've spent a lot of time with Director Wray on this issue, with the FBI and others—reaching out on a very regular basis to the Chinese-American diaspora in this country. They are under, Bill, as you've made comments, under a level of pressure sometimes. That is extraordinary and they are great Americans that they've contributed enormously to our country, but we need them in this challenge against the Communist Party's ideology. And any observant person doesn't need, I think, further proof because you see the very nature of the

treatment of the Uyghurs or the treatment of the people of Hong Kong. And we need to keep that lesson and continue to make that point. I thank all of you for your contribution. There is much, much more to be discussed. We could have had a whole separate hearing just looking at the individual technologies that China is investing in and trying to outcompete us. We will have that opportunity.

But with that, the hearing is adjourned.

Thank you all.

[Whereupon at 4:36 p.m., the hearing was adjourned.]

○