

S. HRG. 119–33

**THE MALIGN INFLUENCE OF THE PEOPLE'S
REPUBLIC OF CHINA AT HOME AND ABROAD:
RECOMMENDATIONS FOR POLICY MAKERS**

HEARING

BEFORE THE

COMMITTEE ON FOREIGN RELATIONS

UNITED STATES SENATE

ONE HUNDRED NINETEENTH CONGRESS

FIRST SESSION

JANUARY 30, 2025

Printed for the use of the Committee on Foreign Relations



Available via <http://www.govinfo.gov>

U.S. GOVERNMENT PUBLISHING OFFICE

WASHINGTON : 2025

59–774 PDF

COMMITTEE ON FOREIGN RELATIONS

JAMES E. RISCH, Idaho, *Chairman*

PETE RICKETTS, Nebraska	JEANNE SHAHEEN, New Hampshire
DAVID MCCORMICK, Pennsylvania	CHRISTOPHER A. COONS, Delaware
STEVE DAINES, Montana	CHRISTOPHER MURPHY, Connecticut
BILL HAGERTY, Tennessee	TIM Kaine, Virginia
JOHN BARRASSO, Wyoming	JEFF MERKLEY, Oregon
RAND PAUL, Kentucky	CORY A. BOOKER, New Jersey
TED CRUZ, Texas	BRIAN SCHATZ, Hawaii
MIKE LEE, Utah	CHRIS VAN HOLLEN, Maryland
RICK SCOTT, Florida	TAMMY DUCKWORTH, Illinois
JOHN R. CURTIS, Utah	JACKY ROSEN, Nevada
JOHN CORNYN, Texas	

CHRISTOPHER M. SOCHA, *Staff Director*
NAZ DURAKOĞLU, *Democratic Staff Director*
JOHN DUTTON, *Chief Clerk*

C O N T E N T S

	Page
STATEMENTS	
Risch, Hon. James E., Chairman, U.S. Senator From Idaho	1
Shaheen, Hon. Jeanne, Ranking Member, U.S. Senator From New Hampshire	2
WITNESSES	
Mattis, Peter, President, the Jamestown Foundation, Washington, DC	4
Prepared statement	6
Stoff, Jeffrey, Founder, Center for Research Security and Integrity, Herndon, Virginia	20
Prepared statement	22
Hart, Dr. Melanie, Senior Director, Global China Hub, Atlantic Council, Washington, DC	70
Prepared statement	71
Lind, Dr. Jennifer, Associate Professor of Government, Dartmouth College, Hanover, New Hampshire	77
Prepared statement	79

THE MALIGN INFLUENCE OF THE PEOPLE'S REPUBLIC OF CHINA AT HOME AND ABROAD: RECOMMENDATIONS FOR POLICY MAKERS

THURSDAY, JANUARY 30, 2025

U.S. SENATE,
COMMITTEE ON FOREIGN RELATIONS,
Washington, DC.

The committee met, pursuant to notice, at 10:42 a.m., in room SD-419, Dirksen Senate Office Building, Hon. James E. Risch presiding.

Present: Senators Risch [presiding], Ricketts, McCormick, Barrasso, Scott, Curtis, Shaheen, Coons, Kaine, Schatz, Van Hollen, and Rosen.

OPENING STATEMENT OF HON. JAMES E. RISCH, CHAIRMAN, U.S. SENATOR FROM IDAHO

Senator RISCH. I want to welcome our witnesses here today, and I want to thank you for being here today, for taking your time to help us explore this important topic.

This is the first policy hearing in this Congress. We felt it important to focus on the greatest long term threat to the United States, that being China.

As both a public official and a private citizen I have watched the Chinese government's malign influence grow. Their political games, economic schemes, and military aggression has only increased over the years.

The Chinese Communist Party has worked diligently to bring China to what it is today and it did it the old fashioned way.

Chinese officials bribed, stole, and cheated at every opportunity to ensure that China comes out on top, and we let them do it virtually uninhibited.

This has to stop. I think all of us agree the threat of Chinese influence on Western society is very real and needs to be addressed.

The same Chinese government that commits genocide against its ethnic minorities and dramatically oppresses the God given freedoms of its people also attempts to influence America.

As we speak, they are working to undermine our national security, our economy, and our values, and it is doing the same to our allies. This is not just wrong, but most of all it is dangerous.

Chinese influence spans industries from government to academia, from research laboratories to farms and factory floors.

No matter where, the Chinese government is determined to use both our people and our institutions to achieve China's political, economic, and military objectives.

China interferes in elections around the world including in the United States. It skirts foreign lobbying laws to influence democratic governments, and it woos State and city officials with elegant trips to adopt pro-China policies in an effort to pressure Federal Government.

It is no secret that the Chinese government conducts espionage on American soil, but China goes far beyond this. China siphons American technology and intellectual property from companies it partners with, repurposing it for their own economic benefit, and riding on the back of American ingenuity.

China pumps money into American universities and think tanks, attempting to secure access to sensitive military technology. Despite these threats, the previous Administration just renewed a science and technology agreement that actually encourages the very collaboration that could provide China with more access.

Abroad, our allies face similar problems, often on a larger scale. China co-opts international organizations like the U.N. and ensures they never get a chance to address the many human rights atrocities and military incursions China commits.

Sadly, while the Chinese government has improved and redefined its tactics over the year, U.S. diplomatic tools and laws have not kept pace to help manage these problems.

My goal today is to begin outlining what this committee can do to push back on China's political, economic, and military influence in our country and abroad.

To start, I hope that we can close the loopholes that allow for foreign agents to lobby government officials, reform our visa process to screen those who pose an intelligence risk, and encourage our national security community to play a larger role to counter the Chinese influence in American universities.

This work will take a whole of government approach but in large part will be spearheaded by Secretary Rubio. I know Secretary Rubio will use State as more than just a diplomatic mouthpiece as has been the case.

I know he will operate the State Department as the United States Government's expert agency on fighting foreign influence and incorporate countering Chinese influence into every aspect of its mission.

The Chinese will use every trick they can come up with to undermine America and other freedom loving nations. But working together across the aisle, across branches of government, and with our allies across oceans, America has and always will beat our authoritarian aggressors, and I have no doubt that we will continue to do so.

With that, I will yield to Senator Shaheen.

**STATEMENT OF HON. JEANNE SHAHEEN,
RANKING MEMBER, U.S. SENATOR FROM NEW HAMPSHIRE**

Senator SHAHEEN. Thank you, Mr. Chairman, and welcome to each of our witnesses.

Thank you all for being here today.

I certainly think Chairman Risch has made some important points that I agree with. We have worked closely together on the Chinese Communist Party's—the CCP's—malign activities in the past, activities like supporting Taiwan and Lithuania that we have worked together on in the face of Beijing's economic coercion, voting to protect America's user data from being captured by the CCP on TikTok.

I think these concerns are, as so many of the concerns about China, very bipartisan. Just last week at our hearing, Senators from both sides of the aisle highlighted the danger posed by China's efforts at the United Nations.

Today, China is targeting and exploiting open societies with every tool that they have. They leverage corrupt investments over decisionmakers in Africa and Latin America.

They have tried to buy off politicians in Australia and New Zealand to undermine democratic elections. They control strategic ports in places like Sri Lanka and Piraeus in Greece, and they conduct covert espionage against American industries from advanced science to aerospace to AI. Given the stakes, I hope each of you today will share recommendations that we can take as policymakers.

Something that I really want to zero in on is the growing cooperation between Beijing and Moscow. At the summit here in Washington last year, NATO labeled China a decisive enabler of Russia's war in Ukraine. But as we have seen this partnership goes both ways.

Russia has a lot to teach China when it comes to disinformation campaigns. Even before the invasion of Ukraine, Russia's Ministry of Digital Development, Communication, and Mass Media was partnering with China's National Radio and Television Administration.

So when Russia published lies about biolabs in Ukraine in the *Global Times*, a Chinese Communist Party outlet, picked up the story, and last year we saw Russia and China working together to spread disinformation and to destabilize the Solomon Islands.

The *Global Times* amplified stories from the Russian state controlled media agency Sputnik, saying the U.S. was seeking a—I am quoting here—"a democratic transition by violent means in the Solomon Islands."

Before our diplomats could refute these allegations the waters had already been muddled to Beijing and Moscow's benefit.

China's leaders have made shaping global and local public opinion a priority. They have bought up entire foreign media companies located outside China to promote pro-Beijing propaganda around the world.

They have also targeted fact based journalists with the *New Yorker*, the *Economist*, the *New York Times*, the *Guardian*, and others, and in many of the worst instances they have gone after female journalists of Asian descent with harassment, trolling, and threats.

Chinese diaspora and human rights groups are also targets. According to the *New York Times*, they not only attacked a writer living outside Philadelphia who criticized Xi Jinping, they also posted

sexually explicit and threatening comments against his teenage daughter.

Beijing has used these tactics on its own population at home, and it has refined them for export abroad. Taken together, these malign actions are a threat to the United States, and our efforts, sadly, in the information space have not been very effective.

The Foreign Malign Influence Center made strides against China and Russia in their attempts to undermine U.S. presidential elections, but Congress' failure to extend the Global Engagement Center last year I believe was a serious setback for the State Department's ability to counter disinformation and propaganda.

China is spending billions of dollars to amplify Russian propaganda, and we need more tools like the Global Engagement Center, not fewer.

Of course, as former Ambassador to China Nick Burns said when I met with him recently on his way home from his ambassadorship, when it comes to how the U.S. responds to China, the devil is in the details.

I am deeply concerned by the Administration's stop work order and foreign aid freeze, actions that can only lead to human suffering and endanger our national security. They undermine America's credibility, and they give an opening to countries like China and Russia, who are very happy to fill the void that we leave.

So I look forward to hearing from each of you today on how we should think about tackling this complex problem.

How can we best defend our transparent, democratic nation from China's malign influence? How do we position the United States for a future that benefits all Americans?

Thank you, Mr. Chairman.

Senator Risch. Thank you, Senator Shaheen.

We will now proceed to our witnesses we are going to hear from today, and let me say, first of all, that the issue as we just heard is not a partisan issue but one that, as far as the problem is concerned, we are very much in agreement on.

We have a really distinguished panel here today. We worked together on a bipartisan basis to put this panel together. We are going to hear from some people who are very schooled in this issue, and it will be helpful to us and to the American people.

So we will take them one at a time, and I will start with Mr. Peter Mattis. He is president of the Jamestown Foundation.

He is a leading expert on the Chinese Communist Party and its united front system, and has previously worked on these issues in the Senate, the House of Representatives, and the intelligence community and elsewhere.

Mr. Mattis, the floor is yours.

**STATEMENT OF PETER MATTIS, PRESIDENT,
THE JAMESTOWN FOUNDATION, WASHINGTON, DC**

Mr. MATTIS. Thank you, Chairman Risch, thank you, Senator Shaheen, and all the other distinguished senators that are here for drawing attention to this important issue because awareness and expertise are two of the key factors in being able to respond and to protect this country and also protect other democracies and

other countries that are standing up to protect their sovereignty and standing.

The Chinese Communist Party's influence activities can loosely be formed under the umbrella of united front work. These can be described best as efforts to monitor, control, and mobilize individuals, institutions, platforms, and other civil society organizations outside the CCP to work on the party's behalf.

So I think, to put this into kind of a context for you, it would be that if you guys maintained your campaign infrastructure in your State and then kept putting a committee into every company, into every Elks Club, Kiwanis, every school, every university, every research institute, national lab if it is there, that would be kind of like what united front work is.

It keeps moving out to make those institutions serve the party's political purpose, and describing it in that context, I think, should make it clear why this is not something where we should describe interference or influence, but this is actually a tool that is pernicious in undermining the very functioning of institutions.

United front is also a way of looking at politics. It is a very clear calculation by the party of who are our enemies, who are our friends, and how do we mobilize those friends, how do we recruit neutrals to isolate our enemies, to strike them, and to make them ineffective.

It is also a huge policy bureaucracy. Now, sometimes people say there is the united front work department, but which one? The central one? The 31 provincial ones? The 300 municipal ones?

The thousands of county level ones, or the ones in companies, the ones in the China Academy of Sciences and China Academy of Social Sciences? Which ones are we referring to?

This is a system that engages hundreds of thousands of people very directly inside the party, on the fringes of the party, and it keeps extending outward.

The CCP's united front—Xi's united front—has a tool to achieve its objectives of national rejuvenation, and that national rejuvenation can broadly be defined as, one, comprehensive modernization, the second, unification.

Now, we think of this in Taiwan, in Hong Kong, but it is really a political, economic, social, and cultural unification. It is not just having control, and it is putting everything together.

The primary targets of united front work are those individuals and institutions and platforms that really make democracy work—their social groups, their media, their universities, their local and national political leaders, their companies. Anything that can be leveraged by the party will be leveraged.

What is the harm, if you will? The first is that in some cases when an organization is taken over by the party, our own citizens lose their voice to speaking to their own elected representatives and their own government because you cannot possibly meet every one of your constituents.

You rely on these groups to tell you what is going on in your State, in districts when you were—if you were in the House.

But if that community organization leader is someone who is speaking for the party, you might think that you are hearing from someone who is representing 500 people or a thousand people, but

really it is somebody who is representing the CCP rather than their fellow Americans.

You can go down a list of things—the distortion of the marketplace of ideas, the loss of technology, as Mr. Stoff will cover, the facilitation of intelligence operations.

Pushing back necessarily requires sort of insider information of institutions and organizations that are being affected, and that person needs awareness.

They need something like a hearing today or other types of information, whether it is RFA reporting abroad or any other form of, say, a report from safeguard defenders or other civil society organizations to say, wait a minute, there is a problem here, and I can go out and find external expertise, which is the next piece.

You need external expertise, and one of the ways in which the United States is very different than the CCP is that we support people who are trying to stand up for their own rights, for their own countries, for their own sovereignty, and the party is paying people to do their own bidding, that of the CCP and not for the benefit of their citizens and fellows.

And last, you need political power, as when I worked with Senator Cruz's staff in 2018 to keep the CCP out of the University of Texas Austin. It took someone who is on the inside, it took the outside expertise, and then it took someone who was willing to draw attention to it and say there are political consequences for this.

So to get through this in terms of recommendations, anything that improves transparency such as FARA reform to make things more accessible, to make sure that it is not a quarterly update that is searchable, would be beneficial.

There is focus on the Chinese malign influence fund, keeping it strategic rather than just repurposing funds for existing programs, and I think it is worth thinking about what are the ways to incentivize action within executive departments such as the Department of State.

So that we are asking Congress or asking the State Department to report when authorities are not used, rather than sort of trying to avoid the congressional reporting requirement of many things that are put forward.

Thank you very much.

[The prepared statement of Mr. Mattis follows:]

Prepared Statement of Mr. Peter Mattis

I. OVERVIEW

Chairman Risch, Ranking Member Shaheen, distinguished members of the Committee, thank you for inviting me to appear before you.

Countering the Chinese Communist Party's efforts to build political influence, recruit and mobilize civil society outside the borders of the People's Republic of China (PRC), and shape the world in coercive, corrupting, and covert ways is fundamental to U.S. success in this rivalry. Any sustainable, long-term strategy for addressing China's challenge requires the integrity of U.S. political and policymaking processes—and those of our allies and partners. This requires grappling with the challenges posed by the party's efforts to shape the United States and others by interfering in our politics and domestic affairs.

The United States, its political and business elite, its thinkers, and its Chinese communities have long been targets for the Chinese Communist Party. The party employs tools that go well beyond traditional public diplomacy efforts. Often these tools lead to activities that are, in the words of former Australian prime minister Malcolm Turnbull, corrupt, covert, and/or coercive. Nevertheless, many activities are

not covered by Turnbull's three "Cs" but are still concerning and undermine the ability of the United States, its allies, and its partners to comprehend and address Beijing's challenge.

Most of my statement will focus on the policies and actions of the Chinese Communist Party. Many Americans are still not prepared to accept the Party has sought to shape and influence U.S. political and business elite for decades. We are still in a process of building awareness and consensus about the nature of the problem. We can know the objectives of the Chinese Communist Party. We can understand its organizations and its policies. And we can observe the Party's actions. It is far harder to determine the motivations of our fellow citizens and those in allied and partner countries, because they may have sincere intentions coupled with naivete or they have only their private benefit at heart. Although much more information is now available about the Party's ambitions and activities, many still are not sufficiently aware or do not know how to operationalize their knowledge. Hearings like this one are a good step for raising awareness. Finally, The Jamestown Foundation is dedicated to helping Americans (and our allies) understand U.S. rivals in their own words and in their own terms. Although I have personal policy views, the institution I lead focuses on providing information, analysis, and context primarily about U.S. rivals.

The central element to understanding on why and what the Chinese Communist Party is doing to shape the world outside the party is united front work. Mao Zedong described the purpose of this work as mobilizing the party's friends to strike at the party's enemies. In a more specific definition from a paper in the 1950's, the Central Intelligence Agency defined united front work as "a technique for controlling, mobilizing, and utilizing non-communist masses." Put another way, united front policy addresses the party's relationship with and guidance of any social group outside the party. The most important point here is that what needs to be shaped is not just the Chinese people or world outside the People's Republic of China, but rather those outside the party.

United front work also is a tool of political struggle. It is not just a question of activities that we would call propaganda or public diplomacy. Nor is it limited to what we would call covert action. As Mao wrote in 1939: "Our 18 years of experience show that the united front and armed struggle are the two basic weapons for defeating the enemy. The united front is a united front for carrying on armed struggle. And the Party is the heroic warrior wielding the two weapons, the united front and the armed struggle, to storm and shatter the enemy's positions. That is how the three are related to each other." Mao's basic framing of united front work within the party's toolbox remains the core understanding within the party today. Jiang Zemin, Hu Jintao, and Xi Jinping all have characterized united front work as a "magic weapon" to facilitate China's rise in the midst of an international ideological battleground.

CCP General Secretary Xi Jinping has put particular emphasis on this element of statecraft and party activity. During his first 3 years in office (2012–2015), Xi launched three major initiatives that correspond to Mao's three tools. The anti-corruption campaign was intended to strengthen the party—a point that was made clear for those in doubt in Xi's address to the 20th Party Congress in 2022. The PLA began a major reform in late 2015 to bring the way the PLA intended to fight into sync with its organizational structure. And finally, Xi launched reforms of the united front policy system. In his speech for the Party's centenary, Xi focused his remarks on these three areas: party-building, the PLA, and united front. Although it is comforting to think that Mao's words "to storm and shatter the enemy's position" belong to a bygone era, Xi has proved otherwise. He was explicit in a speech to the Party faithful early in his tenure about the importance of seeing the basic continuity across Mao's rule and the Reform Era.

United front activities help the party resolve several dilemmas of the post-Mao era and that became ever more apparent after the Tiananmen Massacre and the passing of Deng Xiaoping. These are fundamental questions for the Chinese Communist Party, and they speak to why the party must spend so much effort trying to shape the world beyond the membership of the party.

1. How to motivate and mobilize the Chinese population without the ideological fervor of the Mao Zedong era?
2. How to benefit from the outside world while screening out influences and ideas that might damage the party's positions?
3. How to enlist the outside world in supporting China's rise and keeping those doors open even as the party continues to be repressive and becomes more aggressive internationally?
4. How to shape the world, its institutions and its leaders, so that the CCP can achieve its objectives and they respect Beijing's system of governance?

The Chinese Communist Party has put particular focus on targeting people and institutions with united front work, because these are the fundamental units of society. Controlling the platforms and social groups where people congregate is how a totalitarian regime maintains control even when there might be immense dissatisfaction. The Party's methods at home and abroad have significant parallels. The Party's targets also are the key to pushing back. Civil society organizations and individuals—in some cases supported by the United States through Department of State programs—have helped fight back. In some cases, this means raising awareness and supporting journalistic investigations.

In other cases, civil society organizations provide the first warning of significant developments. For example, the human rights non-governmental organization Safeguard Defenders exposed the existence of “Chinese overseas police service centers” set up by subnational public security bureaus in blatant violation of the territorial sovereignty and national security of other nations, including the United States and many of its allies. These “police stations” were set up in direct cooperation with united front-affiliates in target countries. As a consequence of the exposé, not only has a successful prosecution taken place in New York and investigations remain ongoing around the world. It has also spurred a previously non-existent debate on the nature and activities of the united front in countries around the world. An organization like Safeguard Defenders was only able to do this because they engage in daily grassroots activities with members of the targeted communities that allow them to pick up on developments early on and develop them for further research.

As a general rule, successful pushback against specific instances of CCP malign influence requires a combination of insider concern, expertise, and political power. Someone inside an organization—whether a civil society organization, a government body, a company, a university, or any other institution—will be the first to become aware of an emerging agreement with the CCP or one of its proxies. This person and their knowledge are required to trigger any internal process to bring in expertise, whether that expertise resides inside or outside the organization. Someone or some group with expertise helps to properly contextualize what is taking place and why the surface-level view of the partnership with the united front system (broadly defined) misses the real purpose and effects of that partnership or activity. Sometimes, political power is required to make the risk of proceeding untenable. That could be the threat of executive branch action or some sort of investigation. It also could take the form of congressional or media scrutiny. In the case of the University of Texas-Austin rejecting an agreement with the China-U.S. Exchange Foundation in 2018, the combination of congressional and media scrutiny provided the necessary pressure on university leadership to reject funding that came with conditions that many faculty realized were incompatible with the university's values and stated mission.

The infrastructure and organizations to maintain this expertise are, in a way, the industrial base of strategic rivalry. While we need the defense industrial base to deter and, if necessary, fight a war with the PRC, we also need the people necessary to maintain the strength and integrity of the United States, our allies, and our partners.

II. MAGIC WEAPON FOR NATIONAL REJUVENATION

Achieving the “Great Rejuvenation of the Chinese Nation” [Chinese characters were inserted here] has two significant components. The first is making China a great power with global reach. The second is doing so with the Chinese Communist Party at the helm.

The party defines the “Great Rejuvenation of the Chinese Nation” as having three components. The first is building “a great, modern socialist country that is prosperous, strong, democratic, culturally advanced, harmonious, and beautiful.” Although many of these words are self-explanatory, others like democratic, culturally advanced, and harmonious mean something very different in the party's context than in the American context. “Democratic” is consultative democracy in which the party leads, and other political inputs are provided through controlled mechanisms like the united front policy system. “Culturally advanced” and “harmonious” define the party's relationship with society and the ways in which Chinese people conduct themselves. The second is national reunification of all areas claimed by Beijing, regardless whether they were traditionally part of China. The third is China's emergence as a global leader in terms of comprehensive national power and international influence.

The following quote from Xi Jinping in 2016 explains what united front work is intended to accomplish in bringing together a unity of effort. When U.S. intelligence

officials describe Beijing as presenting a “whole-of-society” challenge, they are describing an important element of what the united front policy system is doing:

“Attaining the ‘Two Centenary Goals’ requires that our entire society works together in one heart and one mind. It requires that people of all ethnic groups focus their thoughts and their efforts toward the same goal. A society that lacks common ideals, goals, and values, and that finds itself in permanent disorder will never achieve anything. China has a population of more than 1.3 billion people, and neither the people nor the country would benefit if we ended up like that. To attain our goals . . . [we must rally] all Chinese people under the leadership of the Chinese Communist Party, and motivating all parties to engage in a concerted effort to bring about the rejuvenation of the Chinese nation.”

The United Front Work Department, the executive agency for conducting and coordinating these operations, provided a similar description of its purpose and activities:

“The history of China and foreign countries shows that whether a political power or a political party is good or not, its success or failure ultimately depends on the back of the people. Paying attention to the people’s sentiments, obeying the public’s will, striving for the people’s hearts, maintaining proper flesh-and-blood ties with the masses, and winning the sincere support of the masses is a solid foundation for our country’s long-term stability and a fundamental guarantee for the sure victory of our cause.”

The second important component of the “Great Rejuvenation of the Chinese Nation” is maintaining the leadership of the Chinese Communist Party. The most important threats to party that must be addressed are the diaspora communities and potentially threatening great powers. The former have the cultural knowledge to introduce subversive ideas that resonate. The latter have the material power to undermine or topple the party-state.

The desire to control the political landscape and protect the party’s position found clear definition in China’s National Security Law (2015). The law describes security in broad terms that go well beyond physical threats to the territory of the PRC. Security comes from the inside out. Articles Two and Three of the law state: “National security refers to the relative absence of international or domestic threats to the state’s power to govern, sovereignty, unity and territorial integrity, the welfare of the people, sustainable economic and social development, and other major national interests, and the ability to ensure a continued state of security. National security efforts shall adhere to a comprehensive understanding of national security, make the security of the People their goal, political security their basis and economic security their foundation; make military, cultural and social security their safeguard . . .”

This definition has two notable features. First, security is defined by the absence of threats, not by the ability to manage them. This unlimited view pushes the Chinese Communist Party toward preempting threats and preventing their emergence. Second, security issues extend to the domain of ideas—what people think is potentially dangerous. The combination of these themes—preemption in the world of ideas—creates an imperative for the party to alter the world in which it operates—to shape how China and its current party-state are understood in the minds of foreign elites.

One way of making this more concrete is to look at party documents about security threats. In April 2013, “Document No. 9”—“Communiqué on the Current State of the Ideological Sphere”—identified ideas that undermine the party-state’s security. Among them were the promotion of constitutional democracy, civil society, and Western concepts of journalism. In the circular’s final paragraph, it stated the party should “allow absolutely no opportunity or outlets for incorrect thinking or viewpoints to spread.” Although it would be easy to dismiss this document as a one-off or unenforced, in 2015 Beijing abducted and held five Hong Kong booksellers, including foreign passport holders, who sold books ostensibly banned in China. Moreover, Beijing issued new regulations on counter-espionage last December that clarified the Counter-espionage Law (2014) and defined activities threatening national security apart from espionage. Among these was “fabricating or distorting facts, publishing or disseminating words or information that endanger state security.” Influencing the outside world, therefore, is not just a historical activity of the party, but an ongoing requirement for national security as defined by the party-state. Over the last decade, the international element of Beijing’s repression has grown immensely, involving convictions on U.S. soil, reports of CCP-instigated violence, arrest warrants and bounties for Hong Kong exiles whose activities were entirely legal at the time of the action, and much more. During his confirmation hearing, Sec-

retary of State Marco Rubio also highlighted the plight of Uyghurs in Thailand who faced forced repatriation, but this is a phenomenon that has been well reported around the world.

III. INTRINSIC TO THE PARTY'S DAY-TO-DAY OPERATIONS¹

The Chinese Communist Party's management of political influence operations—evaluated on the basis of the united front policy system—runs to the very top of the party, involving senior leaders directly. The policy system extends through the party's hierarchy and spills over into the government ministries of the People's Republic of China as well as other state-owned and -administered organizations and enterprises. Put simply, united front work is conducted wherever the party is present. Moreover, united front work is not an “influence operation” or a campaign. It is the day-to-day work of the party. There are not special orders explaining what to do to achieve what objectives or the equivalents of a presidential finding.

At the leadership level, four elements point to the importance of united front work and shaping the world outside the Chinese Communist Party.

1. *A Politburo Standing Committee Member Oversees United Front Work:* The senior-most united front official is the Chinese People's Political Consultative Conference (CPPCC) chairman, who is the fourth-ranking PBSC member. A look at the leaders who have held the CPPCC chairmanship suggests that Western observers have been far too quick to condemn the CPPCC as a mostly useless advisory body. The list is a who's who of the party, including Mao Zedong, Zhou Enlai, Deng Xiaoping, and Li Xiannian. The current CPPCC chairman, Wang Huning, continues a tradition of competent leadership at the top of the united front system. He exemplifies the need of united front personnel to be highly disciplined party cadre, who are nonetheless capable of handling themselves among diverse people and feigning ideological flexibility.

2. *A State Council Vice Premier Has a United Front Portfolio:* The vice premier position serves as the bridge between the party center and the State Council ministries. The vice premier provides prestige to the united front system as well as a necessary position of authority to direct and coordinate the ministries' united front activities. The position often looks as though the portfolio covers education and culture, because of the overlap with united front work. At meetings of the united front policy system, this vice premier appears in protocol order between the CPPCC chairman and United Front Work Department director. Currently, the position is held by Ding Xuexiang.

3. *Two Members of the Central Secretariat Have United Front Policy Roles:* The directors of the party's United Front Work Department (UFWD) and Propaganda Department serve on both the Politburo and the Secretariat of the 20th Central Committee of the Communist Party of China. Because the Politburo does not meet regularly—its far-flung membership includes both central party bureaucrats and provincial party secretaries—the secretariat is empowered to make day-to-day decisions related to policy that has already been settled. This group is also responsible for moving paperwork among the central leaders and coordinating the party's actions. Secretariat membership is not related to relationships that the current UFWD and propaganda chiefs—respectively, Shi Taifeng and Li Shulei—have but rather reflects the structure of post-Deng Xiaoping politics. Their presence on the Secretariat is more institutional than political.

4. *In 2015, Xi Jinping Established a United Front Leading Small Group:* As part of the effort to revitalize and better coordinate united front activities under Xi Jinping, the party established a leading small group. It functions as a platform to coordinate and raise the status of united front work across the bureaucracy, bringing together senior officials from numerous state and party agencies for united front study tours across China. Interestingly, the last time the party created a united front leading small group—in 1986 under the leadership of Xi Jinping's father Xi Zhongxun—it coincided with a similar description of problems to be resolved: expanding scope and responsibilities coinciding with a lack of central direction.

The Chinese Communist Party bureaucracy at the central level has four key bodies for building and exercising political influence outside the party—and especially

¹Much of the following sections draws from my previous testimony to the House Permanent Select Committee on Intelligence, Alex Joske's report entitled “The Party Speaks for You: Foreign Interference and the Chinese Communist Party's United Front System” published by the Australian Strategic Policy Institute (June 2020), Matt Schrader's report entitled “Friends and Enemies: A Framework for Understanding Chinese Political Interference in Democratic Countries” published by the German Marshall Fund (April 2020), and a forthcoming report from The Jamestown Foundation on united front activities in democratic countries by Cheryl Yu.

outside China. The United Front Work and the Propaganda departments also have subordinate elements at the provincial and local levels.

1. *United Front Work Department*: The UFWD is the executive and coordinating agency for united front work. It has a variety of responsibilities at home and abroad, including in the following areas: Hong Kong, Macao, and Taiwan affairs; ethnic and religious affairs; domestic and external propaganda; entrepreneurs and non-party personages; intellectuals; and people-to-people exchanges. The department also takes the lead in establishing party committees in Chinese and now foreign businesses. The UFWD operates at all levels of the party system from the center to the grassroots, and the CCP has had a united front department dating to the 1930's.

2. *Chinese People's Political Consultative Conference (CPPCC)*: The CPPCC, according to the organization's website, is "an organization in the patriotic united front of the Chinese people, an important organ for multiparty cooperation and political consultation." The advisory body mediates between important social groups and the party apparatus. The CPPCC is the place where all the relevant united front actors inside and outside the party come together: party elders, intelligence officers, diplomats, propagandists, military officers and political commissars, united front workers, academics, and businesspeople. They are gathered to receive instruction in the proper propaganda lines and ways to characterize Beijing's policies to both domestic and foreign audiences. Many of these individuals, particularly if they hold government positions, are known for their people-handling skills and have reputations for being smooth operators. CPPCC membership offers access to political circles, political protection for business, and minor perquisites like expedited immigration. The CPPCC standing committee includes 20 or so vice chairpeople who have a protocol rank roughly equivalent to a provincial party secretary. At the central level, the CPPCC includes more than 2,160 members, but the provincial and local levels include another 680,000.

3. *International (Liaison) Department*: The International Department, founded in 1951, is the party's diplomatic arm, handling relationships with more than 600 political parties and organizations as well as individual, primarily political, elites. The department previously handled the CCP's relationships between fraternal Communist parties and cultivated splinter factions of Moscow-dominated Communist parties after the Sino-Soviet split. The activist bent of the International Department disappeared as the department began re-establishing itself in 1970-71 following the tumultuous early years of the Cultural Revolution. Interestingly, the department originated as a UFWD bureau before being carved out into an independent entity.

4. *Propaganda Department*: The Propaganda Department has been a core part of the CCP since 1924. The official description of its duties includes conducting the party's theoretical research; guiding public opinion; guiding and coordinating the work of the central news agencies, including Xinhua and the People's Daily; guiding the propaganda and cultural systems; and administering the Cyberspace Administration of China and the State Administration of Press, Publication, Radio, Film, and Television. The Propaganda Department cannot be regarded as an entirely internal organization that broadcasts outward to the extent that it is involved in influence-building abroad. For example, China Radio International developed in the 2000's a covert international network of radio stations to hide the CCP's direct role in broadcasting Chinese-language propaganda inside target countries. The Propaganda Department presumably also plays a role in the co-optation, intimidation, and purchase of Chinese-language print media outside China.

The State Council ministries and many other organizations with a party committee also conduct united front work. These organizations all offer unique platforms and capabilities that the united front policy system can draw upon for operational purposes. Below are a few of the examples of the organizations outside the party that perform united front work or have united front work departments attached to their party committee:

1. Ministry of State Security
2. Ministry of Foreign Affairs
3. Ministry of Civil Affairs
4. Ministry of Education
5. Ministry of Culture and Tourism
6. Chinese Academy of Sciences
7. China Baowu Steel Group
8. China National Overseas Oil Corporation (CNOOC)
9. State-owned Assets Supervision and Administration Commission (SASAC)

The People's Liberation Army (PLA) deserves special mention, because it operates both inside and in concert with these other influence-building actors as well as outside this system. During the Chinese Revolution, the PLA served almost as the party's expeditionary arm. It duplicated all of the party's functions within a military organization. The PLA was and remains the armed wing of the Chinese Communist Party and not China's national army. As the party's armed wing and as the ultimate guarantor of the party's power, the PLA still mirrors the party structure from leadership to leading agencies to tactical execution.

1. *Central Military Commission*: Headed by Xi Jinping, the Central Military Commission serves as the nexus between the party and military leadership. Historically, the two military vice chairmen included an officer who had risen through the PLA's political work system; however, since 2012, two experienced operations officers have held the vice chairmanships. The CMC also includes the minister of national defense and the director of the Political Work Department. The former, like the vice premier for united front work, serves as the link between the PLA and the State Council. The latter oversees the bureaucracy responsible for military propaganda and political influence operations. Currently, however, Dong Jun, who is the minister of national defense, is not listed as part of the CMC. Miao Hua, who was the director of the Political Work Department, was suspended and put under investigation in November 2024 for corruption. As of January 21, 2025, Miao is still listed as a member of the CMC.

2. *Political Work Department*: This department is the successor to the General Political Department, which was dissolved in the reorganization of the PLA launched in November 2015. The department's Liaison Bureau is the military agency that contributes most to the party's united front work. It operates much like an intelligence service with officers using official and non-official cover, but focused on strategic targets relevant to military operations. Two of the Liaison Bureau's most notable targets have been Taiwan and Okinawa.

3. *Information Support Force and Cyberspace Force*: The creation of the Strategic Support Force as part of the 2015 reforms integrated the PLA's signals and electronic intelligence capabilities with its tactical information warfare elements. In April 2024, the PLA eliminated the Strategic Support Force and created the Information Support Force, the Military Aerospace Force, and the Cyberspace Force. This restructuring reflects the PLA's continued emphasis on information warfare and battlespace information control in multi-domain integrated joint operations.

IV. VECTORS AND MECHANISMS

The Chinese Communist Party's political influence operations target: community organizations, wealthy proxies, universities, local governments, exchanges, and consulting agreements. Initially, these entities are themselves targets of cooptation and/or coercive efforts. Once properly developed, they become additional vectors in the Party's arsenal to further develop other relationships. The party openly exploits (and sometimes subverts) the constitutional freedoms offered by democracies like the United States: many of these avenues for influence are not illegal by themselves. Often only a few individuals camouflaged by the myriad China engagements are working directly on behalf of the united front system, but they might be difficult to point out without implicating individuals who are guilty, if anything, of nothing more than naivete or being the victim of the Party's coercion.

1. *Overseas Chinese Community and Other Civil Society Organizations*: The Chinese communities outside the PRC contain an alphabet soup of ethnic community organizations, including chambers of commerce, hometown associations, friendship societies, and cultural promotion centers. These organizations exist for all the same reasons that ethnic community organizations come together. They provide useful community resources and services, even as ones tainted by the united front system bring the party's influence along with them. In most of the problematic organizations, the majority of membership probably is unaware of the connections. The leadership sitting atop co-opted organizations become the community leaders through which politicians engage their local Chinese communities. They also can be quoted in media as being community leaders, even in cases where the organization exists in little more than name.

There are several indicators for whether a community organization—or rather its leadership or other important member—is working on the party's behalf. None of these indicators by themselves is sufficient, but, taken together, they are strongly suggestive. The first is whether the organization's officers participate in united front delegations and conferences back to the PRC. Sometimes these officers have special advisory roles with united front work units. The second is contact with the local PRC embassy or consulate, and whether these officials participate in the organiza-

tion's events. The third is the organizations' goal and leader remarks alignment with the Party's narratives. The fourth is the activities the organization hosts often have a tendency to amplify Party narratives. The fifth is that the organization becomes a key voice and proxy for the Party at times when the Party deems to be critical. The sixth is whether the organization hosts delegations of party and/or state officials, often at subnational levels of the party-state. Provincial and local level united front elements have become more and more active internationally, and greater attention should be paid to their activities. Changes, such as a shift from using traditional characters to simplified characters or visible changes to the amount of money used to put on events, is another indicator.

2. *Wealthy Proxies*: Wealthy businesspeople working on the party's behalf are one of the most important vectors for the party's influence abroad. Although many of these individuals are PRC citizens or emigres, some businesspeople from other states are influenced, coopted, or fully recruited to the party's cause. Their primary value is the ability to move money quickly outside of China and, in democratic societies, the ability to spend that money legitimately without generating the alarm that comes with more direct state activity. Where the united front system is active, two or more businesspeople will provide a significant chunk of the financial support for large united front-linked community organizations as well as other relevant political or social causes. For example, in Australia, Chau Chak Wing and Huang Xiangmo appear to have been the most active financial supporters of Beijing's efforts to interfere in Australian politics. Their money bought access to the major political parties, platforms for pro-China voices, and supported community groups like the Australian Council for the Promotion of Peaceful Reunification.

The easiest group of these proxies to identify come from Hong Kong. Their wealth has been built with the party's assistance. Although their families may have built successful businesses in one or two industries, a hallmark of these businesses is sprawled across numerous, unrelated industries. These businesspeople often can be identified because they are members of the Chinese People's Political Consultative Conference and the National People's Congress system. Their Hong Kong residency gives them legitimacy and credibility that their counterparts in China do not have. For example, former Hong Kong chief executive Tung Chee-hwa has been able to reinvent himself as a philanthropist to donate money to U.S. think tanks, academic programs, and sponsor trips for journalists, students, and politicians to China. Tung, however, became Beijing's man in Hong Kong after the party bailed his company out of bankruptcy in the mid 1980's, and he began representing the party's interests to the British. Tung now serves as a vice chairman of the CPPCC, which gives him standing within the party at roughly the level of a provincial party secretary.

The CCP also cultivates relationships with prominent Western business leaders through high-level meetings and economic incentives to advance its interests internationally. For example, in March 2024, Xi Jinping met with US representatives including those from the business community. He encouraged the companies to participate in Belt and Road cooperation, attend large-scale business events such as the China International Import Expo, and continue to invest in China. Attendees included people like the Chair of the Board of Directors of the National Committee on U.S.-China Relations Evan G. Greenberg and President of the U.S.-China Business Council Craig Allen.

3. *People-to-People Exchanges/Diplomacy*: The united front policy system sponsors and arranges hundreds of trips to China each year. These trips are used in a myriad different ways to earn good will and to influence analysts and politicians. They offer opportunities for the party to persuade them of China's rectitude or to refute critical arguments. Even if the latter does not persuade the critic, their fellow participants may be persuaded or inclined to see the critic as needlessly provocative. The trips also give party officials evaluate potential targets personally. Not only is there personal interaction, but there often is substantive discussion of ideas and policy positions.

4. *Consulting Agreements*: Hiring senior officials after they retire has become common practice. Beijing may have pioneered the process decades ago, pressing companies that wanted to do business in China to hire their favored former officials to close business agreements. Perhaps the most noteworthy recent example is former Australian trade minister Andrew Robb's \$880,000 (AUS) salary for minimal work on behalf of the Chinese firm Landbridge. Robb resigned from this position ahead of the deadline to register under Australia's new transparency scheme for former officials. In some cases, former officials work for Chinese or Hong Kong businesspeople through their personal consulting companies, obfuscating the sources of their income.

5. *Universities*: The united front system targets foreign universities, leveraging their access to cutting-edge technologies, talents, and opportunities to cultivate relationships that align with China's interests. By engaging with academic institutions, Beijing seeks to gain access to sensitive intellectual property and recruit scholars and students for its broader objectives. The CCP also tries to co-opt academics to build discourse power, reinforcing preferred narratives and whitewashing its track record.

- On cultivating relationships, in September 2024, the “1+10” Sino-U.S. University Presidents’ Dialogue was hosted at the University of Chicago. Wang Dinghua, CPPCC member and secretary of the Party Committee of Beijing Foreign Studies University, gave a keynote on promoting academic cooperation between Chinese and American universities, including people-to-people exchange and the development of joint research initiatives. The event was attended by U.S. universities such as Harvard University, Yale University, University of California, Los Angeles, Carnegie Mellon University, and Georgetown University at least one of which has programs funded by united front-affiliated actors.

- The Confucius Institute program—ostensibly under the Ministry of Education and Hanban—creates a beachhead in university administration through which the party’s influence can expand. Although a Confucius Institute appears focused on language training and cultural programming, they sometimes provide opportunities for staff to move into influential positions. Confucius Institute directors can be found on faculty committees and advising engagement offices on how to handle China. In some cases, the institutes have given Beijing a voice in a university’s hiring decisions for China-related faculty and affected the kind of speakers invited to the university. Australia’s John Fitzgerald, an astute observer of the party’s influence operations, wrote that accepting a Confucius Institute signaled a university was “prepared to make an exception for China on questions of academic freedom, teaching curriculums, and research integrity.” Not every Confucius Institute has proven to be problematic, but it has depended on whether the university avoids exceptions and ensures the institute operates within the agreement. The 2021 National Defense Authorization Act prohibited the Department of Defense from providing funding to U.S. institutions hosting a Confucius Institute. It encouraged most universities to shut the institute down, but the network it has built remains active. The universities maintained close relationships with their Confucius Institute partners.

6. *Companies*: The Party targets foreign companies for their financial resources, and global networks through investments, partnerships, and financial incentives to deepen economic ties. In some cases, corporate revenues inside the PRC are used as a threat to pressure the companies into lobbying their home governments for policy changes, as Ericsson was reportedly pushed to do on Huawei’s behalf in 2020.

7. *Politicians and local governments*: The united front system targets politicians and local governments to push its narratives and agenda abroad. Other mechanisms for building relationships with politicians and local governments include establishing sister states and cities partnerships and hosting economic forums and delegations to the PRC. These partnerships create opportunities for the united front system to influence local policies, shape public opinion, and marginalize competing narratives.

- In March 2023, Associated Press reported that China has successfully influenced lawmakers and has been able to promote China-friendly policies and narratives in Utah. Through Le Taowen, professor of information systems and technologies at Weber State University and a CPPCC overseas delegate, the PRC was able to establish friendly local government relationships, organize friendly visits, and pass resolutions such as promoting the Chinese language education system in Utah and bills that support friendly relationships with China.

- A recent case is Linda Sun, a former employee of the New York State government. Sun acted as an agent under the direction of the PRC representatives to push for the PRC agenda, including blocking Taiwanese government from accessing New York State officers and providing unauthorized invitation letters to PRC officials from the office of New York State officers to facilitate their travel. Sun often attends united front organization events that carry narratives that are pro-Beijing.

8. *Congress*: Congressional members are another key target with which the united front system aims to build relationships. By leveraging lobbying efforts, donations through intermediaries, and coordinated outreach by united front-linked organizations, Beijing seeks to shape legislative decisions and promote narratives favorable to the PRC. The PRC also uses the so-called “civic organizations” in China to engage with congressional members and staffers. The Chinese People’s Institute of Foreign

Affairs, affiliated with multiple united front officials and aims to “dedicated to enhancing people-to-people friendships” and “establishes and strengthens connections and exchanges with prominent political and social figures, parliaments, think tanks, media organizations,” is one of the first to engage in friendly exchanges with the U.S. Congress. This organization alone has hosted at least approximately 500 U.S. Congressional delegations to the PRC.

V. WHAT IS THE HARM?

The harm caused by Beijing’s political influence and united front operations takes several forms, even if many of these problematic activities do not meet a current threshold of illegality. Moreover, Beijing would not allow many of these activities to occur inside its borders with any foreign involvement without first being co-opted by the party-state. The lack of reciprocity helps reinforce the imbalance in most countries’ relationship with the PRC. We should not accept many of these activities as being legitimate actions of a foreign state inside the United States or other countries, because the nature of the Party’s objectives and united front system’s explicit role in political struggle mean that they are not acceptable for democratic societies even when they are not illegal.

1. *Western Politicians Become Symbols for the Chinese Communist Party’s Rule:* By using party-controlled community organizations for their outreach to ethnically Chinese constituents, Western politicians become propaganda fodder for the Chinese Communist Party. Politically aware Chinese in the People’s Republic of China (and sometimes abroad) can recognize these groups for what they are: pawns of the party. The reason for the publicity surrounding these meetings and fundraisers is to broadcast back into China the message that Western politicians care about liberalism at home, but not for Chinese people, and that they stand on the side of the party. They reinforce the image of the party’s strength.

Vaclav Havel captured this dynamic in his essay *The Power of the Powerless* by describing a greengrocer placing a slogan of regime loyalty in his shop window. He does not believe in the regime or its ideology, but he does so to make his life a little bit easier. Nor do people necessarily notice or read the slogan, because similar slogans can be “found in other shop windows, on lampposts, bulletin boards, in apartment windows, and on buildings.” The presence of these slogans becomes part of the “panorama of everyday life.” This panorama “reminds people where they are living and what is expected of them. It tells them what everyone else is doing, and indicates to them what they must do as well, if they don’t want to be excluded, to fall into isolation, alienate themselves from society, break the rules of the game, and risk the loss of their peace and tranquility and security.” By participating even inadvertently in united front-sponsored events, U.S. politicians and their foreign counterparts help the Chinese Communist Party build Havel’s “panorama of everyday life” for the Chinese people and their own ethnic Chinese citizens.

2. *The Chinese Communist Party Mediates Between Chinese Citizens and Their Elected Representatives:* The network of united front “community organizations” creates a fake civil society. The community which is supposedly represented is supplanted by the Chinese Communist Party, unless politicians reach directly to membership or deal with uncompromised organizations. The party’s interests become the constituency interests that are presented to officials.

3. *The Marketplace for Ideas Is Distorted:* Having a pluralistic, democratic society means engaging with differences of opinion. There is a natural ebb and flow. As noted above, the defining feature of the party’s united front operations is the effort to control platforms rather than just the narrative. As platforms are compromised, the voices and messages they carry change. They may not specifically represent the Chinese Communist Party, but they will avoid criticisms or subjects that are intrinsically damaging to the party’s image, standing, and legitimacy.

4. *The Party Suppresses Discussion of China’s Future:* The Chinese Communist Party’s control inside China means that any version of China’s future without the party must be discussed and decided beyond China’s borders. The extent to which the party monopolizes the social space of Chinese people—especially those who would like to return to their home country—is the extent to which the party can preempt the transmission of liberal political values into China and discussion of China without reference to the party.

5. *Undermining the Integrity of Policymaking:* At its worst, the party’s political influence and united front operations distort policymaking and the process of gathering information to feed into the policy process. The primary targets of united front work are socially influential individuals, such as politicians, prominent businesspeople, intellectuals, and sometimes even celebrities.

There is some reason to suspect that the united front system plays a role in feeding foreign intelligence services information. In conversations with former U.S. intelligence officials and serving foreign ones, they described questionable sources over the years whose information seemed too good to be true. The sourcing for their political reporting appeared sufficiently plausible and good to encourage officers to avoid placing too much scrutiny on the policy implications of the reporting or the light in which that reporting seems to paint around the Party's politics and positions. Such reporting can shape the perceptions of U.S. policymakers, reinforcing Beijing's preferred view about the Party's intent or presenting opportunities where none exist to lead policymakers to waste time and energy.

6. *Facilitating Intelligence Operations and Technology Transfer*: The united front network of organizations and relationships in overseas Chinese communities has been used to facilitate the theft and transfer of technology from the U.S. companies and research institutions. There are numerous cases of technology theft in which the risks posed by the individual were foreseeable because of their direct connections to united front organization or because they had established their own united front organization to identify and mobilize others to support their illegal activities. Among the many examples are the following:

- Tan Hongjin, who pleaded guilty of trade secret theft, transmission, and possession in 2019 that was worth more than \$1 billion, was the president of CalTech Chinese Association and received the Chinese Government Award for Outstanding Self-Financed Students Abroad.
- Huang Leping, General Manager of General Technology Systems Integration Corporation (GTSI) who was charged in October 2010 for illegally exporting high-speed analog-to-digital converters to the PRC through the PLA-linked China Electronics Technology Corporation's 24th Research Institute, was the president of the U.S. Wenzhou Association and the U.S. Zhejiang Commerce & Culture Association.
- Li Tao, who pleaded guilty for conspiracy to steal trade secrets from GlaxoSmithKline to benefit his own China-based pharmaceutical company Renopharma in September 2018, was a Science and Technology Committee member of united front-linked Jiangsu Overseas Chinese Entrepreneurs Association and was part of several other talent programs.

Current and former intelligence officials inside and outside the United States believe the Chinese intelligence services make use of the spotting and assessing opportunities created by united front system-sponsored visits to China for education, culture, and business. Alex Joske showed how the UFWD system provides cover to Ministry of State Security intelligence officers operating from within the PRC and abroad.

VII. THE ROLE OF THE U.S. DEPARTMENT OF STATE

The U.S. Department of State plays several important roles in countering united front work and the CCP's other political warfare operations, particularly outside the United States. First, U.S. diplomats are America's eyes and ears on the ground for identifying and observing CCP influence and other related activities around the world. They might well be the first to spot new trends, developments, or the evolution of CCP tactics. Many developments in united front work or other CCP influence operations are first used outside the United States. Diplomats and their local contacts may well provide the earliest warning of new tactics and techniques being used by the Party. Second, the State Department identifies, supports, and maintains connections to local civil society organizations, individuals, and other partners who are working to counter CCP interference. This is about helping those who are trying to help their own country resist the Party's interference and manipulation. It is consistent with long-standing U.S. practices going back to the beginning of the cold war with the Soviet Union. Third, the department should be coordinating the U.S. Government's international activities toward a common purpose. It is easy to fall into the trap of acting as a traffic cop, simply providing "stop" and "go" commands. The State Department in conjunction with the White House should be providing clear guidance about what kind of activities support U.S. objectives, counter the CCP's activities, and support the local partners standing up for their own country's sovereignty and interests.

From a historical perspective, we should remember the American way of modern political warfare emerged from the State Department. Many of the initiatives, like the Marshall Plan and support to democratic parties in Europe and elsewhere, were, at least internally, understood as coordinating the non-military elements of national power to counter the Soviet Union. The State Department needs to reclaim this generalship today, which is more a question of priorities, interest, and guidance than

it is of authorities. When the Secretary of State emphasizes these activities, especially in the information space, and takes a personal and supportive interest in them, then the United States performs well. The American approach to political warfare has been underpinned by the idea of providing a true experience of Americans to the world and that supporting people's hunger for truth and meaning in their lives will create better conditions for U.S. national interests to be achieved.

VIII. GUIDING PRINCIPLES IN RESPONDING

It is impossible to provide a comprehensive list of policy recommendations, and many of those recommendations could be hypotheses about what works to counter the CCP's efforts to shape foreign perceptions and mobilize people on its behalf. Nor could one individual provide an exhaustive list. Below I outline several principles that are consistent with democratic values and my own understanding of what has been successful in specific cases of countering CCP united front operations. These principles provide a framework for generating and evaluating policy recommendations.

1. *Transparency*: Sunlight is the best disinfectant. Out in the open, people have to make choices about whether to continue on in their conflicts of interests or compromised relationships. This applies equally to government and law enforcement responses to political interference. Administrative responses done quietly are not as effective as public prosecutions and explanations, which help create risk and inject new information into the public sphere for discussion.

2. *Conversation and Debate*: The legislature draws the line between legal and illegal. Federal Government resources always will focus predominantly on the illegal side. In a democracy, we would not want it any other way. What is unacceptable or improper, however, is not necessarily what is illegal. Civil society must be able to discuss in reasonable terms what is taking place.

3. *Protect Space for Critical Discussion of China*: Whether it is Chinese-language media outside of China, university spaces, or any other platform where discussion of contemporary China takes place, they all are vulnerable to the party's pressure. And they all are targets of the Chinese Communist Party. They need support, protection, and sometimes even cultivation.

4. *Consequences Create Risk*: Until the Chinese Communist Party faces consequences for its actions, they are not in danger of overstepping the mark or overestimating their ability to influence or intimidate. Without successfully taking cases to and winning at trial, without administrative penalties, Americans who actively assist the Chinese Communist Party at the expense of U.S. interests will have no reason to scrutinize their actions or to desist. Risk is required to deter behavior that undermines democracy.

5. *Civil Liberties as much as National Security*: Because the Chinese Communist Party puts so much emphasis on overseas Chinese communities and individuals, countering Beijing's efforts means ensuring ethnically Chinese citizens and residents can enjoy equal protection under the law. National security and the resources brought to bear in its name are negative, defensive powers rather than positive or creative. Civil liberties protections and the resources deployed for this purpose, however, are the latter. They serve to guarantee constitutional freedoms, creating and preserving the free space for speech and association. Enabling democratic practices is at least as important as preventing the exploitation of democracy.

6. *Maintain the Integrity of Rules and Processes*: When relationships with Chinese Communist Party organizations go awry or become exploitative, most cases—excepting those involving recruited or compromised agents—involve foreign partners who do not monitor and enforce their own guidelines and procedures. To protect against conflicts of interests and outright compromise, organizations that seek to do business, promote exchanges, collaborate on research, or otherwise have institutional relationships need to establish and stick to rules and procedures. Exceptions and exemptions need to be done in the open with clear explanation; otherwise, it is too easy to slip toward compromise and exploitation.

IX. RECOMMENDATIONS FOR CONGRESS

1. Revise the Foreign Agent Registration Act (FARA) to include more robust reporting requirements, more robust penalties for non-compliance, and a publicly accessible data base of FARA registrants updated frequently.

Others have more fully outlined the fixes that need to be made related to the Foreign Agent Registration Act, but I would like to emphasize a few points. First, the reporting requirements for describing the activities are quite minimal. Companies and individuals that wish to be safe provide more; however, that is not the general rule. Expanding the reporting requirements to include more substance and speci-

ficity about the messages delivered or services provided would make the reporting mechanism more transparent. Separately, additional reporting could be made a part of congressional ethics standards. Second, non-compliance with FARA seems to have few if any consequences. The current approach to enforcement is largely about voluntarily self-policing. Third, the United States should revise its approach to presenting FARA data, modeling its public-facing data base on the Australian Foreign Influence Transparency Scheme (FITS). The FITS data base is updated on a regular, rolling basis rather than the quarterly approach to FARA. The data base and accompanying documentation is comparatively clear and accessible.

2. Request a review of the Department of State's Countering People's Republic of China Influence Fund (CPIF) and new strategic guidance on how the funds are applied.

The CPIF fund is the product of bipartisan recognition that funds need to be devoted to the purpose of countering CCP malign influence. Anecdotal evidence from the State Department suggests that much of the funds goes to existing programming that may or may not be directed at the Party's influence and interference. A Confucius Institute in a foreign city or university does not make an English-language program in that city or university an initiative to counter Beijing.

New strategic guidance will necessarily be broad, but should include at least some of the principles outlined above. Moreover, priority should be given to programs that interrupt the political process through which the CCP builds power. When the United States or its allies wait too long and allow the CCP to become too established, they end up deflecting tactical efforts. While this sometimes is effective in the short term, it requires forewarning to take action and over time a relentless CCP will succeed in achieving its objectives, whether a military base, a policing agreement, or a telecommunications deal. This has been seen over and over in places like the Solomon Islands and the fights over whether a country recognizes the People's Republic of China or Taiwan.

Such guidance also could carry over to the U.S. Agency for Global Media and its media outlets, such as Voice of America and Radio Free Asia. The law is clear about the separation between USAGM content and U.S. Government direction, preserving journalistic integrity and the desire to ensure that these are not simply U.S. propaganda outlets, equivalent to Xinhua, the Chinese Global Television Network, China Radio International, and the like. However, the law is also clear that these organizations should report on news relevant to U.S. policy, that the U.S. Government thinks is important, even if the content is independently produced and reported. Exposing the CCP for what it is and the perniciousness of its activities is in the U.S. interest.

3. Invest in expertise building inside and outside the U.S. Government.

Countering the CCP's interference and malign influence requires country-specific expertise, even if the laws and regulations are country agnostic. U.S. access to the PRC, however, is becoming more constrained for both the public and private sectors as Xi Jinping has tightened security measures and the U.S.-PRC relationship has become more fraught. Fewer Americans are studying China and Chinese language(s). And the United States does not have the expertise it needs to enforce the policies it already has.

In the 116th Congress, none of the various U.S.-PRC competition bills included investments in developing expertise and language skills. This stands in stark contrast to the early cold war, when the White House and Congress realized the need to invest in expertise. The National Defense Education Act of 1958 created substantial investments in area studies, particularly related to the Soviet Union, and the United States continued such programs through Title VI of the Higher Education Act. 45 Congress should create and fund educational programs to support mid-career expertise building and language skill maintenance. Existing programs focus almost exclusively on undergraduate and graduate students at the beginning of their careers. Creating space and time for experienced professionals to brush up on language skills or pursue useful personal projects would help ensure continued learning. Government employees have some access to similar programs, but there needs to be greater recognition of the value of education and being away from the desk. Private sector employees need new programs and sources of support to be able to take the time to study and return to work.

4. Reverse reporting requirements on sanctions and other congressional authorities relevant to executive branch actions, so that agencies like the Department of State have to report when authorities go unused.

Congressional reporting requirements often create a perverse incentive for the Department of State and other executive departments to not take action using the au-

thorities provided by Congress. As a general, U.S. Government officials do not like providing congressional reports on their activities. As a result, significant authorities have gone unused because they do not want to go through the process of providing the report to Congress. Alternative authorities are applied or nothing is done at all. By requiring U.S. officials to report to congressional oversight every 90 days or some other appropriate length of time that the authority goes unused, Congress will strengthen its oversight of U.S. policy and create a better incentive for U.S. officials to follow congressional intent.

5. Congressional reporting on CCP malign influence should focus on enabling action rather than situational awareness.

Most congressional reports required of the executive branch are requests for situational awareness. This has overburdened the departments and, in many cases, Congress would be better served turning to the Congressional Research Service, the Government Accountability Office, or universities, think tanks, or other external research organizations. The problem of CCP malign influence is well known, and many aspects of it have been catalogued in detail by The Jamestown Foundation, the Australian Strategic Policy Institute, Sinopsis (Czechia), Safeguard Defenders, and many individual analysts. Where once there was a paucity of information, analysis, and expertise, there is a growing global network of analysts, journalists, and officials who can provide the general information usually required in congressionally mandated reports.

Instead, congressionally mandated reports should request information that enables action, like targeting packages for sanctions, entity lists (such as those at the Departments of Defense, Commerce, and Homeland Security). Congress cannot require the executive branch to take certain actions. There is a bipartisan presidential consensus, for example, that Congress cannot require the executive branch to place sanctions on companies or individuals. Presidents claim that is not a congressional power. And practice has made this a reality. However, by demanding the compilation of materials required for specific executive actions, Congress will create reports that entrepreneurial U.S. officials can leverage to drive action either in the moment or at some time in the future.

6. Use Congress's institutional powers to press the executive branch for transparency on actions taken against China, especially where the actions are administrative.

American opinions are shifting about China, but much of the public discussion remains caught in limbo between the old policy paradigm and the uncertainty of today's new era of competition. Consequently, the administration needs to be more transparent than the executive branch typically is inclined.

The visa denials for Chinese scholars is a perfect example from recent news. Many U.S. and international scholars have been dismayed by the news, and the merits of excluding those individuals or revoking their visas is not obvious to the public. The particular case of Zhu Feng, a Nanjing-based professor, having his visa revoked shows why the executive branch needs to be more transparent publicly. Although he is a well-known scholar known for his amiable humor, Zhu also has been supported by and done work for the political warfare element of the People's Liberation Army. This is available from open sources. Putting a few simple criteria out in public for visa denials and alerting inviting institutions what criteria was triggered would be a useful positive step for handling the visa issues going forward. Without such information, many otherwise knowledgeable people about China assumed the worst about the administration's intentions and actions.

The administration also should be encouraged to use the legal system and press charges where appropriate. The legal process forces the U.S. Government to commit to a course of action and make some information public. That information, especially after a conviction, becomes as close to ground truth as possible on sensitive subjects for which there is not much clear, public information.

Senator RISCH. Thank you very much, Mr. Mattis.

We will turn now to Mr. Jeffrey Stoff. He is the founder of the Center for Research Security and Integrity. He previously spent nearly two decades in government focused on risks to the security and integrity of research from adversarial or authoritarian nations. He now advises academia, governments, and businesses on these matters.

Mr. Stoff, the floor is yours.

**STATEMENT OF JEFFREY STOFF, FOUNDER, CENTER FOR
RESEARCH SECURITY AND INTEGRITY, HERNDON, VIRGINIA**

Mr. STOFF. Chairman Risch, Ranking Member Shaheen, and distinguished members of the committee, thank you for the opportunity to testify today on this critically important topic.

Now that I no longer work in the government I can speak very candidly about the PRC's method to exploit our innovation ecosystem and the failures within both the government and academia to address this problem.

Over the last 15 years I have studied China's research ecosystem and how the party state exploits our innovation. I worked closely with most Federal agencies that fund scientific research as well as law enforcement and intelligence components.

That support has exposed me to a range of deficiencies and failures of the U.S. Government, which were a source of my frustration and the reason I resigned from Federal service in 2021.

Today, neither academia nor governments of liberal democracies have sufficiently adapted to a contradictory reality. One of the most significant participants in the global scientific enterprise is also our greatest adversary, an extremely oppressive regime that seeks to dominate and displace the U.S. technologically and militarily, to reshape the world order, and to preserve the Communist Party's interests.

It is past time to have candid and uncomfortable conversations about the current state of how the PRC's unfettered access to our research ecosystem and its malign influence activities have profound effects on our national and economic security and the corrupting and corrosive effects that are enabled by the negligence of U.S. partners.

U.S. universities are run like businesses with the primary objective of generating revenue. Academia's incentives are often not aligned with U.S. national security and economic interests.

Systemic noncompliance on Federal research grants and its willingness to accept and fail to report PRC sources of funding often run counter to the values of transparency and integrity that academia espouses.

My written testimony shows examples of academia's widespread disregard for security or ethical concerns. I provide low estimates of over 27,000 articles published just in the past 5 years involving collaboration between U.S. institutions and PLA medical entities, weapons design and production facilities, state owned defense enterprises that supply the PLA, key defense research universities, and entities that develop and deploy mass surveillance technologies to PRC public security organs enabling human rights abuses.

Much of this research is funded by Federal agencies, private foundations, and corporate sponsors with few restrictions or regulatory oversight.

The U.S. Government has done little to deter academia from failing to comply with Federal research grant rules such as failing to disclose PRC money and support, which sometimes appear to be an attempt to disguise contracted research for the PRC as unrestricted gifts.

This, combined with PRC programs that task and incentivize U.S. faculty members to bypass merit based hiring decisions, con-

duct research projects at the PRC's behest, and a swath of other malign activities, create corrosive secondary effects as well.

These include a vicious cycle of inequity in the system. Smaller schools that are being honest but denied Federal funding have smaller budgets and fewer resources to hire Ph.D. students, attract top talent, et cetera, which then makes them less competitive on future grant proposals. This also translates to fewer opportunities domestically and an erosion of STEM talent pipelines.

Compounding these problems are abject failures by the FBI's near exclusive focus on criminal investigations as a hammer looking for a nail that fails to protect earlier stages of our research ecosystem as well as the intelligence community's failure to adapt to post-cold war realities and the asymmetric threats posed by China, which only seldom involve espionage activities.

The scale and scope of China's predations in our research ecosystem are largely unknown, making it impossible to determine the level of influence the PRC exerts over U.S. research that overwhelmingly benefits China.

My testimony discusses issues that go beyond the jurisdiction of this committee. My recommendations seek to close regulatory gaps and bolster compliance and enforcement mechanisms, and have State Department play a much larger role in many of these areas to ensure that real costs are imposed to the PRC when it violates commonly accepted norms and values of scientific research.

To effectively counter the PRC's malign influence, we must find the courage to break down silos and build new paradigms for cooperation among and between Federal agencies, legislative committees, and our key allies and partners around the world.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Stoff follows:]



Written Testimony of Jeffrey Stoff

Founder of the Center for Research Security & Integrity

**Before a Hearing of the Senate Foreign Relations Committee
 “The Malign Influence of the People’s Republic of China at Home and Abroad:
 Recommendations for Policy Makers”
 January 30, 2025**

Chairman Risch, Ranking Member Shaheen, and distinguished Members of the Committee:

Thank you for the opportunity to testify today on this critically important topic. Now that I am no longer working in the government, I can speak candidly about the PRC’s methods to exploit our research and innovation ecosystem and the failures within both the government and academia to address this problem. The last section of this testimony provides specific recommendations to combat the threats posed by the PRC at home and abroad.

Over the last 15 years, I have focused on China’s research and innovation ecosystem and its state-driven knowledge and technology acquisition apparatus. The collection and analysis programs I ran while serving in the government provided insights into China’s technology transfer strategies, PRC state-sponsored talent programs, and other methods of PRC influence over research at national laboratories and academic institutions. I worked closely with most federal agencies that fund scientific research - including the National Science Foundation, National Institutes of Health, NASA, the Departments of Defense, Energy, and Commerce - as well as law enforcement and intelligence components. That support has exposed me to a range of deficiencies, vulnerabilities, and failures of the US government and academia, which were a key source of my frustration and the reason I resigned from federal service in 2021 after 18 years.

This testimony catalogs various ways the PRC exploits our R&D ecosystem, acquiring and diverting knowledge for purposes that undermine our national and economic security, and how the PRC violates norms and values of transparency, integrity, and reciprocity regarding scientific research and international research collaborations. I provide specific case examples from my research as well as observations and trends derived from my support to various civil, criminal, and national security investigations when I served in the government; some of this material lacks detail on specific entities as that information is not approved for public release.

Throughout this testimony, I candidly discuss the abject failures of the intelligence and law enforcement communities concerning its ability to protect our innovation ecosystem from China’s predations and highlight some structural deficiencies that impede its progress. Equally important, I also highlight US academic institutions’ failures to live up to the value system they espouse *and the corrupting and corrosive nature of PRC activities that affect our research enterprise*. Some of this involves raising uncomfortable truths that heretofore have not been discussed in public.

Many of the issues and recommendations discussed in this testimony go beyond the jurisdiction of this committee. One of our impediments is the siloed nature of the Executive Branch, and China's predations transcend the responsibilities or authorities of individual agencies (and legislative oversight committees). We must have the courage to upend the status quo where our collective responsibility has been a collective action problem. The last section of this testimony provides specific recommendations that seek to address some of the problems I highlight. Throughout this testimony, I also pose questions that require further inquiry and policy deliberations before specific actions or recommendations can be made.

Table of Contents

Introduction	3
<i>Sampling</i> of Challenges and Failures of the US Government	3
<i>Sampling</i> of Methods of PRC Malign Influence and Exploitation of Our Research Ecosystem	4
I. US Academia: Vulnerabilities, Misaligned Incentives, Negligence, and Complicity	5
Research Collaborations of Concern	7
Patents: Directing or Diverting US Innovation for China's Benefit	13
Ethical Risks in PRC Research Collaborations	16
Malign Influence from PRC Funding and Resources	19
Case Examples	20
II. Understanding PRC Talent Programs Beyond Research Security: Integrity and Malign Influence Matters	23
Case Example 1: Corrupting NOAA Research and Operations	25
Case Example 2: Former UCLA Professor	27
Exploitation of Other Federal Funding Sources	28
Hijacking NSF CAREER Awards	28
Exploiting SBIR Programs	29
Technology Acquisition Networks	29
III. China's Role in Undermining Research Integrity and US Inaction	30
Case Example: 'Comfort Letters'	32
Reciprocity	33
IV. Brief Discussion of IC, FBI Failures, Knowledge Gaps	33

Persistent Knowledge Gaps	35
China's Defense and Surveillance Research and Industrial Bases.....	35
University-Industry Integration.....	36
V. Brief Overview of Allied Nations and Innovation Security	36
VI. Recommendations for Policy Makers	40

Introduction

Sampling of Challenges and Failures of the US Government

I founded a 501(c)(3) organization, the Center for Research Security & Integrity, in part to address government failures and the structural impediments to knowledge building and threat mitigation. A *non-exhaustive* list of these failures include:

- A focus on pursuing criminal cases to mitigate threats that overlook most of the threats to – and malign influence over – our research and innovation ecosystem (especially at earlier research stages) that is subject to minimal regulatory oversight. China's predations often do *not* involve espionage or intellectual property (IP) theft as defined by the US criminal code within fundamental research domains. Messaging by the US government that China is stealing secrets from academia is misleading and misguided.
- A dearth of Chinese language-capable analysts and subject matter experts in the US government has led to a fundamental lack of understanding of the magnitude and complexity of China's state-supported technology acquisition and transfer apparatus.
- Failure of the counterintelligence community to sufficiently adapt to post-Cold War realities. A myopic focus on chasing PRC spies leaves most of our research unprotected as the PRC deploys a range of tactics, infrastructures, and human capital to acquire US technology and knowhow that rarely involve its security services. While I was in the government, my support to counterintelligence elements in the FBI and DoD showed that those offices prioritized criminal investigations over leveraging operational approaches to deny and disrupt PRC state-directed technology transfer activities.
- Failure of the Intelligence Community (IC) to understand, track, analyze, and respond to significant components of PRC's "united front" influence operations that support technology transfer efforts. The US government holds a prevailing view that the Chinese Communist Party's united front is strictly a political influence apparatus.
- A multi-decade descope and devaluation of open-source intelligence within the IC has led to unaddressed and yawning knowledge gaps, a lack of expertise, and an inability to share information with public and private sectors.
- Similarly, persistent knowledge gaps on PRC academic and commercial entities conducting R&D tied to defense and public security apparatuses limit our ability to identify risks, especially in

critical and emerging technology fields.

- A lack of any significant or material support to US research institutions regarding research security and integrity; the burden of conducting due diligence and risk assessments is placed almost entirely on individual institutions. To date, the US government has been unable to provide a knowledge base, data, or other resources to aid US universities in their risk assessments related to their foreign partners. This situation will hopefully improve with the newly created SECURE Center funded by NSF, but there will be limits to the ways it can support all research institutions.
- Inadequate resources and personnel in Offices of Inspectors General severely constrain their ability to investigate fraud or malign foreign influence or interference in federally sponsored research.
- A lack of understanding of how China has built a massive apparatus to recruit experts globally and exploit US (especially federally funded) research. Experts are primarily targeted by the PRC *after* gaining knowledge and experience overseas. The argument that high percentages of PRC nationals stay in the US after post-graduate education and thus benefit the US is too simplistic; much of China's strategy is to tap into overseas-based experts who "serve in place." Creating incentives to stay with no corresponding protections has allowed the PRC to exploit and influence our research to its benefit with impunity.

Sampling of Methods of PRC Malign Influence and Exploitation of Our Research Ecosystem

The threats and malign influence posed by the PRC on our research and innovation ecosystem and the implications - including the corrupting and corrosive effects - is an under-recognized problem. The scale and scope of PRC influence are largely unknown, but this testimony provides insights into the enormity of the problem. Also note that most advanced nations, particularly our key allies, face many of the same predations from China. Much of the PRC's malign influence activities also undermine the integrity and trust of scientific and engineering research. A *sampling* of some of the threats include:

- Converting or diverting US government-funded research into IP that is commercialized in the PRC that may be in violation of research grants or university terms and conditions or, at minimum, solely benefit the PRC.
- Repurposing US research, including in seemingly innocuous fields like climate change and hearing aid research, to PRC defense programs and weapons system development that can undermine or eliminate US military superiority.
- Directing or redirecting US critical technology research funded by industry and federal and state governments by selectees of PRC talent recruitment programs who are under contract with and tasked by the PRC government.
- Improperly influencing or manipulating federal research grant evaluations and award decisions.

- Applying US research to enable or enhance the PRC's domestic surveillance apparatus and human rights abuses.
- Influencing or co-opting US academics' hiring or sponsoring of PRC national PhD students, postdoctoral fellows, and visiting researchers that circumvent merit-based processes and build talent and training pipelines that overwhelmingly benefit China.
- Establishing or co-opting networks of organizations in the US that enable knowledge transfer, talent recruitment operations, and venture capital investments intended to offshore critical technology to China.
- Influencing or tasking researchers at federal research facilities and laboratories to facilitate formal cooperative agreements with PRC institutions, sometimes violating internal conflicts of interest and ethics policies
- Engaging in behaviors that violate norms of integrity, transparency, reciprocity, and other areas that equate to deception, fraudulent publications, laundering the reputations of foreign research institutions, and numerous other ill effects.

I. US Academia: Vulnerabilities, Misaligned Incentives, Negligence, and Complicity

In some respects, academia has been victimized by China's exploitation and malign influence through vulnerabilities inherent in the open nature of how science is conducted. It is unrealistic to expect individual institutions (and even large technology firms that engage in research) to be able to sufficiently protect themselves against the predations of the PRC party-state and the massive resources and infrastructures it has put in place to target US and allied nations.

Some of China's exploitation comes from a natural evolution of how scientific and engineering research is conducted. Academic institutions have traditionally viewed science as a borderless endeavor; pursuing the frontiers of knowledge and betterment of humanity supersedes transitory geopolitical concerns. Governments in liberal democracies have also shared this view: science and technology diplomacy and academic freedom (and freedom to pursue any partnerships and flows of talent) have greatly benefited technological and economic development and such benefits have in the past outweighed any risks. That principle held true for at least half of a century after the Second World War. But this era of progress was partly due to the fact that allied nations were so much stronger technologically and economically that authoritarian regimes played a very small role – or even participation in – the scientific enterprise.

Today, neither academia nor governments of liberal democracies have sufficiently adapted to a contradictory reality: one of the most significant contributors to and participants in the global scientific enterprise is also our greatest adversary and strategic rival: one of the world's largest and most technologically advanced economies is also one of the most oppressive authoritarian regimes in history and has a primary objective of dominating and

displacing the US technologically and militarily to reshape the world order and to preserve Chinese Communist Party (CCP) interests.

But this is not the whole story. An uncomfortable truth is that much of China's efforts to exploit, influence, and corrupt our research ecosystem require at least, in some part, the willing participation by US academia – especially where PRC influence has had the most corrupting and corrosive effects. The reality is US universities are run like businesses: their principal objective and motivation is to generate revenue. Money drives most decisions, not security or integrity. When describing “willing participation,” I include in that concept a lack of awareness, negligence in taking responsibility for identifying and mitigating concerns, complicity, willful violations of integrity, and disregard for grant rules and conditions intended to ensure fairness, equity, and responsible allocation of federal resources.

This testimony describes both aspects: the victimization of our research by China through the exploitation of our open system and how US research institutions have enabled (willingly or not) PRC malign influence and exploitation.

Federal funding agencies, law enforcement, and intelligence community (IC) elements have done a good job of raising awareness among universities on national security risks and compliance and integrity concerns. US research institutions understand and recognize that there are real risks and concerns that need to be addressed and mitigated. But this often conflicts with academia's primary goal of attracting sustaining revenue sources (and human capital) from anywhere and anyone. Security and compliance, like the private sector, is a cost burden, not an operational priority. *Consequently, the financial incentives and operations of universities often run counter to US national and economic security interests.*

Many US universities have put research security programs in place, partly due to new requirements stipulated in National Security Presidential Memorandum-33 (NSPM-33). That policy requires research institutions receiving more than \$50 million in annual federal funding to certify to funding agencies that the institution has established and operates a research security program, which includes elements of cyber security, foreign travel security, insider threat awareness and identification, and, as appropriate, export control training.”¹ However, NSPM-33 requirements offer no detail or standards of what a research security program should look like. This can become simply a box-checking exercise for universities to claim they have put in place a program.

National Security Decision Directive 189 (NSDD-189), a policy that has been in place since the 1980s, states that the US government will not restrict sharing or collaboration in fundamental research domains except in rare circumstances where national security concerns require classifying the information. This also means that fundamental research, which is defined as both basic and applied research that is published openly, is not subject to export controls or other regulatory restrictions or oversight. There are currently only two

¹ <https://trumpwhitehouse.archives.gov/presidential-actions/presidential-memorandum-united-states-government-supported-research-development-national-security-policy/>

exceptions where Congress has put in place restrictions concerning fundamental research collaborations with adversarial nations including China.

The first relates to an appropriations law that places “Chinese Funding Restrictions” on NASA (also known as the “Wolf Amendment”), prohibiting recipients of NASA funding from engaging in bilateral participation, collaboration, or coordination with the PRC or Chinese-owned companies, including Chinese universities.² Multilateral research exchanges involving China and any additional country are exempt from this restriction. The second is a restriction stipulated in the recently passed FY25 National Defense Authorization Act (NDAA), (Sec. 238) that makes institutions ineligible for Department of Defense funding for fundamental research if the US institution collaborates with a set of PRC entities listed in other provisions of the NDAA (as stipulated in Sec. 1286 of the FY19 NDAA).

All other sources of federal funding currently have no restrictions; researchers and institutions are free to partner, collaborate, establish cooperative programs, etc., with any PRC entity of their choosing. Like other countries except Canada,³ the government can merely provide guidance on national security risks, but universities can ignore this provided they are compliant with existing federal grant requirements. From a legalistic perspective, there are few incentives for universities to create robust security policies that restrict their fundamental research activities or partnerships.

Research Collaborations of Concern

To be fair, universities rightly point out that most lack the resources, foreign language capabilities, and subject matter expertise on PRC entities and geostrategic concerns to conduct robust due diligence and national/economic security risk assessments; this is a burden placed almost entirely on the research institution. Further complicating this issue are knowledge gaps and the IC’s structural impediments (discussed later) that have resulted in insufficient scrutiny of many PRC entities and the level of national security risks they may pose.

What about partnerships and collaborations with PRC entities that are widely known to represent national security risks? The data that follows provides a current snapshot of very high-risk US-China scientific and engineering research collaboration.⁴ This data is limited to a *sampling* of military entities, weapons R&D facilities, and select defense-affiliated civilian universities. Such data is not a precise indicator of malign foreign influence; **it is rather intended to demonstrate systemic unwillingness in academia to examine national and economic security risks or ethical concerns regarding their research collaborations with**

² Pub. L. No. 112-10, § 1340 and Pub. L. No. 112-55, § 539.

³ The Canadian government issued a policy that will deny federal funding for research grants if that research involves collaborations with specific PRC (and Russian and Iranian) institutions in specified critical technology fields. This policy on “Sensitive Technology Research and Affiliations of Concern” was established in the Fall of 2024. Canadian institutions are still free to collaborate with PRC, Russian, and Iranian entities, but no federal funding would be provided to them.

⁴ My testimony focuses on STEM and critical technology areas; I am not addressing PRC research collaboration in most social sciences and humanities disciplines that pose fewer national security risks.

China. Furthermore, the huge scale of these high-risk collaborations suggests dependencies and vulnerabilities that China then exploits.

Tables 1 - 4 break down the number of articles published from 2019 to January 2025, coauthored by researchers from a US-based institution and researchers affiliated with specific PRC entities part of the People's Liberation Army (PLA), subordinate to the Central Military Commission (the CCP organ overseeing the PLA), and select PRC state-owned defense conglomerates. This data reflects collaborations that represent the highest risks to national security. The data was compiled using the *Dimensions* tool by Digital Science that aggregates bibliographic metadata of journal articles, conference proceedings, preprints, patents, and other data related to published research. **Disturbingly, a total of 9,398 unique articles were identified involving coauthors based at US institutions and researchers affiliated with select PRC military institutions in just the past five years.** This understates the actual amount of US collaborations with PRC military entities due to the scoping limitations of this testimony and knowledge gaps discussed later.

Table 1 lists a *sampling* of PRC military medical units that have coauthored the most articles with US partners. This is not an exhaustive list of all US-China collaborations with PRC military medical entities. (Note: totals in these tables may exceed the total number of unique articles as there can be more than one PRC entity listed in the same article)

Table 1: US Institution Collaboration with Select PRC Military Medical Entities

PLA / Central Military Commission Medical Entity	Number of Articles with US-based Coauthors
Chinese PLA General Hospital	1,526
Army Medical University	1,012
Air Force Medical University	888
Academy of Military Medical Sciences	289

Some medical research conducted by these entities may be considered low-risk or beneficial (such as cancer research). However, the PRC party-state does not share the same values and ethical principles as liberal democracies concerning research involving human subjects, and thus even research that is beneficial in nature may be diverted to military or unethical purposes. Examples of where this matters include: China's horrific and well-documented record of human organ harvesting, incarceration of political dissidents in psychiatric hospitals, involuntary collection and use of genetic information for mass surveillance purposes, and medical research with military applications such as fighter pilot and soldier performance enhancements and human-computer interfaces for weapons programs, etc.

Consequently, collaborations with PLA medical entities can pose national security, ethical, and reputational risks for US and allied nation collaborators and their funders. It is also worth noting that both the US government and private sector entities are acknowledged as funders of this research (presumably funding the US scientists). Government funders include, but are not limited to: the Agricultural Research Service, Air Force Office of Scientific

Research, Centers for Disease Control and Prevention, Congressionally Directed Medical Research Programs, Defense Threat Reduction Agency, Department of Veterans Affairs, NIH, and NSF. A *sampling* of private companies and foundations credited as funders include Abbott, Amgen, Biogen, Boston Scientific, Bristol-Myers Squibb, Eli Lilly, Intel, Intuitive Surgical, Johnson & Johnson, Medtronic, Pfizer, the American Cancer Society, American Red Cross, Bill & Melinda Gates Foundation, Mayo Clinic, Memorial Sloan Kettering Cancer Center, and the Welch Foundation.

Table 2 lists the number of collaborations with the China Academy of Engineering Physics (CAEP) and a few of its subdivisions that are often named separately in English-language publications, i.e., CAEP is not listed as the parent organization. CAEP is China's nuclear weapons design and production complex, which also includes other advanced weapons, components, and delivery systems.

Table 2: US Institution Collaboration with PRC Nuclear and Advanced Weapons Complex

China Academy of Engineering Physics (CAEP)	Number of Articles with US-based Coauthors
CAEP (including subdivisions naming CAEP as a parent entity)	308
CAEP Subdivisions NOT Stating an Association with CAEP	
Beijing Computational Science Research Center	425
High Pressure Science & Technology Advanced Research	398
Institute of Applied Physics and Computational Mathematics	160
Science and Technology on Surface Physics and Chemistry Laboratory	16

Notes: The Beijing Computational Science Research Center works with (and is possibly subordinate to) the Institute of Applied Physics and Computational Mathematics, also known as CAEP's 9th Institute responsible for numerical / computer simulations for nuclear and other weapons designs. The Science and Technology on Surface Physics and Chemistry Laboratory is subordinate to CAEP's Institute of Nuclear Physics and Chemistry located at CAEP's primary facility in Mianyang.

Table 3 offers a *sampling* (not an exhaustive list) of PLA technical schools whose researchers have collaborated with US entities.

Table 3: US Institution Collaboration with Select PLA Scientific Institutes

PLA / Central Military Commission Entity	Number of Articles with US-based Coauthors
National University of Defense Technology (NUDT)	601
PLA Army Engineering University	69
PLA Information Engineering University	66
PLA Air Force Engineering University	36
PLA Academy of Military Science	32

China Aerodynamics Research and Development Center	29
Naval University of Engineering	19

Notes: The National University of Defense Technology is the PLA's premier scientific and engineering research institution. The China Aerodynamics Research and Development Center is the PLA's premier hypersonics R&D facility, although no English-language source indicates the center is affiliated with the military.

Table 4 offers a *sampling* of US collaboration with some of China's largest state-owned defense conglomerates and a few of their subsidiaries. Subdivisions of these state-owned enterprises have research institutes, some of which house state key laboratories and function like academic institutions. Although some of these firms do engage in civilian research and technology areas, they are run by the PRC central government with a primary mandate to support the PLA through the development of weapons systems and components, including China's missile programs. Even if US researchers can credibly claim that their research is strictly for commercial purposes, collaboration with these PRC defense firms can improve these conglomerates' commercial operations and bolster their financial position. This provides the firms more resources to advance their primary purpose of developing defense or weapons R&D and production programs, strengthening the PLA and emboldening China to become more hostile toward its neighbors, supplying and supporting other autocratic regimes (especially Russia), and challenging US military superiority and deterrence in strategic areas such as the Taiwan Strait and the South China Sea.

Table 4: US Institution Collaboration with Select PRC State-Owned Defense Conglomerates

PRC Defense Enterprise	Number of Articles with US-based Coauthors
China Academy of Space Technology	166
China Electronics Technology Group Corporation	133
China Aerospace Science and Technology Corporation	103
China State Shipbuilding (includes China Shipbuilding Industry Corporation)	77
Aviation Industry Corporation of China	56
China North Industries Group Corporation (NORINCO)	52
China Academy of Launch Vehicle Technology	29
Aero Engine Corporation of China	24
China South Industries Group	21
China Aerospace Science and Industry Corporation	18

Notes: The China Academy of Space Technology and the China Academy of Launch Vehicle Technology are subsidiaries of the China Aerospace Science and Technology Corporation. The China Academy of Launch Vehicle Technology is China's largest R&D and production facility for space launch vehicles, liquid-fueled

surface-to-surface missiles, and solid-fueled surface-to-surface and submarine-launched ballistic missiles.⁵ CALT also produces the Dongfeng series of intercontinental ballistic missiles (ICBMs), the latest versions equipped with multiple independent nuclear warheads able to strike Western Europe and the United States.⁶

In addition to PLA institutes and state-owned defense firms, there are groups of civilian universities with a primary mission to support military research and defense industries. These universities are known as the “Seven Sons of National Defense” and the “Seven Sons of Ordnance Industry” (two of these schools belong to both groups). The former group of entities originated as military academies but are now directly overseen by the State Administration for Science & Technology Industry for National Defense, the PRC government organ responsible for implementing military-civil fusion policies. These universities work on classified defense programs, house departments and laboratories that work closely with PLA organs, and partner with state-owned defense conglomerates. The universities in the latter group were previously under the supervision of the then Ministry of Ordnance Industry and continue to conduct weapons R&D as part of their core mission.

Some STEM research conducted at these universities are in civilian sectors or may lack obvious defense applications; however, it is prudent to assume that these schools will pursue potential military applications as a matter of policy and thus represent high national security risks. **There were 17,630 unique articles published between 2019 and January 2025 involving a coauthor from one of these ‘seven sons’ defense universities and a coauthor affiliated with a US institution.**⁷ Table 5 lists the number of articles involving coauthors from these schools and US institutions.

Table 5: US Institution Collaboration with PRC ‘Seven Sons’ Universities

Seven Sons of National Defense, Seven Sons of Ordnance Industry Universities	Number of Articles with US-based Coauthors
Beihang University	4,909
Harbin Institute of Technology	3,836
Beijing Institute of Technology	3,335
Northwestern Polytechnical University	2,396
Nanjing University of Science and Technology	1,770
Nanjing University of Aeronautics and Astronautics	1,507
Harbin Engineering University	723
North University of China	356
Chongqing University of Technology	208

⁵ “China Academy of Launch Vehicle Technology (CALT),” Nuclear Threat Initiative, February 1, 1994, www.nti.org/learn/facilities/59/.

⁶ “China Academy of Launch Vehicle Technology – CALT 1st Academy,” <https://www.globalsecurity.org/wmd/world/china/calt.htm>.

⁷ Articles involving hyper-coauthorship (that list 100 or more coauthors) were excluded. Many articles also list more than one ‘seven sons’ schools, so the totals in this table exceed the total of unique articles.

Changchun University of Science and Technology	127
Shenyang Ligong University	53

The data in the above tables are admittedly a crude measure.⁸ The statistics provide no indication of the nature or frequency of the US collaborations, which are often informal and sometimes unbeknownst to their federal sponsors or even the US employers. Investigating these collaborations for approximately 27,000 articles is a daunting task. Additionally, as discussed in the knowledge gaps section of this testimony, this data significantly underrepresents the number of collaborations posing national security risks: there are many defense and state key laboratories, Chinese Academy of Sciences institutes, subdivisions of civilian universities, and research institutes subordinate to state-owned enterprises that also conduct defense research but have not been compiled in this dataset.

Nevertheless, this cursory survey of US research collaboration with high-risk entities demonstrates academia's widespread disregard for national security concerns, despite the increased scrutiny the US government has placed on these PRC institutions and its outreach efforts to academia. Also note that many of the publications in this data involve other country participation - especially NATO and Five Eyes allies. In 2023, I published a large study that cataloged and assessed German research collaboration with China that also illustrated extensive partnerships with these same PRC entities listed in Tables 1 through 5.

Academia has argued that per NSDD-189, most "fundamental research" should remain unrestricted and any additional rules federal agencies place on international collaborations in fundamental research domains would stifle innovation and cause more harm than it seeks to address. Fundamental research includes both basic and applied research that is published. *But who decides if/when research that is more applied in nature crosses into areas that pose sufficient risk to warrant some form of restriction?* This appears to be arbitrary and largely at the discretion of the individual researcher. Some applied research, especially Department of Defense (DoD)-funded projects that can be sensitive, require significantly more administrative oversight (and restrictions) on who is authorized to conduct the research, who has access to the data and research, dissemination rules on publications (e.g., controlled unclassified information designations), etc.

The incentive is to avoid these issues by publishing openly and, thus, by default, designating the research as fundamental. I lack the technical expertise to make such determinations, but some published research funded by DoD involves very specific applications and raises questions on whether it makes sense to publish that research openly. A recent report by the House Select Committee on China provided examples of research disciplines involving US collaborations with China that appear highly applied and intended for the US military. After all, DoD-funded research is intended to produce breakthroughs for war-fighting capabilities. The report noted:

⁸ This data excludes Chinese-language publications appearing in domestic PRC sources and probably understate the actual number of coauthored publications.

“These studies found that the relevant collaborations covered a wide range of sensitive technologies crucial to national security, including cryptography, eavesdropping, hyperspectral imaging, lithium-ion batteries, aerodynamic angles of attack, electronic warfare, cyber-attack detection, high-density explosives, high entropy alloys, radar target detection, quadcopters, artificial intelligence, quantum technology, multi-target tracking, missile impact penetration, and surveillance technologies.”⁹

Should all of those articles have been published openly? Should any PRC institution be allowed to materially support or partner with the US in these research areas?

PRC’s exploitation of US federally funded research also goes far beyond just DoD-funded research projects. Entities such as the Department of Energy also fund research in nuclear, weapons and energy development that are dual-use technologies. The same is true for NSF, which funds research on radar, underwater acoustics, artificial intelligence, and many other areas with obvious dual-use applications. Even NIH funding is at risk. My research on US and German collaborations with China revealed multiple instances where scientists developing advanced hearing aids using signal and speech processing techniques funded by NIH had dual appointments and/or work with a PLA Navy underwater warfare research division of Northwestern Polytechnical University and a defense laboratory on radar signal processing at Xidian University (which is co-supervised by China’s largest defense electronics and radar systems developer).

Does NIH have the ability or mandate to evaluate potential national security risks associated with every grant it awards involving health or medical research? Should they? Does the DoD have jurisdiction over NIH grant award decisions or monitor this type of activity? Should they?

Patents: Directing or Diverting US Innovation for China’s Benefit

Another way to observe how China exploits our research ecosystem to gain knowledge, experience, and technology that can be commercialized and weaponized in China is by surveying patent filings, specifically patents filed in China and/or that have PRC organizations as the patent assignee or co-assignee. **The apparent blind spots on the scale and scope of this phenomenon also mean we have little insight into how and why some of the patents are filed in China by US academics.** One US university compliance official told me that he knows of some faculty members who have only filed patents in China their entire academic careers at that US university - they have never filed patents in the US. Additionally, government investigations of PRC talent programs (discussed in a later section) have uncovered contracts mandating that all intellectual property generated from research by program selectees will be exclusively owned by China. Filing patents with PRC assignees may meet this requirement.

Comprehensive analyses and assessments of patents exceed the scope of this testimony and my area of expertise. I merely provide a sampling of patent records that sufficiently

⁹ “CCP on the Quad: How American Taxpayers and Universities Fund the CCP’s Advanced Military and Technological Research,” House Select Committee on the CCP, Sep. 2024.

raise serious concerns and policy questions and, once again, suggest negligence or indifference by US universities.

To survey a sampling of data, I compiled patent filing metadata records using the *Dimensions* tool courtesy of Digital Science, where a listed co-inventor has/had an association with select US universities. I chose some of the most research-intensive universities based on the assumption that there would be more patent data available and that some of the patents could have resulted from federally funded research. Using usaspending.gov, I compiled the top 10 recipients of federal grants (excluding contracts) reported for Fiscal Year 2024. The universities and the total amounts of grants received are:

1. University of California, San Francisco (\$964.8M)
2. University of Washington (\$929.2M)
3. Johns Hopkins University (\$893.9M)
4. Columbia University (\$839.1M)
5. University of Wisconsin (\$810.4M)
6. University of Pennsylvania (\$803.4M)
7. Stanford University (\$771.5M)
8. Washington University in St. Louis (\$766.3M)
9. University of Pittsburgh (\$744.2M)
10. Yale University (\$731.4M)

I limited patent records to those filed within the past 5 years (2019-present) that have the following criteria:

- List a co-inventor who had a recent affiliation with one of the 10 US universities listed above.¹⁰
- Name at least one China-based organization assigned to the patent (assignee) **that the US government has determined poses a national security risk**. These include entities on the BIS Entity List, DoD-designated military-affiliated organizations (as stipulated in Sections 1286 and 1260H of the NDAA), or entities sanctioned by the Treasury Department's Office of Foreign Assets Control (OFAC).
- Patents records that appear current and valid (based on the *Dimensions* data); i.e., patents that have a legal status of being pending, granted, or active. Patents marked as abandoned, ceased, expired, or withdrawn were removed.¹¹
- The number of co-inventors in these tables is broken down by researchers who appear to maintain a current affiliation with the US university and those who had some affiliation with the US university in the past five years.

This data is a cursory survey, and there are limitations that almost certainly result in an underrepresentation of the actual number of patents filed. For instance, only PRC entities on *current* US government entity lists were used; there are other PRC research-performing organizations that support defense research that warrant inclusion on US government lists.

¹⁰ Dimensions relies on publication, grant, and clinical trial information to assign a co-inventor's affiliation. A lack of records and publishing timelines (delays) may not accurately reflect an individual's most current affiliation.

¹¹ A small percentage of the patent records lack information on legal status (marked N/A); I chose to include those records.

Additionally, I cannot characterize the nature of each of the co-inventors' previous and current affiliations/employment due to scoping limitations. There are many co-inventors in this data that no longer have an affiliation with the US university in question; some of these individuals were probably visiting scholars and postdoctoral researchers who did not have full-time or permanent employment status with the US institution. More in-depth research is needed to determine the nature of the US affiliations or whether any of the co-inventors were recipients of federal research grants.¹²

Table 6: Patents Dated 2019-2025 Listing PRC Assignee on US Restricted Lists

US University	Number of (co-)Inventors Recently Associated with US University	Number of (co-)Inventors Currently Affiliated with US University	Number of Patents with (co-)Inventor Currently Affiliated with US University	Total Patents with PRC Assignees on Restricted Lists
University of California, San Francisco	41	5	13	199
University of Washington (includes Applied Physics Laboratory)	66	3	4	338
Johns Hopkins University (includes Applied Physics Laboratory)	110	9	26	350
Columbia University	63	14	92	441
University of Wisconsin - Madison	66	4	23	395
University of Pennsylvania	65	10	21	273
Stanford University	113	17	31	388
Washington University in St. Louis	38	14	34	307
University of Pittsburgh	63	7	18	271
Yale University	82	6	31	383
Totals	707	89	293	3,345

¹² In a few observed cases, the patent filing actually credits US federal funding support, but that is rare.

Despite these scoping limitations, this data covering the past 5 years is alarming: **it shows that 89 researchers who appear to be currently affiliated with these 10 universities have filed 293 patents with a PRC assignee organization the US government has placed sanctioned or restrictions on; a total of 3,345 patents filed with high-risk PRC assignees list a co-inventor who had a recent affiliation with these US universities.** We do not know how pervasive this is across the research community. Technical analyses of these patent records would help determine the nature of the proposed technology and provide insights into specific research areas China seeks to turn into practical applications.

A simple scan of patent records can sometimes be revealing without relying on technical analysis. Patents listing two co-inventors associated with Johns Hopkins University (one of whom claimed an affiliation with the university as recently as June 2024; the other appears to have held a visiting scholar position and left in 2023), are quite concerning: the filing dates appear to overlap with the co-inventors' association with Johns Hopkins and the titles suggest military applications. The assignee of the first patent listed below is a university extensively involved in PLA Navy and Air Force research; the second university is principally engaged in microelectronics, radar systems, and other technical infrastructure for the PLA and China's largest defense electronics firm.

Patent CN-111190430-B: "Unmanned aerial vehicle suspension load control method using tether rotor coordination," assignee: Northwestern Polytechnical University

Patent CN-113111786-B: "Underwater target identification method based on small sample training diagram convolutional network," assignee: Xidian University

For individuals who lack policy expertise on patents (including me), this data and its implications raise numerous questions, such as:

- How and why did a US researcher file a Chinese patent, i.e., what motivations, incentives, or taskings by PRC entities were involved that may indicate malign PRC influence?
- What are appropriate policy measures individual research institutions, federal funding agencies, and foreign policy elements of the government should take when US academics file a patent where the only assignee is a PRC institution? Would policies differ depending on the PRC entity involved, e.g., if the patent assignees are on US restricted lists?
- To what extent are university administrators and government agencies aware of this activity taking place? If the universities are aware, are there formal licensing or revenue sharing agreements or contracts in place, especially if a patent has both a US and PRC co-assignee? If so, would such arrangements create compliance issues with federal funding agencies or export controls (when the patent assignee is on the BIS Entity List)?
- What monitoring and oversight mechanisms are in place, if any, to identify, assess, and mitigate national and economic security when patents are filed in China and/or with China-based (co-)assignees?

Ethical Risks in PRC Research Collaborations

The previous section sampled *some* US-China research collaborations that pose very high national security risks yet receive little regulatory oversight. Academia's indifference to such

concerns is not limited to national (and economic) security concerns that run counter to the national interests of the US. This section demonstrates the *ongoing indifference or lack of awareness by academia of the ethical risks of research collaborations with China*. I am referring to collaborations that involve research disciplines that are intended for or can be diverted to mass surveillance technologies or involve partnerships with PRC research institutions that support the CCP's public security apparatus that engages in human rights abuses. I exclude from this discussion ethical concerns regarding how the research is conducted, particularly as it relates to human subjects due to my lack of knowledge in that area.

A study I published with the Hoover Institution examined the Chinese Academy of Sciences Institute of Automation (CASIA), one of China's premier AI, computer vision, and neuroscience research institutes. CASIA enjoys global collaboration with academia and industry, including major technology firms like Google, Dell, and Intel. Yet CASIA is extensively involved in developing and commercializing mass surveillance technologies, including facial, iris, and gait recognition, and video surveillance. CASIA owns commercial spinoffs that have developed these surveillance technologies for PRC public security organs, including for use in the Xinjiang region used to oppress and detain Muslim minority populations.¹³

I compiled data on US collaborations involving US-based coauthors alongside CASIA researchers published from 2019 to January 2025 and found 676 unique articles. US collaborations with CASIA appear to continue unabated, suggesting academia is not concerned with the ethical or reputational risks of working with CASIA.

CASIA is just one organization in China that extensively supports the party-state's surveillance apparatus and corresponding human rights abuses. To survey a larger set of ethically troubling research collaborations, I compiled bibliographic metadata on scientific publications whose abstracts contained one or more of the following keywords that have obvious surveillance applications:

- biometrics
- facial identification
- facial recognition
- iris recognition
- gait recognition
- pose estimation
- person tracking
- person re-identification
- video surveillance
- scene understanding

¹³ See Stoff, Tiffert, "Eyes Wide Open: Ethical Risks to Research Collaboration with China," *Hoover Institution*, December 2021, https://www.hoover.org/sites/default/files/research/docs/stoff-tiffert_eyeswideopen_web_revised.pdf.

- emotion recognition
- expression recognition

Researchers from the US and other nations that collaborate with China on topics related to these areas may be focused on innocuous, commercial applications. However, when PRC institutions partner in these research disciplines, we must assume they may be seeking mass surveillance applications that can benefit the PRC's public security apparatus or, in some cases, may be subordinate to or a supplier of PRC public security organs. Table 7 shows the results of collected publication metadata that have abstracts involving one of the keywords listed above. The table shows the number of articles naming a coauthor from China and a coauthor from another nation ranked by the total number of articles.

US-based coauthors are the largest collaborators with China in these surveillance-related disciplines, but US dominance may also be a function of its size as the world's largest or 2nd largest producer of scientific publications annually. Regardless, *the data here is a small sampling* of articles that are easy to recognize as raising ethical concerns. More scholarship is needed that builds comprehensive keyword ontologies associated with research disciplines with potential surveillance use, the PRC research institutions involved, and the foreign collaborators.

Table 7: Top 10 Countries Coauthoring Articles on Surveillance Research with PRC Institutions (articles published 2020- Jan. 2025)

Country	Number of Articles
USA	1,472
Australia	633
Singapore	539
Japan	438
Canada	419
Germany	317
India	220
UK	219
Italy	161
France	157

Collaborations in these ethically troubling areas that can enable or enhance China's surveillance and oppression of its citizens *and* the export of related technologies to authoritarian regimes around the world raise important questions for governments and policymakers:

- Given a lack of regulatory oversight regarding fundamental research, what policy changes (if any) should be made to disincentivize universities and firms from engaging in ethically troubling collaborations with China? For instance, is it OK for researchers at IBM to collaborate with researchers from the *People's Daily* - China's official newspaper of the CCP that is a propaganda tool for both domestic and foreign messaging purposes?¹⁴
- What if the US-based researchers who work with the PRC on surveillance disciplines are recipients of federal

funding, such as NSF, DoD, NIH, and the Office of the Director of National Intelligence? **All of these agencies were** acknowledged as funders in some of the publications that formed the basis of Table 7.

- Do program managers at federal agencies have a set of ethical guidelines when awarding grants on this type of research separate from ethical review boards, which only address

¹⁴ See <https://dl.acm.org/doi/10.1145/3474085.3478574>.

research that directly involves human subjects?

- Who is monitoring formal and informal research partnerships and exchanges between US institutions and PRC entities in areas that have clear surveillance applications and that can enable human rights abuses?¹⁵ Do universities have a set of ethical guidelines or values that discourage or prohibit collaborations with authoritarian nations in these research areas?

Malign Influence from PRC Funding and Resources

Up to this point, I have focused on problematic research collaborations that can lead to exploitation by China, including diverting or applying such research for military or surveillance use. The massive amount of concerning collaborations, as reflected in publications and patent records should be framed within the context of malign PRC influence because China's partnerships with the US often serve a much different and dangerous purpose than the intentions, norms, and values of the US partners. That also holds true with China's collaborations with allied nations. *This section describes a more explicitly malign influence activity that has profound corrupting and corrosive effects, some of which have not been discussed in public given the associated compliance and reputational risks: PRC funding and resources provided to US research institutions.*

In oversimplified terms, US universities run like businesses in that their primary objective is to bring in revenue. This is partly due to the fact the federal and state governments do not provide enough funding to universities for them to operate; academia must rely on a diverse set of revenue sources. This creates inherent vulnerabilities that foreign entities - especially the PRC - can exploit for their benefit and create incentives that are often not aligned with US national interests. An uncomfortable truth is that US universities have a history of accepting gifts, contracts, and grants from nearly any entity in the world without discrimination (or due diligence) on those funders.

Section 117 of the Higher Education Act requires institutions that receive any form of federal funding to disclose foreign sources of funding to the US Department of Education on a biannual basis.¹⁶ However, both Congressional and Department of Education investigations found widespread non-compliance with this law. An early 2019 report by the US Senate Permanent Subcommittee on Investigations found that foreign funding in America's higher education system is "effectively a black hole," with up to 70% of colleges and universities failing to disclose mandatory foreign funding.¹⁷ A report issued in late 2020 by the Department of Education revealed more than \$6.5 billion in previously undisclosed foreign

¹⁵ PRC institutions extensively involved in surveillance research and support or are part of public security organs is a knowledge gap – arguably another failure by the IC to systematically identify such entities and share that information with the public. BIS does add companies to the Entity List that demonstrate they contract with or supply PRC public security organs, but few, if any, efforts have been made that look at PRC academic institutions.

¹⁶ See 20 U.S. Code § 1011f.

¹⁷ "China's Impact on the U.S. Education System," U.S. Senate Permanent Subcommittee on Investigations (Feb. 2019), www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/PSI%20Report%20China's%20Impact%20on%20the%20US%20Education%20System.pdf.

funding (from China, Russia, Iran, and Qatar) and found that “historically, fewer than 300 of the approximately 6,000 U.S. institutions self-report foreign money each year.”¹⁸

What follows is a discussion of specific cases and observations from my experience supporting PRC influence investigations when I was in the government. **What is usually missing from public discourse related to these issues are the secondary effects and implications that undermine integrity, trust, fairness, and equity in our institutions of higher education.** US academic institutions are naturally not monolithic, and I do not suggest every institution operates in the same unscrupulous ways described here. There are some universities, for example, with robust research security and compliance programs that seek to serve as responsible stewards of taxpayer money.

Case Examples

The first set of cases relates to PRC firms sponsoring research in non-transparent ways that undermine research security and integrity and have led to non-compliance on federal research grants. Like other threats and challenges, this phenomenon is not unique to the US. Canadian media revealed multiple agreements between Canadian universities and PRC technology giant Huawei that totaled more than \$50 million, and those agreements required that all intellectual property rights born out of the collaboration belong solely to Huawei.¹⁹ Huawei has built R&D centers around the world and sponsors research in academia. However, the conglomerate has come under scrutiny from Five Eyes nations and key EU allies due to its reported ties to PRC military, intelligence, and public security organs. Additionally, the US government placed Huawei on the BIS Entity List that restricts exports, and the company has been accused by the Department of Justice of committing intellectual property theft, obstruction of justice, and fraud related to the evasion of US sanctions against Iran.

In essence, the Canadian universities performed contracted research for China. Besides having no real benefit to the universities or Canada other than a temporary source of revenue, it is even more problematic when some of that research and facilities are supported by federal funding. What about in the US? What do Huawei and other PRC sponsorship agreements with US research institutions look like? Given the widespread disclosure failures of foreign funding by US institutions, this is largely unknown. Some US media sources have exposed a few examples where PRC surveillance technology firms like SenseTime and Megvii have partnered with US universities. There are two recent cases that also shed some light on this.

US Research Institutions and Huawei

In a case uncovered by *Bloomberg*, Huawei provided funding to Optica Foundation, a US-based non-profit organization. Optica then awarded research grants to academics while not

¹⁸ “Institutional Compliance with Section 117 of the Higher Education Act of 1965,” U.S. Department of Education, Office of the General Counsel (Oct. 2020), www.ed.gov/sites/ed/files/policy/highered/leg/institutional-compliance-section-117.pdf.

¹⁹ Robert Fife and Steven Chase, “Huawei Still Filing Patents Tied to Work with Canadian Universities after Ottawa’s Restrictions,” *Globe and Mail*, November 9, 2023, www.theglobeandmail.com/politics/article-huawei-canadian-universities-patents/#:~:text=In%20the%20past%20two%20years,University%20of%20British%20Columbia%20and.

disclosing that Huawei was the source of funding. Optica Foundation sponsored a research competition that awards a total of \$1 million per year to winners to conduct research on a specific area. According to the *Bloomberg* report, universities, applicants, and even one of the competition's judges were unaware that Huawei was the source of funding. *Bloomberg* reviewed a "non-public document" that appears to be the contract between Huawei and Optica Foundation. The document included a provision stating that the existence of the agreement and all details contained therein shall be considered confidential information.²⁰ Thus, Huawei used a third-party professional society (Optica Foundation) as its proxy to hold multi-year contests to grant researchers funding on specific projects in a secretive way. This was almost certainly intended to avoid scrutiny by not having to provide funding to universities directly.

In July of 2024, the University of Maryland (UMD) entered into a settlement agreement with the Department of Justice that also involved funding from Huawei. The United States alleged that UMD "knowingly failed to disclose current and pending foreign funding that three UMD researchers had sought and received, in five research grant proposals submitted to the NSF and the Army. Specifically, the United States alleged that UMD failed to disclose to NSF gift funding from Huawei Technologies Co., Ltd. to a PI²¹ for research in 'high energy density FeF3 conversion cathode materials and Li metal anodes.'" The government also alleged that UMD failed to disclose to the NSF and Army funding provided to two other PIs from Taobao (China) Software Co, a subsidiary of Alibaba titled, "Large-Scale Behavior Learning for Dense Crowds" and "Cyber-Manufacturing of Customized Apparel."²² Note that the first project clearly has mass surveillance applications.

This UMD case appears to be consistent with other investigations I supported when I was in the government, where PRC entities basically contract with US academia to conduct research on specific projects led by specific PIs. Yet the recipient US institutions claim those sources of funding are unrestricted gifts, meaning that they are donations to US institutions that are free to use the funds in any way they see fit. Academia has argued that it does not have to report that as current or pending support on federal grant applications because those "gifts" do not relate specifically to the research grants.

In at least some observed cases, these gifts are really contracts or grants in disguise; they "recommend" specific US faculty work on specific research projects at the PRC's behest. PRC institutions are directing US institutions to perform research by specific personnel. Naturally, US universities will abide by the wishes of the PRC "donors" to avoid jeopardizing those revenue streams.

A secondary compliance concern may also be taking place. Unrestricted gifts may not have to be counted when universities calculate the administrative/overhead costs associated with the federal grants they receive. Universities charge a portion of each federal grant to

²⁰ Kate O'Keeffe, "Huawei Secretly Backs US Research, Awarding Millions in Prizes," *Bloomberg*, May 2, 2024, <https://www.bloomberg.com/news/articles/2024-05-02/huawei-secretly-backs-us-based-research-with-millions-in-prizes-through-dc-group?srnd=undefined>.

²¹ PI refers to principal investigator, the researcher(s) that leads a project funded by federal research grants.

²² <https://www.justice.gov/usao-md/pr/university-maryland-college-park-agrees-pay-500000-resolve-allegations-it-failed>

cover the administrative costs of executing the research. The implication is that if a university receives a federal grant to perform research that is materially similar to the research sponsored by a “gift,” then in essence, the university may be overcharging the US government on its administrative costs. That may be considered fraud - a violation of the False Claims Act.

One observed way PRC entities funnel money into US academic institutions is through US academics that hold concurrent positions at PRC universities (such as visiting professors), often recruited through one of the hundreds of PRC state-sponsored talent programs described in the next section of this testimony. The US academics holding these PRC positions then serve as a proxy for PRC institutions, brokering gifts, contracts, grants, and cooperative agreements with the US institutions where they are employed.

Stanford's Settlement of False Claims

In another settlement, the United States alleged that on 16 grant proposals submitted to the Army, Navy, NASA, and NSF, Stanford University “knowingly failed to disclose current and pending foreign funding that 11 Stanford PIs and co-PIs had received or expected to receive in direct support of their research.” The United States further alleged that Stanford “knowingly failed to disclose to the Army, Air Force, and NSF that a Stanford professor received research funding in connection with his employment at China’s Fudan University and from a foreign government’s national science foundation” (refers to the PRC).²³ The US alleges that these disclosure failures violate the False Claims Act.

Federal agencies require grant applicants to disclose all current and pending support received by the institution and the PIs and co-PIs on the grant proposals. Current and pending support is defined as all resources from any source - including foreign governments- that are made available to researchers in support of their research endeavors.

Interagency efforts to pursue civil remedies should be lauded as they are a more effective and fairer approach to mitigating these concerns compared to pursuing criminal prosecutions. In the Stanford case, the settlement agreement required Stanford to pay \$1.9 million to resolve allegations of False Claims Act violations. However, a cursory survey of the grants listed in the settlement agreement that were (allegedly) fraudulent totaled over \$14 million. The False Claims Act allows for damages of *up to triple* the amount of the federal grants, plus a flat penalty per occurrence of each false claim submission. Consequently, these small settlement agreements are unlikely to create any real deterrent for universities to change their behavior. The penalties have been a modest cost of doing business, and universities can maintain the status quo of receiving an unknown amount of funding and support from PRC entities and, in essence, “double-dip” by taking federal grant dollars to do the same research.

There are secondary and corrosive effects that are not being discussed. When universities or their faculty fail to disclose these outside sources of funding (regardless of whether they are

²³ <https://www.justice.gov/opa/pr/stanford-university-agrees-pay-19-million-resolve-allegations-it-failed-disclose-foreign>

characterized as gifts, grants, or contracts), that affects federal grant award decisions. This violates the principles of integrity and transparency that universities espouse as core values. Federal research grants are highly competitive as only a fraction of the total submissions are usually awarded. There are finite taxpayer dollars; if universities are, in essence, double-dipping by taking both PRC and US government funding, this means that other universities – especially those with fewer resources like smaller institutions and Historically Black Colleges and Universities – are denied those federal research dollars that could have otherwise been awarded.

This creates a vicious cycle of inequity in the system: schools that are being honest but denied federal funding means they have smaller budgets and fewer resources to hire PhD students, attract top talent, etc., which then makes them less competitive on future grant proposals. This also translates to fewer opportunities domestically.

How pervasive is this problem, and how much PRC funding and resources are being funneled to (and hidden by) US universities? *In addition to the corrosive effects described above, a lack of awareness of this problem means it is impossible to determine the level of influence the PRC is exerting over the conduct of US research that may be overwhelmingly (or unilaterally) benefitting China to our detriment.*

II. Understanding PRC Talent Programs Beyond Research Security: Integrity and Malign Influence Matters

PRC state-sponsored talent recruitment programs number in the hundreds and play an instrumental role in China's economic development and military modernization efforts. They

“Overseas returnee scientists are the talent power behind knowledge and technology transfers and have gradually become China's new force in academic development and S&T innovation, promoters of high and new technology applications, and frontrunners in promoting China's innovative development.” (A “responsible person” who is a member of the CCP Central Committee Talent Work Coordination Small Group, the key policy body on talent recruitment programs in a Xinhua article - 海归梦, 中国梦,” November 7, 2017, www.xinhuanet.com//mrdx/2017-11/07/c_136733044.htm)

are statutorily designed to transfer technology and knowhow from overseas through any and all means at the PRC party-state's disposal. There has been considerable US government scrutiny on these programs - often described in various policies as “malign foreign talent recruitment programs” to differentiate them from scholarships and talent programs of other nations. Federal agencies have exerted considerable efforts to explain to academia and the private sector the national and economic security risks these programs pose. Primers on the PRC's talent programs have been published elsewhere and thus are not included in this testimony. The focus of this testimony is the features and activities of these programs that intersect with malign influence and research integrity concerns.

Some institutions in the US and EU have downplayed the risks and threats posed by China's state-sponsored talent programs and view the US government's concerns as overblown. Some arguments center around the mirror imaging of our systems with the PRC - that most countries have talent promotion programs of various kinds, such as government-sponsored fellowships and scholarships that send citizens abroad to gain knowledge and experience and attract talent from the international community to further domestic endeavors. At a basic level, the goals of many government-led human capital investments are indeed similar to those of the PRC: to help advance science and technology to bolster a country's economic development.

However, this argument overlooks key differences between programs in allied democracies and those in the PRC concerning the methods, requirements, supporting infrastructures, and how PRC talent programs integrate into and support a state-directed strategy to acquire technology and knowhow from around the world. The arguments downplaying the risks also overlook China's system of governance and *rule-by-law* approaches. This is particularly relevant as PRC talent program selectees, regardless of nationality, are under contract with the PRC government: they are tasked and funded by party-state organs and subject to PRC law.

Another structural difference between China's talent programs and other nations relates to scale and scope. PRC programs, in addition to their sheer size and number, have supporting infrastructures and ecosystems, such as:

- Dedicated research funding lines
- Venture capital investment structures
- Global recruitment and candidate evaluation networks
- Government-run databases of overseas experts used for targeting
- Co-opted domestic and overseas support organizations, many of which are part of China's United Front influence apparatus

There are other elements of PRC talent programs that encourage insidious behaviors, many of which should be viewed as malign foreign influence. Selectees of these programs can have corrupting effects on our academic institutions, exploit individual and institutional vulnerabilities through money and resources; undermine values of academic research, such as integrity and transparency; create conflicts of interests or conflicts of commitment; and incentivize intellectual dishonesty and academic fraud. Depending on the academic institution, administrators have been unaware, turn a blind eye to (or admit they do not want to know), or are complicit; all of which demonstrate the corrosive nature of China's influence.

Talent program selectees have requirements that undermine our values system beyond national security threats, including:

- Attribute awards, patents, and projects to PRC entities, even if the research used US funding
- Recruit and train specific individuals: coordinate with the PRC government to hire/sponsor PRC nationals to come to the US and circumvent merit-based hiring processes; recruit others

into talent plans

- Fail to inform US employers of their commitments in the PRC; redact information on faculty pages and CVs related to talent program appointments or use innocuous or alternative titles such as “honorary” or “visiting professor,” “advisor,” or “academic committee member” when actually serving in a talent program-sponsored position
- Replicate or transfer US-funded research to the PRC or request duplicative grant funding from PRC and US sources on the same research
- Retain positions in the US and concurrently advise or lead research efforts in the PRC; direct, divert, or influence R&D for China’s benefit, such as running parallel labs in the PRC
- Facilitate the brokering of gifts, grants, cooperative agreements, joint PhD training programs, or other contracts between US and PRC institutions

Case Example 1: Corrupting NOAA Research and Operations

An investigation I supported when I was in the government illustrates the various ways talent programs can involve malign influence and create corrosive effects on our research. This case is also important because it shows federal research facilities are also affected, not just universities. The US government pursued a criminal investigation in part because the subject was a federal employee - a climate scientist at the National Oceanic & Atmospheric Administration (NOAA). The scientist was recruited through two nationally run PRC talent programs to take a part-time position at a PRC university while retaining his full-time employment with NOAA. The criminal elements of the case centered around prohibitions against government employees taking outside, concurrent employment (especially with a foreign government).

However, the requirements of the PRC talent program appointments were the most concerning with respect to malign influence, some of which are not illicit. For instance, the NOAA researcher’s contracts with the PRC government obligated him to:

- Sponsor specific PRC national researchers to work in his NOAA lab *as directed by the PRC*. The subject failed to evaluate multiple candidates for these positions as required; he bypassed merit-based hiring processes and systematically denied US applicants.
- Work on research projects at NOAA as determined by his PRC sponsors; collaborate on PRC government-funded research projects with specific scientists using NOAA facilities.
- Travel to and work in China for two full months per year, which exceeded federal annual leave accruals. This meant the researcher was certifying time and attendance reports that he was working at NOAA and lying to his supervisors about his China-based commitments.
- Publish research that credited the PRC institution as the primary affiliation, even if the research was principally (or entirely) conducted at NOAA facilities. A literature review showed that the scientist published some papers listing his NOAA affiliation and other papers listing him as exclusively affiliated with a PRC institution during his tenure at NOAA.

- “Serve an important bridging role” by facilitating academic exchanges and formal partnership agreements between NOAA and the PRC institutions at which the subject held concurrent positions, thus representing both parties during negotiations and violating US government ethics rules.

Clearly, most of these activities undermine the basic values of research integrity. Another highly disturbing element was discovered when federal investigators interviewed at least one of the PRC national researchers the subject hired. At least one of these PRC nationals stated that the NOAA researcher pressured him or her to work exceedingly long hours in the lab: they had to sleep and work in the lab on the weekends and do the lion's share of the research and drafting of publications that the NOAA researcher would claim as his own. The NOAA researcher exploited a power dynamic where the PRC nationals needed positive performance reviews for their careers back in China; if they complained to NOAA management, the NOAA researcher would take retaliatory measures against those PRC nationals.

Other investigations I supported involving talent program selectees at US academic institutions resulted in similar findings. Many part-time talent program selectees (those that retain their US positions) are tasked by their PRC employers or party-state organs to hire or sponsor specific PRC national PhD students and postdocs to work at US institutions to gain access to and support the research done there. Many of these talent program selectees were PIs on federal grants. Investigations also discovered that some of these US faculty members who were talent program selectees coordinated with the China Scholarship Council to provide funding for the PRC graduate students and postdocs' study in the US. A few of these cases *also found abuse and exploitation of the PRC national students, unbeknownst to the US institution.*

Academia has argued that recruiting individuals from personal and professional networks is a normal practice. However, it is important to differentiate this from the activity I am describing, which involves direct taskings - often under contractual obligations - by the PRC government to sponsor specific individuals and ignore standard, merit-based hiring practices. At a minimum, this undermines the integrity of our open system; it is more damaging when individuals carry out research projects conducted by specific individuals at the behest of the PRC party-state in critical technology fields.

We do not know the scale or scope of this phenomenon. Nevertheless, when we examined numerous talent program selectees in prominent positions at US universities who are PIs on federal research grants, it was not uncommon to find that the majority of their graduate student body are PRC nationals, typically from select (and often high-risk) PRC institutions with which these faculty members have formal relationships via PRC talent recruitment programs. This calls into question oft-used arguments that there is insufficient US and other allied nation STEM talent available to fill graduate degree and postdoctoral programs at US universities or laboratories and that we are critically dependent on PRC talent. When some US faculty are financially obligated by their overseas (PRC institution) sponsors to appoint personnel, domestic STEM talent is simply overlooked or a lower priority. This practice has

been observed to take place for two decades, making this “dependency” on PRC talent highly concerning and a self-fulfilling prophecy.

Case Example 2: Former UCLA Professor

While in government, I also supported efforts that identified then-UCLA Professor Songchun ZHU as part of a larger survey of US-China collaboration on AI and computer vision disciplines. We looked closely at Professor ZHU because of his extensive partnerships with PRC entities that represent national security, integrity, and grant compliance concerns. ZHU had worked on DoD and NSF-funded research totaling over \$30 million while simultaneously having significant commitments with PRC organizations, including via China’s flagship Thousand Talents Program. In addition to suspected disclosure failures of current and pending support on grant applications, ZHU appeared to divert federally funded research to private companies he founded and ran (based in China and the US). In other words, he was commercializing federally funded research for personal (and arguably China’s) benefit.

ZHU also partnered with and had talent program appointments at the Beijing Institute of Technology (BIT) and other PRC research institutions heavily involved in defense R&D. BIT is a “Seven Sons of National Defense” university involved in weapons and defense program research. Even if he was not violating US law, his PRC collaborations and appointments represented serious national security and conflicts of interest and commitment concerns.

In 2019, I provided extensive information on ZHU to DoD law enforcement and intelligence components as well as senior DoD leadership to demonstrate the nature of these threats. No actions appear to have been taken, at least while I was in government. ZHU recently relocated to China and now leads a massive AI research effort there, as reported by *Newsweek*.²⁴ The decades of knowledge and research projects he conducted for DoD are presumably furthering China’s AI efforts, including in applied domains through his companies. Many of the PhDs and postdocs he sponsored and trained at UCLA subsequently worked at his companies. Some of those individuals are now in China, leading major AI, computer vision, and related research that have mass surveillance and military applications. The US taxpayer, especially through DoD funding, trained multiple generations of PRC scientists in critical technology fields who are now at institutions supporting PRC military and public security organs.

Case Example 3: Influence Over NSF Grant Award Processes

NSF relies heavily on Intergovernmental Personnel Act (IPA) assignees, typically academics in scientific and engineering fields, to take temporary assignments to serve as program directors and grant managers. These individuals oversee NSF grant application submissions, evaluation and award processes, and related grant program management functions. IPAs

²⁴ Didi Kirsten Tatlow, “Exclusive: U.S. Gave \$30 Million to Top Chinese Scientist Leading China’s AI ‘Race,’” *Newsweek*, November 1, 2023, <https://www.newsweek.com/us-gave-30-million-top-chinese-scientist-leading-chinas-ai-race-1837772>.

are not federal employees but are subject to provisions of law governing the ethics and conduct of federal employees.²⁵

While in government, as part of my interagency efforts to assess risks and threats associated with PRC talent programs, my colleagues and I discovered a troubling issue: some talent program selectees who were faculty at US universities took IPA assignments at NSF to serve as grant managers. We compiled data on the NSF grants that those individuals were responsible for (which included making grant award decisions) and found that some of the grants were awarded to researchers who were also selectees of the same PRC talent programs. Additionally, several of the awardees (PIs) of these NSF grants who were recruited by PRC talent programs subsequently became IPAs at NSF themselves and then awarded grants to *other* PIs who were PRC talent program selectees and to former IPAs. One of the talent programs that all of the identified IPAs were affiliated with was established around the year 2000; the first IPA position of one of these talent program selectees began around 2005.

Consequently, we observed a vector of influence where individuals simultaneously under contract with the PRC government were making NSF grant award decisions for two decades. The number of individuals we found implicated in this scheme was small. However, due to limited resources, our focus was only on one NSF division. We do not know whether this type of activity has taken place at other NSF divisions. Additionally, *I am not aware of any efforts since that discovery to identify similar activity at other federal agencies that employ academics (typically as IPAs) as part of their grant management structure.* This is just one method of the PRC's malign influence over federally funded research.²⁶ Based on my experience, it appears that the scale and scope of PRC influence activities over federal grant award decisions are largely unknown.

Exploitation of Other Federal Funding Sources

Hijacking NSF CAREER Awards

The PRC government clearly prioritizes the recruitment of individuals who received or supported federal research grants. PIs on DoD grants are obviously of very high interest for China to recruit, but talent programs have also recruited many recipients of other agency funding. A troubling trend is China's recruitment of academics who recently completed or are nearing completion of their term as an NSF CAREER awardee. "The Faculty Early Career Development (CAREER) Program is a Foundation-wide activity that offers NSF's most prestigious awards in support of early-career faculty who have the potential to serve as academic role models in research and education and to lead advances in the mission of

²⁵ <https://new.nsf.gov/careers/rotator-programs/intergovernmental-personnel-act-ipa-assignments>

²⁶ NIH has discovered and disclosed publicly a situation where the confidential peer review process of grant applications was compromised by some PRC-affiliated actors. This represents a similar type of influence, but it is not known how pervasive this activity is.

their department or organization. Activities pursued by early-career faculty should build a firm foundation for a lifetime of leadership in integrating education and research.”²⁷

In other words, NSF's CAREER program is an investment in future science and engineering leaders, where they are given a prestigious line of funding to kickstart their promising and lengthy careers in the US. PRC talent programs have been observed to recruit some of these individuals to work in China, *thus benefitting from (and exploiting) the significant investments made by the US government and further eroding our STEM talent pipeline.*

Exploiting SBIR Programs

PRC talent programs have also targeted recipients of DoD-funded Small Business Innovation Research (SBIR) programs. A small (government-use only) study I supported while I served in government found that China has benefited from DoD's SBIR programs and revealed vulnerabilities to potential future DoD supply chains. Not all of China's exploitation of SBIR contracts involved the use of talent programs, but in many observed cases, key personnel (founders, chief scientists or engineers, CEOs, etc) of startups receiving SBIR funds were recruited through a talent program or received PRC state-backed start-up capital.

- Some key employees of US firms receiving SBIR contracts were recruited via a PRC talent program and relocated to China, but they continued research collaboration with officers of the US companies where they were previously employed.
- US firms established PRC-based subsidiaries, receiving funding through entrepreneurial contests that function similarly to talent programs. In some cases, the firms subsequently dissolved their US operations.
- In one observed case, a recipient of multiple DoD SBIR contracts established another firm in China based on the same technologies, developing combat vehicles in partnership with the state-owned defense conglomerate China North Industries Group Corporation (NORINCO).

Technology Acquisition Networks

There are organizations in the US (and around the developed world) that demonstrably partner with, take tasking and direction from, or serve as a proxy to CCP organs and the PRC diplomatic missions. In the US, these entities are typically non-profit professional associations that claim to be NGOs. While many of these organizations engage in professional networking and entrepreneurial activities that are not illicit in nature, they have supported PRC state-directed activities, *including substantial involvement with PRC talent programs.* Details on specific organizations and case examples cannot be provided in this testimony, as the preparation and dissemination of the information is considered government use only.²⁸ However, I can offer some key findings:

²⁷ <https://new.nsf.gov/funding/opportunities/career-faculty-early-career-development-program>

²⁸ Note however, that some organizations, particularly those principally engaged in technology transfer activities, are described in the edited volume, *China's Quest for Foreign Technology: Beyond Espionage*, Hannas and Tatlow eds., Routledge, 2021)

- Key leadership of some of these non-profit organizations are federal government researchers at NOAA, NASA, the Department of Energy, etc. Yet these organizations routinely meet with and receive taskings from CCP organs and PRC diplomats (especially in the S&T and Education sections of the PRC Embassy and its consulates).
- Some organizations organize, host, and serve as judges for talent programs and start-up contest activities operated or sponsored by the PRC government. The leadership of these organizations runs venture capital and angel investment structures in the US.
- Some of these organizations also routinely meet with (and likely take instruction from) CCP United Front organs and PRC diplomatic mission personnel in the US.

One organization that is publicly known to have overseas operations and closely partner with (i.e., task) diaspora organizations is the Western Returned Scholars Association (欧美同学会 - 留学人员联谊会, WRSA). WRSA is a CCP organ directly subordinate to the United Front Work Department, described as “a mass organization led by the CCP, composed mainly of returned overseas scholars, [serving as] a bridge and link between the Party and the vast majority of overseas scholars, helping the Party and state do overseas scholar work well, [and acting as] a home for the vast majority of overseas scholars.”²⁹ WRSA has been observed to partner extensively with some of the non-profit organizations I described above.

III. China’s Role in Undermining Research Integrity and US Inaction

Research security, research integrity, and malign influence are often intertwined, especially when dealing with the PRC. Governments and research institutions in liberal democracies espouse and stress the importance of values such as academic freedom, transparency, integrity, and reciprocity concerning the conduct of research and international research collaboration. The G7 Security and Integrity of the Global Research Ecosystem Working Group defined a set of “Common Values of Research Integrity,” which included transparency concerning disclosures of researcher affiliations, conflicts of interests, and sources of funding, and honesty regarding proposing, undertaking, reviewing, and communicating research.³⁰ However, **PRC party-state organs and research institutions routinely violate these norms and values that are critical to beneficial research collaboration and trust in science.**

Research organizations in liberal democracies rarely take transparency and integrity factors into account when engaging with the PRC. When allied nations, especially G7 countries, espouse “common values” of transparency, integrity, and reciprocity but impose no cost to Chinese researchers and institutions that violate these values, they signal to PRC entities that the status quo is acceptable. *The US government has taken no observable policy*

²⁹ The original source is no longer available online; an archived version can be found here: https://web.archive.org/web/20190802122850/http://www.xinhuanet.com/politics/2016-08/03/c_1119332162.htm.
³⁰ “G7 Best Practices for Secure & Open Research,” Security and Integrity of the Global Research Ecosystem (SIGRE) Working Group, May 2023.

measures to mitigate PRC practices that undermine research integrity, and these practices are often intended to influence the international research community.

My non-profit's latest publication catalogs numerous ways China has violated these norms and the implications of academia and government inaction.³¹ My colleagues and I examine China's lack of transparency, which often is intentional to mislead the international community, as well as types of fraud in published scientific literature. Academic fraud in publications is a global phenomenon and by no means unique to China. However, China is by far the world's largest producer of fraudulent publications, which has a profound impact on trust in the global research enterprise.

As Glenn Tiffert writes in the foreword of my publication, "The party has grown less tolerant of open inquiry, debate, and free flows of information...It controls knowledge at home with the most sophisticated regime of propaganda, surveillance, and censorship on the planet, and abroad by cutting off foreign access to PRC scientific, judicial, and economic information, and to the academic theses and journals that nourish independent judgments. It is securitizing data and has recriminalized forms of collection and analysis that are routine in open societies."

The issues Tiffert describes should warrant rigorous policy responses from both governments and academia, yet the silence is deafening. The incentives and interests of individuals and their research institutions probably drive inaction. Research institutions routinely make exceptions to their espoused values and core principles of academic research when dealing with China. Examples of China's practices include:

- Adding foreign coauthors who had no material involvement in the research to bolster the reputations of the other coauthors and institutions
- Listing a PRC institution as the only affiliation when most or all of the research occurred outside of China
- Creating fictitious coauthors with stated affiliations to reputable foreign institutions
- Producing fake papers in paper mills; intentionally using falsified or manipulated images or data
- Denying access to PRC websites of institutions from outside China or removal of content
- Obfuscating or misrepresenting PRC entity names, missions, projects or funding sources, parent organizations, etc.; discrepancies between English and Chinese information that strongly suggest intentional deception
- Failing to disclose financial conflicts of interest or outside involvement (as a shareholder, company board member, founder or chief scientist/engineer of commercial firms) on any CV, faculty page, or (co)authored publication

³¹ Stoff, McIntosh, and Lee, "Transparency and Integrity Risks in China's Research Ecosystem: A Primer and Call to Action," *Center for Research Security & Integrity*, 2024.

For-profit academic journal publishing firms have few incentives to self-police and systematically identify and retract fraudulent papers. The journal industry earns money from paper mills, and retracting papers is a burdensome process. It is assumed that a substantial number of fraudulent publications remain undetected (not retracted) and continue to be cited. Outside of publishers, monitoring to detect fraudulent research and publications is largely limited to voluntary and often self-funded efforts by a disturbingly small international community of individuals, many of whom contribute to PubPeer.com and Retraction Watch.

PRC entities that lack transparency or integrity undermine trust, complicate due diligence and risk assessment efforts, and create an unsecured research environment. Fraudulent publications can be harmful when scientists, clinicians, or even policymakers make decisions based on fake or manipulated science.

Case Example: ‘Comfort Letters’

I advised on other investigations when I was in government – some of which involved instances where a PRC institution provided a letter to NIH that contained demonstrably false information to mislead a grant compliance investigation. The cases involved PIs at US research institutions under investigation for allegations of failure to disclose outside appointments or affiliations with a PRC institution. In a few cases I supported, the PIs were assigned to work 12 months per year on a federal grant; thus, undisclosed appointments may represent conflicts of commitment and violate NIH grant terms.

NIH posted an illustrative case on its website. A Senior Deputy Director of Research at a PRC university provided an official “comfort letter” (as NIH describes it) to the scientist and the US institution, stating that the scientist under investigation was merely honorably invited as a guest professor, did not hold any official faculty position, and had no formal contract through a PRC state-run talent program; the individual just had a “gentlemen’s agreement” with the PRC entity. However, the employing US institution reported to NIH that it discovered documents indicating the researcher did, in fact, receive a talent program position and had a formal agreement with the foreign university to work as a “distinguished part-time professor” for three years.³²

This “comfort letter” provided to the US institution was intended to deny and deceive NIH, and having it sent by a senior leader from a PRC institution indicates institutional-level dishonesty. NIH has received an undisclosed number of “comfort letters” from PRC research institutions. Thus, it is not known how many PRC institutions were involved or how pervasive this dishonesty has been. Regardless, this problem calls into question whether US researchers should receive federal research funding on projects that involve collaborations with PRC entities that have sent false and misleading information to federal agencies. I am not aware of any policy at federal funding agencies that addresses this issue. *Consequently, neither the US employing institution nor the federal agencies are imposing any costs to this*

³² Posted case studies are available on the Policy and Compliance page of the NIH website: <https://grants.nih.gov/policy/foreign-interference/case-studies>.

behavior, despite it fundamentally violating academia's core principles and "common values."

Reciprocity

Issues of reciprocity are also not receiving scrutiny, and government and academia's inaction raises important policy questions. Here are two examples:

US-China research collaboration also takes place at federal agencies via national laboratories, federal facilities, and other government-run infrastructures that carry out their own research. Some of these agencies oversee collaborative projects with the PRC through formal agreements. When I was in the government, officials at several federal agencies discussed the fact that sometimes, the partnering PRC institutions failed to abide by the terms of a research agreement, such as failing to provide the promised resources, data, or personnel. In some cases, an agency decided to cease or not renew such a partnership. In other cases, collaborations continued despite the PRC not meeting its obligations - perhaps in the interest of furthering diplomacy or gaining cooperation from the PRC in other areas.

Similarly, PRC data/information laws can restrict or prohibit PRC research institutions from sharing the underlying data on published research with the rest of the world. When findings are published based on data, but the PRC prohibits its release, then the research community cannot validate or replicate the research results or methods elsewhere. I have seen very little investigation or scholarship on when and how often this occurs, whether federal research funding was involved, or whether the US government has developed any policy response.

IV. Brief Discussion of IC, FBI Failures, Knowledge Gaps

The introduction section listed some of the shortcomings that hamper the Intelligence Community (IC) and law enforcement (particularly the FBI) efforts to protect our research and innovation ecosystem. This issue is too complex to examine comprehensively here, nor is this the focus of the hearing. *However, there are areas worth noting that relate to the government's (in)ability to identify and disrupt the PRC's malign foreign influence activities in the US.*

There has been an observable decline in researching, investigating, and mitigating the threats posed by PRC talent programs due to unforced errors by the FBI and the Justice Department. Execution of the "China Initiative" led to a reckless focus on attempting to arrest and prosecute selectees of PRC talent programs in academia. The US government had to learn a painful lesson: criminal statutes often do not apply to fundamental research activities in academia. The failures resulted in a backlash within academia and the Asian-American community in particular, who justifiably felt unfairly targeted and, in some cases, severely disrupted the careers of academics.

When I was in government, there were a few individuals (including me) who unsuccessfully tried to convince agencies to focus their resources on leveraging civil, administrative, and other tools and tactics to mitigate the threats rather than pursue prosecutions. Offices of

Inspectors General began pursuing civil investigations and remedies, but those efforts were nascent, and a lack of sufficient expertise limited their scope.

To be fair, the FBI *successfully prosecuted* several important cases involving economic espionage and IP theft, some of which involved talent programs. I would be remiss not to underscore the fact that PRC talent program selectees can be tasked or incentivized to steal materials, data, and IP, and provide false statements or claims to the federal government that can be illicit in nature. Much of these activities are not limited to targeting or exploiting academia; the private sector has been affected, but there is even less public knowledge about the scale and scope of that malign activity because capital markets (and shareholders) do not look kindly on public companies that are victims of technology theft. Nevertheless, a consequence of the FBI's failures is that there has been little space for nuanced discussions of the insidious nature of many of China's talent programs, including aspects that go beyond the national and economic security concerns discussed in this testimony.

Another key impediment of the IC is the paradox of mission priorities. The early stages of our research and innovation ecosystem have, by design, the least amount of regulatory oversight. This lack of oversight has meant a lack of resources or mission priority within the national security community to protect these areas. That has left our ecosystem largely unprotected from China's predations, which, unsurprisingly, China has increasingly exploited.

Additionally, the IC's continued descope and devaluation of open-source intelligence (OSINT) and diminishing use and reliance on publicly available data sources and information further degrades the government's ability to protect academia and private sector entities. This has led to persistent and yawning knowledge gaps in the PRC's research ecosystem that pose strategic risks and is one cause of the dearth of subject matter expertise on China's technology transfer apparatus.

The IC cannot be trusted to collect and provide OSINT, especially data collection and analysis that can support institutions outside of the government. This is not as controversial as it seems; numerous studies by think tanks, policy papers, etc., have advocated radical changes to the process and prioritization of OSINT activities of the US government. Yet variations of these recommendations started in earnest after 9/11, and the same conversations have continued with no meaningful change in structure, mission priorities, or budget.

Part of this problem is structural and bureaucratic: SIGINT, HUMINT, and other technical collection means are sophisticated and expensive, and the IC places a much higher premium on clandestinely acquired information than publicly available information. OSINT elements of the IC, particularly the CIA, have been gradually descope and underfunded. Leadership considers the OSINT profession second-class, where expertise is devalued, and career progressions of officers are limited. I do not foresee any real change to this situation.

As an example, when I was in government, I oversaw several pilot open-source projects that built databases and related repositories of information on China's research ecosystem, especially elements of China's defense research and industrial base. As the information was derived from public sources, the intent was to make the information available broadly to federal agencies, scientific funding agencies, the State Department, the Department of Homeland Security (DHS), and export and financial regulatory bodies. All of these projects were ultimately discontinued, and the information has largely remained in silos within the IC. These efforts were not a mission priority.

I also provided information to counterintelligence elements on organizations that have demonstrable ties and partnerships with CCP organs, the PRC diplomatic establishment, and PRC state-backed investment structures. Little action was taken (at least while I was in government). My interactions with FBI and DoD counterintelligence elements showed that those offices prioritized criminal investigations over leveraging operational approaches to deny and disrupt PRC state-directed technology transfer and related influence activities.

Persistent Knowledge Gaps

Research institutions and federal agencies will continue to be ineffective at identifying and mitigating risks associated with research partnerships with PRC entities as long as yawning knowledge gaps persist. Some examples follow.

China's Defense and Surveillance Research and Industrial Bases

Areas where there is little information nor any systematic efforts to collect such information include:

- A knowledge base (such as lists and descriptions) of all subsidiaries of PRC state-owned defense conglomerates that house research institutes and conduct defense R&D or sponsor academic research
- Identification and assessment of national and provincial-level key laboratories' and Chinese Academy of Sciences institutes' level of involvement in defense (or classified) research and their partnerships with the PLA, defense industries, and civilian universities principally engaged in defense research
- A knowledge base on PRC universities that have substantial ownership stakes in companies supplying the PLA, defense conglomerates, or public security organs
- A knowledge base on PRC universities that conduct research with mass surveillance applications or other disciplines enabling human rights abuses and/or receive funding from PRC public security organs
- Identification of PRC research centers of excellence that are domestic leaders in fields the US government has designated as critical and emerging technologies, such as AI, quantum computing, certain biotech fields, and semiconductors

University-Industry Integration

There is also insufficient knowledge on how PRC research institutions integrate with or support domestic industries. Integration occurs in a myriad of ways, yet there is little scholarship on the subject. I am also not aware of any efforts to systematically examine these topics by federal agencies. Examples of topics include (but not limited to):

- Some universities are co-managed by or have partnership agreements with state-owned enterprises, where students and faculty directly support commercialization efforts and train future technicians for those enterprises. Beijing University of Chemical Technology (BUCT), for example, is a top chemical engineering school that is partially overseen by Sinopec (one of China's state-owned oil giants). BUCT conducts research on behalf of this large state-owned firm and the two entities share some personnel.
- Some professors at research institutions concurrently serve as scientists, engineers, and/or founders of technology firms while enjoying extensive international R&D collaborations in their academic capacity, raising the risk of unknown technology or knowledge transfers that solely benefit PRC enterprises.
- Some PRC universities and Chinese Academy of Sciences entities have majority or substantial ownership stakes in dozens, if not hundreds of commercial enterprises. This is often opaque to the international community. A report by US-based non-profit C4ADS examined corporate records of the Harbin Institute of Technology and found that the school has direct or indirect ownership interests in approximately 1,000 China-based companies and owns a 50 percent or greater ownership interest in about 50 entities.³³
- PRC commercial sector interests and ties to academia may influence the research or content of publications; how and to what extent does the PRC use academic research as an instrument of its industrial policy.

V. Brief Overview of Allied Nations and Innovation Security

Despite my frequent criticisms of US government in this testimony, I would be remiss not to recognize that many federal agencies have led the international community in raising awareness of the risks and threats the PRC poses to our collective research ecosystems and have made great efforts in promoting research security. Our key allies and partners are becoming increasingly aware and concerned with research security and integrity concerns thanks in no small part to the US government. That said, government efforts to date have been mostly limited to raising awareness of current problems and challenges, and it has been less effective when it comes to mitigating and reducing the threats, especially within fundamental research domains that are subject to less oversight in liberal democracies.

Key allies have investigated and discovered similar threats posed by China to those encountered by the US. An infamous example is the case of a Canadian scientist who was

³³ Jason Arterburn, "The Party-State in China's Military-Industrial Complex: Implications for U.S. National Security," Testimony to the U.S. - China Economic Security Review Commission, March 19, 2021, https://www.uscc.gov/sites/default/files/2021-03/Jason_Arterburn_Testimony.pdf.

fired from her position at a level-four virology lab due to allegations of misconduct and national security concerns associated with her collaborations with PRC institutions, including military medical entities.³⁴ Another case involved a Beihang University student funded by the China Scholarship Council to study in France, who repeatedly accessed laboratory computers using other students' credentials, a clear violation of the IT policy. The student also stayed overnight in the laboratories and facilitated unauthorized access for a compatriot who had no official business in the lab. This individual reportedly used laboratory equipment, potentially for unknown purposes.³⁵

Many EU governments appear to take a “country agnostic” approach to research security to avoid the appearance of having discriminatory policies. It is true that many policy mechanisms to mitigate risks can be framed more broadly – that our standards, values, and restrictions are not country-specific, especially concerning authoritarian and adversarial regimes. Nevertheless, the uncomfortable reality is that probably over 90% of all the threats and challenges to our collective research ecosystem come from the PRC. Within the EU, for example, nearly all partnerships and research collaborations with Russia have stopped due to its invasion of Ukraine. And several EU nations have discussed the need to build better competencies on China (i.e., subject matter expertise).

Having 27 individual member states in the EU creates inconsistencies in how research security is approached across the region, with some states having more robust measures in place while others may have a higher tolerance for risk and/or lack of capabilities to address their vulnerabilities. An absence of centralized oversight in the EU also allows China to engage in partnerships or research activities with less oversight or scrutiny.

My direct engagements with foreign partners have been limited to a few EU nations; as such, I cannot provide a comprehensive view of the current research security landscape across all of our key allies and partners. Instead, I offer some observations based on personal interactions with government organs and research institution leaders.

I have engaged the most with Germany and The Netherlands, and their governments have been active in raising awareness and addressing issues on research security, including providing concrete guidelines and recommendations for academia. There are more open discussions (and recognition) of the concerns related to China's unilateral knowledge transfers, malign influence - especially when it impinges on academic freedom, and diversion of research that enables human rights abuses or supports the PLA.

The Netherlands appears to have the most well-developed set of policies and programs on research security among EU member states, based on my observations. The Dutch government has created a “national contact point” - an office where research institutions can request due diligence and risk assessment support (especially on China) regarding any

³⁴ See for example: <https://www.cbc.ca/news/canada/manitoba/scientists-fired-from-winnipeg-lab-rightly-under-probe-1.7150560> and <https://www.cbc.ca/news/politics/winnipeg-lab-firing-documents-released-china-1.7128865>.

³⁵ <https://www.mediapart.fr/journal/france/140222/une-etudiante-chinoise-espionnait-des-laboratoires-francais> Clément Le Foll et Matthieu Suc, Feb. 14, 2022.

partnerships they are pursuing. However, there is still a need to build Chinese language and subject matter expertise even in the Dutch government, to be more effective in providing support. That said, partly due to the small number of universities in the Netherlands, there appears to be a close-knit research security and compliance community that is exploring ways to share information among and between them and is well aware of the PRC's malign influence risks. The Dutch also appear to be a valued and contributing partner to the international innovation security community.

Germany is much more active compared to just a few years ago in raising awareness and deliberating on policies on research security. Yet, many challenges remain. Generally speaking, Germany, like the US, is mentally and politically ill-equipped to deal with the malign influence and threats posed by China, partly because there is a general lack of understanding of the *systemic, networked nature of China's strategy*. Problem areas are viewed as "individual cases" within academia. (I have heard similar arguments in the US.)

German sinologists Alicia Hennig and Andreas Fulda recently opined that German policies still leave critical "blind spots" that need addressing. For instance, they argued that "reciprocity is not achievable with regard to Chinese laws" and that the German side "still assumes that access to and use of information from joint research projects can be secured through framework conditions to its own advantage."³⁶

While there is an observable decline in Sino-German institutional cooperation, PRC national students continue to flow into Germany in very large numbers. Many of them start at undergraduate and Master's levels, which limits federal government oversight. However, this serves as a gateway for individuals to stay in Germany and further advance to PhD, postdoctoral, and higher levels within academia, many of whom focus exclusively on critical technologies. However, commercial spinoffs and other entrepreneurial endeavors of individuals earning PhDs and postdoc positions are rarely founded by PRC nationals. Many return to China after gaining the critical knowhow to launch enterprises there.

Another challenge Germans have articulated relates to a lack of reciprocity, which is also not unique to the German experience. Thousands of PRC students go to Germany every year, but almost no Germans go to China because critical technology disciplines are taught exclusively in Chinese. Worse still, PRC nationals have unfettered access to German equipment, data, algorithms, and supercomputers; however, in China, the PRC government considers these strategic assets to be mostly closed to foreigners.

German professors are civil servants with employment protections and few incentives or pressures to commercialize their research. The PRC takes largely an opposite approach. Academic freedoms and the system Germans operate in create no incentives to cut ties with China, especially when allied nations share the same view or the US chooses not to apply

³⁶ Hennig and Fulda, "Blind spots in scientific cooperation with China," *Table.Media*, January 14, 2025, <https://table.media/en/china/opinion/blind-spots-in-scientific-cooperation-with-china/>

pressure on restricting PRC collaborations. Unfortunately, the current political climate in the US is also driving many German scientists to prefer working with the PRC rather than the US.

Another common theme I have encountered is that EU-based professors become increasingly reliant on PRC young talent if they cannot find sufficient STEM talent from the US and other friendly nations. Germany, and especially smaller nations like The Netherlands and Denmark, have world-class scientific institutions but rely heavily on large international student bodies. This creates more student mobility opportunities (especially at graduate degrees) for the US and would be welcomed by our EU partners.

VI. Recommendations for Policy Makers

The challenges we face in mitigating and disrupting the PRC's malign influence and exploitation of our research ecosystem are daunting. However, the following recommendations, if implemented, would go a long way in closing regulatory and knowledge gaps, re-aligning incentives and grant compliance of academia, limiting the PRC's near unfettered access to federally funded research, and leading the international community to ensure the integrity of research is not an abstract construct – that real costs are imposed on the PRC when it violates commonly accepted norms and values.

Many of these recommendations go beyond the remit of the Senate Foreign Relations Committee. The challenges and threats posed by the PRC transcend the missions of individual agencies and legislative committees. We must find the courage to aggressively break down silos and partisan barriers and build new paradigms for cooperation among and between federal agencies and legislative committees. Otherwise, our fragmented and piecemeal measures will not be able to stand up to China's whole-of-society approaches.

It is worth noting that my recommendations *exclude* much-needed efforts to bolster domestic STEM research and education to reduce dependencies on adversarial nations like China. Research security is pointless if we lose the technology at the point it is ready to leave the lab because we lack the ability to manufacture it competitively or an engineering workforce and risk capital to support pilot projects and work through scaling challenges. We have allowed many of the links in the chain to atrophy by outsourcing so much of our inputs, including human capital. However, as we bolster domestic investments in R&D, we need a corresponding increase in protection and research security policies and measures, especially given the current abysmal state of neglect by both the government and academia.

My recommendations include a) bolstering research grant compliance and enforcement by federal agencies; b) enhancing disclosure laws and policies; c) improving the State Department's visa vetting processes; and d) through State Department leadership and interagency cooperation, build programs, infrastructures, and policies exclusively dedicated to research security and integrity. These recommendations are not presented in any hierarchical order in terms of priority; I start with listing recommendations that involve the State Department and are most relevant to this Committee's oversight functions.

1. Enact new legislation similar to the requirements of Section 117 of the Higher Education Act for the purposes of reporting information to the State Department.

Similar to the current requirements of reporting foreign contracts, gifts, and grants to the US Department of Education, institutions of higher education and other research organizations (such as hospitals and medical research facilities) should be required to report to the State Department all MOUs, cooperative agreements, joint degree programs, joint venture educational institutes based overseas, and other related agreements with foreign countries of concern. "Foreign countries of concern" are determined by Congress and should be consistent with other legislation (which usually names Russia, Iran, the PRC, and Cuba). Information should include details on the foreign entities (and their subdivisions) that are

counterparties to the agreements; the periods of performance or length of the agreements; and a listing of responsible persons overseeing the execution of the agreements. State Department should create a dedicated repository of this information that is made available to all law enforcement agencies (FBI and Offices of Inspectors Generals), DHS, the Intelligence Community, and federal agencies that provide research funding to higher education institutions.

Additionally, US institutions that sponsor foreign nationals for PhD, postdoctoral, or visiting researcher positions should be required to include in their invitation letters that accompany the visa applications of the foreign nationals indications that the invitations are part of a formal MOU, cooperative agreement, joint training program, etc.

2. Amend the Foreign Agent Registration Act (FARA) to expand the definition of an “agent of a foreign principal.”

The Department of Justice has recently sought public comment on proposing some amendments to FARA regarding the scope of certain exemptions, to update and add various definitions, and other implementing regulations. However, a cursory examination of these proposed changes suggests key elements of the rules would remain intact: the scope of FARA is largely limited to political activities - purely commercial and academic pursuits are exempt from current FARA regulations. FARA needs to evolve with the changing geopolitical landscape, particularly concerning PRC influence activities in the US.

All selectees of any PRC state-sponsored talent program, which includes programs run by national, provincial, and municipal level party-state organs, should be required to register as agents of a foreign principal. This holds true even if the selectees are academics. All PRC talent program selectees are under contract with / employed by the PRC government, subject to PRC laws, and receive tasking and direction from the PRC government to pursue the PRC’s strategic objectives, which invariably harm US interests. While the act of being a selectee of a PRC talent program is in itself not illegal, individual selectees should be registered foreign agents. Failure to register under FARA should result in criminal penalties or, in the case of foreign nationals, visa revocation and deportation.

Similarly, entities incorporated in the US, including non-profit organizations and associations, that execute the duties of or receive taskings or monetary support from PRC party-state organs (including but not limited to PRC diplomatic missions) should also be required to register as foreign agents. China has exploited loopholes in FARA by deploying proxy organizations that, while claiming to focus only on academic, educational, or commercial pursuits, are, in fact, executing state-directed and sponsored technology acquisition efforts, political lobbying and policy advisory activities, and support functions to PRC public security organs including serving as overseas “police stations.”

3. Improve the State Department’s visa information storage systems and sharing processes and bolster enforcement of current visa restrictions.

Consular offices face huge resource constraints in terms of due diligence and vetting of PRC nationals on visa applications, given the sheer numbers involved. Improvements in IT

systems and processes regarding visa applications would allow for more interagency support - especially from DHS - that assists with the Security Advisory Opinions (SAO) process for visas that require security background checks on applicants. PhD students, postdocs, and other visiting scholar applications (usually on F and J visas) include supplemental information such as an applicant's CV or resume, invitation letters from the sponsoring US institution, and other supporting documents. It is my understanding that most of these supporting documents are manually scanned as images, losing the original file formats. Consequently, none of this supporting documentation attached to visa records can be indexed, searched, or retrieved by DHS or other national security agencies for risk identification or inputs into the SAO or related processes.

Congress should appropriate funding for the State Department to modernize its information system storage and retrieval infrastructure that allows for the retention of original file formats (such as requiring electronic submissions) and a process for indexing all information contained in visa applications that can be searched and retrieved through automated processes and incorporated into other internal government databases as appropriate.

The State Department should also expand the scope of organizations that would be included in visa denials in accordance with Presidential Proclamation 10043 of May 29, 2020. This proclamation is intended to deny certain student visas (limited to PhD students and postdoctoral applicants) if they are affiliated with any entity that supports the PRC's "military-civil fusion strategy"; that strategy is defined as any actions "to acquire and divert foreign technologies, specifically critical and emerging technologies, to incorporate into and advance the PRC's military capabilities."³⁷ Knowledge gaps and varied interpretations of what entities constitute support to "military-civil fusion" have limited the effectiveness and enforcement of this rule.

In the short term, an easy (partial) solution to this problem is to simply include in this proclamation all PRC entities already listed on the various US government restricted lists. Specifically, visa denials should be applied to any individual employed at or affiliated with entities on the BIS Entity List, Treasury's OFAC sanctions list, and organizations listed based on the provisions of Sections 1286 and 1260H of the National Defense Authorization Act. These lists are by no means exhaustive and need to be updated. Nevertheless, the US government has already determined that entities on these various lists pose significant national security threats and should thus form the basis for visa denials outlined in Proclamation 10043.

4. **Create a new office in the State Department focused exclusively on technology transfer, research security, and research integrity issues.** This office, nominally referred to here as the Office of Innovation Security and Integrity (OISI), should develop new policies and programs and coordinate/expand on existing department-wide efforts.

³⁷ <https://www.federalregister.gov/documents/2020/06/04/2020-12217/suspension-of-entry-as-nonimmigrants-of-certain-students-and-researchers-from-the-peoples-republic>

Regional bureaus, public diplomacy elements, and the Bureau of International Security and Nonproliferation currently oversee programs and international engagements that deal with research security and technology transfer to some extent. However, these efforts sometimes lack coordinated, strategic approaches. Additionally, while the State Department has received additional funding for and actively engages in efforts to counter China's predations in a variety of areas, there are still important elements that are missing or receive inadequate attention. In addition to policy development and coordination functions, this new Office of Innovation Security and Integrity³⁸ should carry out (but not be limited to) the following lines of effort:

A. Lead the international community in greatly expanding knowledge and capacity building (i.e., competency) on China relating to research and innovation security.

This testimony has highlighted many knowledge gaps on PRC entities and programs of concern regarding its research ecosystem and technology transfer apparatus, which I attribute mostly to failures of the IC. State Department should take a leading role in this space, leveraging a variety of public and private sector institutions and the international community in the following areas.

*Oversee the creation of a new version of the existing "China Defense Universities Tracker" created by the Australian Strategic Policy Institute (ASPI).*³⁹ This is a web-based repository of information on select PRC universities and research institutions tied to China's military and defense industries and has been wildly successful in terms of its use around the world. Most research security and compliance offices have leveraged this tool extensively to support due diligence efforts. However, this web-based tool is quite limited in scope. For example, it has not been updated, nor does it comprehensively identify all research institutions or their subdivisions and laboratories that conduct defense research. The tracker also has minimal information on research institutes attached to defense state-owned enterprises and contains no information on Chinese Academy of Sciences institutes (which number over 100).

State Department's new "OISI" should replicate this effort but significantly broaden the scope to address the ASPI tracker's limitations. The tool should also be made available publicly to assist the international research community. OISI should also replicate this model to build other information repositories, as discussed below.

Sponsor and/or oversee additional international research collaboration projects that expand the knowledge base on China's research ecosystem, starting with projects on identifying PRC centers of excellence in critical technology R&D areas.

OISI should develop programs that build a consortium of organizations that collaborate on research projects. Projects should tap into experts and organizations across the EU, Five Eyes, and Indo-Pacific allies, such as experts in particular critical technology disciplines in academia, think tank scholars and NGOs, private sector data providers, and other

³⁸ This is simply a placeholder name; Congress and State Department can create an appropriate title for this office.

³⁹ <https://unitracker.aspi.org.au/>

organizations that can collaborate on methods and studies that identify PRC technology centers of R&D excellence: the research institutions, labs, key personnel, supporting infrastructures, etc. These efforts can include technical evaluations of research conducted in the PRC, surveys of domestic and international partnerships, examination of funding sources, etc. A key element to these projects would also include risk assessments: whether and to what extent these PRC centers of excellence support PRC defense and public security/surveillance apparatuses. Allied nation governments and research institutions could use this information to inform policies and processes on innovation security and integrity. Having these reports and studies produced by a consortium of international partners also enhances trust and buy-in from our allies around the world.

B. *Sponsor programs, workshops, and training to the international community that focus specifically on building competency and subject matter expertise on China concerning innovation security and integrity.*

Much of the engagements and workshops the State Department has facilitated or sponsored to date have focused on raising awareness of the threats and concerns posed by the PRC's malign influence activities and building institutional processes and procedures for improved governance. These efforts are important, and the State Department has arguably made a significant impact within the international community. However, there are insufficient efforts to build workshops that substantively focus at granular levels on the PRC's policies, programs, tactics and methods, and infrastructures that support malign influence and technology transfer activities. Notwithstanding a training course my organization has developed, I am not aware of any (other) training or workshops on how to conduct due diligence and risk assessments on China that specifically relate to research security and integrity.

C. *The Office of Innovation Security and Integrity should create a subdivision that oversees policies, research programs, and international engagements specifically dedicated to research integrity.*

There is no US government office or organization that has a dedicated mission of understanding and setting or advising policies on *research integrity*. Research integrity is loosely defined in various policies and is co-mingled conceptually with research security without addressing it specifically. Additionally, transparency and integrity risks are rarely assessed and factored into deliberations over whether to pursue or continue research partnerships with PRC institutions across liberal democracies. There are knowledge and policy gaps that must be addressed. For example, the US government (and the international community) has imposed no costs on the PRC when it corrupts the integrity and trust of our research ecosystems. Upholding our common values requires robust and collaborative efforts from governments and research institutions in liberal democracies, and a new OISI should take a leading role in these issues with support from other federal agencies.

A sampling of mission areas the integrity office within OISI includes:

- 1) **With possible support from other federal agencies (such as NIH and NSF), OISI should work with the international community to fund research programs and build infrastructure for tracking, monitoring, and identifying fraudulent publications.**

Current efforts to uncover fraudulent science are largely limited to individuals around the world who monitor scientific publications on a volunteer (unpaid) basis. While academic journal publishers are making some efforts to identify fraudulent activity on their own, as for-profit organizations, there are few incentives (or requirements) for the publishing industry to self-police. OISI and other agencies should sponsor research projects that build tools and methodologies such as the emerging field of “forensic scientometrics” for identifying fake science, citation cartels, authorship-for-sale and other schemes, as well as efforts to force retractions of fraudulent publications. OISI should also lead programs to track and report on frequent offenders: individuals, institutions, and publishers found to produce multiple fraudulent publications.

- 2) **OISI's integrity division should oversee multiple projects and information-sharing mechanisms that track other integrity and reciprocity failures.**

OISI should oversee programs and sponsor projects to identify and build formal data-sharing mechanisms and platforms that track a variety of other research integrity issues that heretofore have been largely ignored. Other federal agencies and governments of allied nations should also contribute related information, which would be limited to PRC entities and behaviors of concern to maintain the legal privacy protections of entities in liberal democracies. Examples of areas that should be tracked and shared include:

- Identifying published research where the PRC partners fail to provide underlying data due to PRC data laws. This can help inform decisions on to what extent international partners should collaborate with specific PRC institutions or on specific disciplines if there are high risks of data reciprocity failures.
- Identifying and characterizing instances of transparency failures by PRC research organizations that are intentionally designed to obfuscate their missions, research activities, etc., or mislead or misrepresent such activities.
- Descriptions from governments or research institutions of PRC entities that have acted in bad faith, such as failing to abide by the terms of cooperative agreements; or entities that have provided federal agencies “comfort letters” that are intended to deny and deceive federal regulators or research grant managers.

5. Harden the False Claims Act (FCA) to enforce public institution compliance.

Amend the FCA to include a provision that all public (state) universities or research institutions that apply for and receive federal contracts or grants waive their rights to sovereign immunity claims under the 11th Amendment of the Constitution.

One interpretation of the 11th Amendment⁴⁰ is that any state institution, *including public universities*, is immune from False Claims Act civil suits as this equates to the federal government suing a state government, thus violating a state's sovereign immunity. This hampers the ability of federal agencies to pursue false claims cases against state universities. Any public institution should be subject to the same responsibilities, standards of compliance, and fraud provisions as private entities. Waiving state sovereign immunity claims should be a condition for a public university to accept grants or contracts from the federal government.

6. Increase funding for OIG personnel and civil litigation.

Congress should appropriate funding to increase the number of Office of Inspectors General (OIG) agents, attorneys, and support personnel - as well as training to OIG elements - to more aggressively pursue False Claims Act cases. Increases in OIG resources directly result in increases in monetary recoveries by the government that far exceed the additional costs.

FCA litigation has proven to be an effective yet insufficiently pursued civil remedy to punish academic institutions for non-compliance with federal grant and contract rules and conditions. This is especially the case regarding universities' failure to disclose support from the PRC and other foreign sources. Civil false claims cases do not require proof of intent to defraud the government; grant or contract submission documents that contain misrepresentations (or fail to contain required information) are considered false claims.

To be most effective, OIGs and the Department of Justice should more aggressively exercise the law's authority that demands larger penalties (up to triple the amount subject to the false claim) when universities are found liable. This would require the government to demand higher settlement amounts out of court or a willingness to pursue a court's judgment. Enforcing higher penalties as stipulated in the FCA would be a more effective deterrent than the status quo, which to date are simply minor costs of doing business for most universities; most FCA settlements on allegations of false claims amount to a small fraction of the potential liability.

The increased allocation of resources is a budgetary gain, not a deficit because the amount of money that can be recovered through litigation of false claims cases invariably exceeds (sometimes by factors of three or higher) the cost of the increased government personnel and litigation. In essence, it is a substantial return on investment.

7. Federal funding agencies should use grant suspension and debarments more aggressively and modify grant submission certification requirements.

Federal funding agencies should institute policies that more aggressively suspend and debar federal grants to institutions that have lapses in institutional governance and grant

⁴⁰ The 11th Amendment states: "The judicial power of the United States shall not be construed to extend to any suit in law or equity, commenced or prosecuted against one of the United States by citizens of another state, or by citizens or subjects of any foreign state."

compliance. Research institutions need to bear greater costs for non-compliance with federal awards. For instance, agencies should suspend all new awards to an institution that has submitted false claims until it can demonstrably show remediation measures have been put in place.

Federal funding agencies should also require that the presidents or CFOs of each institution certify all submissions to the federal government that the information provided in grant or contract documents is complete and accurate.

8. OIGs and grant program management offices at federal agencies should create a central, government-use only repository of information on the results of investigations, such as findings of non-compliance and false claims.

The purpose of such an effort is to create a rough equivalent of vendor past performance reports accessible to all grant program managers across federal agencies. Previous judgments or settlements related to fraud or false claims by a university should then be factored into future grant award decisions. Priority should be given to universities that do not have a history of false claims or other non-compliance on competitive awards. Such a repository could also be used for active investigations so that investigators can more easily share information between agencies. Previous investigations have often shown that non-compliance with grants can involve grants from more than one agency.

9. Pass the DETERRENT Act in the Senate.

In late 2022, the House passed H.R.5933: Defending Education Transparency and Ending Rogue Regimes Engaging in Nefarious Transactions Act, or the DETERRENT Act. *The Senate should review and pass this bill largely in its current form.* This bill would go a long way in bolstering enforcement of foreign gift, contract, and grant reporting requirements of higher education institutions, especially when supplemented with the other recommendations of this testimony.

10. Require recipients of NSF CAREER awards to sign a continuing service agreement with the US government.

The PRC has benefitted from substantial NSF investments in future scientific leaders by recruiting recipients of NSF CAREER awards who relocate to China. To prevent this, NSF should create a new condition that CAREER award recipients must stay in the US and work at a research institution or in the US government for a specific length of time deemed appropriate by NSF and Congress, but should at minimum be equal to the period of performance of the award.

11. Create new legislation that expands on Sec 238 of the FY25 NDAA by placing restrictions on all federal sources of fundamental research funding if recipient institutions collaborate with select PRC entities.

Sec. 238 of the FY24 NDAA⁴¹ restricts DoD fundamental research funding to institutions if they collaborate with academic entities listed pursuant to provisions of Section 1286 of the FY19 NDAA. This is a significant and positive step in curtailing research collaborations with PRC military-affiliated research institutions. However, this rule should be applied to all federal funding, and the list of “covered entities” to which funding restrictions apply needs to be expanded to other government-restricted lists.

The current list associated with the requirements of Sec. 1286 is too narrow in scope. Similar to Recommendation 3 on visa restrictions, federal funding on fundamental research should also be denied to institutions collaborating with PRC organizations on the BIS Entity List, the OFAC sanctions list, and DoD’s 1260H list of military-affiliated companies (as some of those entities conduct and publish research).

Efforts are also needed to revise and expand on the entities on these various lists. For instance, there are dozens of officially designated “national defense key laboratories” that are excluded from these lists, and many enjoy international research collaboration. There are also “private” and state-owned enterprises that conduct and publish research with international partners that also need to be added, including firms that support PRC public security organs that engage in human rights abuses.

⁴¹ “LIMITATION ON AVAILABILITY OF FUNDS FOR FUNDAMENTAL RESEARCH COLLABORATION WITH CERTAIN ACADEMIC INSTITUTIONS”

Senator RISCH. Thank you very much.

We will now hear from Dr. Melanie Hart. She is the senior director of the Global China Hub at the Atlantic Council.

Immediately prior she served at the Department of State and played a central role on U.S. responses to Chinese economic coercion as well as strategy and international engagement on semi-conductors.

Dr. Hart, the floor is yours.

**STATEMENT OF DR. MELANIE HART, SENIOR DIRECTOR,
GLOBAL CHINA HUB, ATLANTIC COUNCIL, WASHINGTON, DC**

Dr. HART. Senator Risch, Ranking Member Shaheen, distinguished members of this committee, thank you for the opportunity to testify today.

The U.S. and China are engaged in systemic competition. It is a competition over which model prevails—the U.S. model of political and economic development or China's. If China prevails, the U.S. and the world will be less free, less prosperous, and less safe.

Beijing is deploying a range of tactics to achieve its objectives. Some constitute traditional diplomacy. Some constitute malign influence. The State Department must be empowered to fight on both fronts.

I would like to make five key points. First, showing up in the traditional diplomatic arena is foundational to America's success. Our diplomats must be resourced to show up and pull every lever to advance U.S. national interests. When they do, they win.

In 2020 China held four of the 15 leadership roles across the U.N. specialized agencies. Today, Beijing is down to just one.

The department made those positions a priority, starting with the International Telecommunication Union. The department identified and ran compelling candidates and launched a whole of department effort to rally the votes needed to win. Diplomacy works.

Second, when combating malign influence, transparency is our super power and Beijing's kryptonite. Beijing knows the China model is deeply flawed. That is why Beijing resorts to malign influence.

It relies on information control to hide the costs associated with the China option and coercion to force others to bear those costs.

Examples include engaging in widespread graft to sway foreign official decisions in Beijing's favor, filing libel suits against PRC critics to silence them, engaging in economic coercion and disinformation, and electoral interference.

Boosting transparency should always be step one when combating malign influence. These tactics are covert by design, so exposure often neutralizes them.

Third, the global information space is an active battlefield that impacts every arena of U.S.-China competition. Beijing engages in information warfare. It seeks to control information at home and abroad and use that control to advance its objectives at America's expense.

The now shuttered State Department Global Engagement Center was the primary U.S. mechanism for combating China's information warfare. GEC enabled Washington to broadcast its own mes-

sages to the global public, sharing our vision and exposing the truth about China's.

GEC was not just a government megaphone. It provided grants to third party researchers around the world, empowering an entire global army of counter malign influence warriors to combat CCP disinformation.

That is why the Chinese foreign ministry has referred to GEC as Washington's command center of perception warfare.

I urge Congress to reauthorize the Global Engagement Center. Keeping these counter influence warriors off the battlefield boosts Beijing at America's expense.

Fourth, economic coercion requires active defense. During the Biden administration, the department launched an internal unit to provide support to nations facing Chinese economic coercion.

That effort was wildly successful, so much so it neared case capacity due to the number of nations coming in for assistance.

At present, there is no single state department, FTE, or office with authorization and appropriations to counter Chinese economic coercion. I urge Congress to provide dedicated resources for this effort.

Fifth and finally, I would be remiss in my duty to this committee if I did not raise the current foreign assistance freeze, which is hobbling America's ability to compete with China in every domain.

Over \$1 billion in foreign military financing for Taiwan frozen. NDI and IRI are shutting down global operations. Human rights organizations frozen. Washington has effectively abandoned the Hong Kong pro-democracy movement.

I understand the need to maximize strategic focus and foreign aid. I applaud Secretary Rubio's steps to lift some restrictions. But this broad freeze hobbles America at a moment when we are in the battle of the century.

It is a massive gift to Beijing. The longer it goes on, the harder it will be to regain the grounds we are already losing today, tomorrow, and this week.

Thank you for the opportunity to testify today. I look forward to your questions.

[The prepared statement of Dr. Hart follows:]

Prepared Statement of Dr. Melanie Hart

Senator Risch, Ranking Member Shaheen, distinguished members of the committee, thank you for the opportunity to testify today.

The current global system is rules-based. Beijing is promoting an alternative vision in which the Chinese Communist Party (CCP) determines—at a global level, not only in China—whose interests prevail. Some of the tactics Beijing deploys to push this vision constitute legitimate diplomacy. Beijing also deploys “malign” influence tactics, which are not legitimate. Australia has defined those tactics as “foreign influence activities that are in any way covert, coercive or corrupt.”¹ Unlike legitimate diplomacy, malign influence tactics aim to subvert nation-state sovereignty, distort public information, and undermine the function of key political systems, particularly democratic systems. To prevail in the global competition with China, the United States must fight effectively on both fronts: advancing our interests and

¹Malcolm Turnbull, “Speech Introducing the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017,” December 7, 2017, <https://www.malcolmturbull.com.au/media/speech-introducing-the-national-security-legislation-amendment-espionage-an>.

maximizing our own attractive power through smart diplomacy; taking targeted action to directly counter Beijing's malign influence activities.

My testimony will cover five main points:

1. We are engaged in a global governance competition that will define which system prevails—ours, or Beijing's. Step one is showing up. We cannot vacate key diplomatic battlefields.

2. When combatting malign influence, transparency is our superpower and Beijing's kryptonite.

3. The global information space is an active battlefield that impacts every arena of U.S.-China competition. If the U.S. stands on the sidelines, we cede that field—and the upper hand in other arenas—to China.

4. The United States must directly—and robustly—counter PRC economic coercion.

5. Congress should empower the State Department for full-spectrum competition.

(1) The United States has the upper hand in global governance competition—to prevail, we must compete at full strength.

The United States and China are promoting alternative global visions. The U.S. vision is rooted in democracy. It is based on individual rights, freedoms, and a separation of powers. It is a vision in which all nations and individuals have a voice in determining their own fate. Beijing's vision is rooted in autocracy. It is a vision in which the Chinese Communist Party (CCP) decides which interests prevail. It does not support individual rights or freedoms, or any limits on what the CCP can do to pursue its own interests. It does not respect nation-state sovereignty when another nation's sovereign decision conflicts with CCP desires.

Beijing is battling to advance its global vision on two fronts: legitimate global governance competition and malign influence. The United States must fight effectively on both fronts for the U.S. model to prevail. Between these two systems, the U.S. version—the democratic version—provides better outcomes for a larger majority. In contrast, the Beijing model depends on information control to hide the costs many individuals pay as the powerful pursue their own interests. That gives the United States the upper hand in global governance competition. Step one is showing up to advocate for that vision diplomatically. When the United States does not show up—for example, when we disengage from international institutions—we cede the playing field to China despite our comparative advantages. For example:

- *Engaging diplomatically in international organizations.* Nations that provide funding to international organizations, promote their own nationals to key staff and leadership positions, push a positive agenda, and engage partners ahead of key votes to advocate for that agenda shape global rules.² Beijing is maximizing every one of these levers on issues ranging from human rights to setting global technology standards to shaping how the international community views Taiwan. If we cede that field to Beijing, every element of competition will become an uphill battle.

- *Providing commercial incentives to help companies and standards compete for global market share.* The United States and China are in a global battle to determine which companies, technologies, and standards shape global infrastructure. The Development Finance corporation (DFC), the U.S. Export-Import Bank, and the U.S. Trade and Development Agency decrease the cost of choosing to partner with U.S. companies over PRC competitors. Trade deals create a similar pull, as they lower the cost of doing business with covered partners. Beijing deploys its own banks and trade policy to lower the cost of doing business with Chinese companies and make it harder for U.S. and other foreign companies to compete.

- *Using educational diplomacy to attract top global talent.* The United States is competing with China and other nations for top global talent, particularly STEM talent. Nations with a global talent strategy and education policies (including streamlined visa programs) to attract top talent outperform others at doing so. The United States is currently lagging behind other OECD nations on this front.

When the United States competes in these arenas at full strength, we generally prevail. For example, the United Nations International Telecom Union (ITU) sets global telecom standards. PRC national (and former PRC telecom ministry official) ZHAO Houlin served as ITU Secretary-General from 2015 to 2022, giving Beijing

² As one State Department official plainly stated: “[O]ur influence at the U.N. is greatest when we pay our bills in full and on time.” U.S. Assistant Secretary of State for International Organization Affairs, Michele J. Sison, Testimony to the House Foreign Affairs Committee, “Renewed American Engagement with International Organizations: Goals, Priorities, and Successes,” February 15, 2022, <https://foreignaffairs.house.gov/hearings?ID=5E89A2AC-7A9E-46E0-A0B1-2007FF2E0C5E>.

an avenue to shape global telecom standards in ways that favored Huawei and ZTE over non-PRC firms. The Biden administration made ITU leadership a priority from day one. The State Department identified and ran a compelling candidate, Dorreen Boden-Martin, in the leadership election, and launched a whole-of-Department effort to support her candidacy. In September 2022, she won the member state vote for ITU Secretary-General, defeating Russia's (and China's) attempt to put a former Russian telecom ministry official and Huawei executive in that position.

In 2020, China held four of the 15 leadership roles across the U.N. specialized agencies. Today, Beijing is down to one (the Food and Agricultural Organization, or FAO). In addition to the ITU election, the State Department successfully supported U.S. candidates at the International Organization for Migration (IOM) and the International Court of Justice (ICJ).

When the United States does not compete at full strength—or does not show up—we cede these playing fields to Beijing. For example, for decades, Washington did not prioritize supporting U.S. companies to win global infrastructure projects in the developing world. Beijing stepped into that void with the Belt and Road Initiative, which provided state-backed loans and other incentives to support Chinese infrastructure bids. The result: Beijing gained a dominant position in global port and telecommunications infrastructure. Today, the United States is once again showing up. Washington is deploying the DFC and other U.S. Government levers to help U.S. and allied companies compete for global infrastructure projects.³ That progress is slowly pushing the global system back toward U.S. and allied standards.⁴

(2) When combatting malign influence, transparency is our superpower and Beijing's kryptonite.

Beijing knows the China model is deeply flawed. Economically, growth has stagnated and youth unemployment is soaring. The party maintains significant control over various sectors of society and government—when the party issues an order, all must obey. That is not something other nations and peoples would opt into if given free choice. Thus, Beijing resorts to coercion—malign influence tactics—to undermine free choice. The difference between legitimate diplomatic competition and malign influence is that the latter is by design “covert, coercive, and corrupt.” It forces acquiescence through coercion instead of inducing it through attraction.

Examples of Beijing's malign influence tactics include:

- *Elite capture*: influencing political decisions through graft. In Malaysia, Chinese officials offered to undermine a graft investigation into former Malaysian Prime Minister Najib Razak (including by deploying China's security services to find out who was leaking his activities to journalists) in exchange for preferential access to infrastructure contracts.⁵ The U.S. Department of Justice has uncovered evidence of PRC corruption campaigns compromising U.S. Government officials, including an IRS agent and a high-ranking New York State government employee.⁶

- *Using open academic systems to steal intellectual property*: the U.S. Department of Justice has publicized cases of People's Liberation Army officers entering the United States and enrolling in U.S. universities as “students” to gain access to U.S. academics and proprietary academic information.⁷

³Elizabeth Economy and Melanie Hart, “America's China Strategy is Incomplete: Putting Beijing on the Back Foot Requires Economic Tools Beyond Tariffs,” January 14, 2025, Foreign Affairs, <https://www.foreignaffairs.com/united-states/americas-china-strategy-incomplete>.

⁴For example, The DFC joined forces with Japan's development bank to help Australia's Telstra acquire telecom assets in the Pacific Islands, outbidding a Chinese state-owned enterprise and successfully keeping those networks out of Beijing's hands. DFC also financed the winning bid that acquired the Elefsina shipyard in Greece, keeping a strategic port asset out of Beijing's hands.

⁵Tom Wright and Bradley Hope, “WSJ Investigation: China Offered to Bail Out Troubled Malaysian Fund in Return for Deals,” January 7, 2019, Wall Street Journal, <https://www.wsj.com/articles/how-china-flexes-its-political-muscle-to-expand-power-overseas-11546890449>.

⁶“Two Men Plead Guilty to Acting as Illegal Agents of Chinese Government and Bribery,” U.S. Department of Justice Press Release, July 25, 2024, <https://www.justice.gov/opa/pr/two-men-plead-guilty-acting-illegal-agents-chinese-government-and-bribery>; “Former High-Ranking New York State Government Employee Charged with Acting as an Undisclosed Agent of the People's Republic of China and the Chinese Communist Party,” U.S. Department of Justice Press Release, September 3, 2024, <https://www.justice.gov/usao-edny/pr/former-high-ranking-new-york-state-government-employee-charged-acting-undisclosed>.

⁷“Harvard University Professor and Two Chinese Nationals Charged in Three Separate China Related Cases,” U.S. Department of Justice Press Release, January 28, 2020, <https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related>.

- *Lawfare*: Chinese companies hire U.S. law firms to attack U.S. China-watchers.⁸ These lawsuits appear intended to deter U.S. researchers from publishing negative information about PRC companies and their ties to Beijing. For example, Chinese auto company BYD hired U.S. libel attorney Charles Harder to file suit against the Alliance for American Manufacturing (AAM) and individual AAM staffers, accusing them of “libel” for publicizing information about BYD’s CCP ties.⁹

- *Economic coercion*: Beijing uses its commercial ties with other nations to force them to abide by its political edits. Many cases are never made public. Beijing threatens to take these measures, and countries comply to avoid economic damage.

- *Disinformation and election interference*: China seeks to sow discord and undermine faith in democratic elections—including our own. The Atlantic Council’s DFRLab uncovered a network of pro-PRC accounts, known as “Spamouflage,” that engaged in opportunistic amplification of disinformation on the day of the 2024 U.S. Presidential election. One campaign featured a deepfake video that first appeared in Russian networks of then FBI Director Christopher Wray claiming the U.S. system was “overrun” with thousands of fake ballots. Other campaigns focused on swaying the results of down ballot races, targeting voters with disinformation and false claims of financial fraud against PRC-skeptical congressional candidates.

Boosting transparency should always be step one when combatting malign influence. These tactics are covert by design. Exposure often neutralizes them. For example, when corrupt officials are exposed, Beijing loses that avenue to exert influence (as it did in Malaysia and in the U.S. IRS case). When visa officers and universities know a “student” applicant is a PLA officer, they have the information needed to decline admittance. When the public knows information is coming from the CCP they are more likely to distrust the message.

In some cases, active defense measures are also required to prevent Beijing from using our open systems and society against us. For example, transparency is not enough to protect the U.S. electoral system; the United States is also strengthening cyber security protocols to make it harder for Beijing to intervene. Targeted visa restrictions are key to protecting certain U.S. academic sectors from covert PRC intrusion. Active defense is also required for disinformation and economic coercion, as will be discussed in the following sections.

When engaging to shore up systemic defenses, it is critical to avoid measures that reduce the benefits the U.S. gains from our open democracy and society, or that undermine U.S. efforts in other battlegrounds (such as promoting our system over China’s or attracting global STEM talent). In education, for example, the now-shuttered DOJ “China Initiative” fostered fear throughout the Chinese American scientific community that U.S. national academics could be targeted based on their race or country of origin, and that they could face civil rights abuses. Those fears triggered an exodus of scientific talent.¹⁰

(3) The global information space is an active battlefield that impacts every arena of U.S.-China competition. If the U.S. stands on the sidelines, we cede that field—and the upper hand in other arenas—to China.

Beijing engages in political warfare. In the Chinese system, every security institution answers to the Chinese Communist Party (CCP), and its primary mandate is to keep the party in power. In the early days of the CCP, that warfare was primarily about protecting the Party from domestic challenges. Today, Beijing is taking that fight global: it engages in political warfare in the international arena to advance PRC objectives at U.S. expense.¹¹ The United States tends to view warfare in simplistic military terms: one military engaging in kinetic action against another. China’s military is weaker than ours, so Beijing moves that battle to fields where it holds an advantage. The information space is one such battlefield. The People’s Liberation Army (PLA) has a “three warfare” concept that applies both at home and

⁸Bethany Allen, “Libel Lawfare: Is there a Legal Risk to Criticizing Chinese Companies?” July 28, 2024, The Wire China, <https://www.thewirechina.com/2024/07/28/libel-lawfare-chinese-companies-defamation-suit-anti-slapp/>.

⁹“Supreme Court Rejects Meritless Libel Lawsuit Filed by Chinese Company BYD Against AAM,” Alliance for American Manufacturing, <https://www.americanmanufacturing.org/press-release/supreme-court-rejects-meritless-libel-lawsuit-filed-by-chinese-company-byd-against-aam/>.

¹⁰Yu Xie, Xihong Lin, Ju Li, Qian He, and Junming Huang, “Caught in the Crossfire: Fears of Chinese-American Scientists,” June 27, 2023, Proceedings of the National Academy of Sciences, Vol. 120, No. 27, <https://www.pnas.org/doi/10.1073/pnas.2216248120>.

¹¹Catherine A. Theohary and Martin A. Weiss, “What is ‘Political Warfare,’” updated January 9, 2023, Congressional Research Service, [chrome-extension://efaidnbmnnnibpcajpcgclclefindmkaj/https://crsreports.congress.gov/product/pdf/IF/IF11127#:~:text=In%20broadest,to%20achieve%20its%20national%20objectives](https://www.congress.gov/product/pdf/IF/IF11127#:~:text=In%20broadest,to%20achieve%20its%20national%20objectives).

abroad: public opinion warfare, psychological warfare, and legal warfare.¹² At home, if the Party can keep its own people under control through public opinion and psychological means, it can stay in power without having to resort to kinetic force and paying the costs that come with that (such as scaring foreign firms and capital out of the China market). The same applies globally. In a Taiwan contingency, for example, if the PRC can use public opinion warfare, psychological warfare, and legal warfare to scare the global community into staying on the sidelines in a future Taiwan crisis, Beijing can likely take Taiwan.¹³ Within Taiwan, Beijing could deploy these same methods (as it is already doing in Hong Kong) to create enough pro-China sentiment and political instability to justify its takeover, effectively neutralizing the Taiwanese resistance.

Washington tends to assume private-sector media are enough to expose Beijing's actions around the world and convince other nations to support our objectives rather than China's. The problem is that no U.S. media company has the resources to stand up against the entire CCP war machine. Furthermore, their interests are profit-driven: independent media outlets do not take on national security objectives.

In the economic space, we now recognize that expecting individual U.S. companies to compete against a whole-of-government CCP effort is a losing battle. Thus, the United States and many other nations are deploying government tools to level the playing field. The same applies in the information space. The United States has world-class independent media organizations, including both traditional and social media. But those organizations cannot compete with the massive CCP info-war machine. Just as it is doing in the economic realm, the U.S. Government must deploy state tools to level the playing field.

The now-shuttered State Department Global Engagement Center (GEC) was the primary U.S. Government mechanism for public diplomacy and combatting China's information warfare. When it was active, GEC enabled the U.S. Government to broadcast its own messages to the broader global public. The aim of that messaging was to convince people around the world to pursue the same outcomes the U.S. was pursuing. The State Department also engages in government-to-government diplomacy to push messaging with partner governments; public diplomacy aims to do the same with their publics, creating an environment in which entire nations are rowing with us.¹⁴ Critically, GEC was not simply a government megaphone. GEC provided grants to third-party research institutions in the United States and abroad, empowering them to do their own due diligence on China's actions and expose that information to inform their own publics. That third-party voice was critical. Local publics view their own local think tanks, academics, and NGO's as more credible than the U.S. Government. When local organizations conduct their own China due diligence and share that information in their own voice, that resonates in a way U.S. Government messaging cannot. It also exposes PRC actions the U.S. government—and U.S.-based researchers—cannot, because local researchers have unique access to their own officials, institutions, and local PRC actors. Third-party grants (with appropriate safeguards in line with the Smith-Mundt Act) were a huge force-multiplier for U.S. counter-malign-influence efforts.

The former GEC office also directly investigated and exposed PRC disinformation to expose malign influence tactics at critical moments in U.S.-China competition. For example, the former GEC team tracked and publicly exposed how Beijing repeated Russian propaganda regarding its invasion into Ukraine.¹⁵ That public exposure—which tied specific PRC Statements to specific Kremlin talking points—helped demonstrate to European audiences, in particular, the degree to which China was complicit in the invasion.

(4) The United States must respond robustly to support target nations in resisting PRC economic coercion.

China's economic might is its biggest lever for global influence. For many nations, China is their largest trading partner and/or largest foreign direct investor. Beijing can exert control over all lanes of commerce, including the companies buying from, selling to, or investing in partner nations. It frequently orders PRC companies to halt those activities to force other nations to abide by Beijing's political edicts. Some

¹²Peter Mattis, "China's 'Three Warfares' in Perspective," January 30, 2018, War on the Rocks, <https://warontherocks.com/2018/01/chinas-three-warfares-perspective/>.

¹³Dan Blumenthal et al., "From Coercion to Capitulation: How China Can Take Taiwan Without a War," May 13, 2024, American Enterprise Institute, <https://www.aei.org/research-products/report/from-coercion-to-capitulation-how-china-can-take-taiwan-without-a-war/>.

¹⁴Joseph S. Nye, "Public Diplomacy and Soft Power," *The Annals of the American Academy of Political and Social Science*, March 2008, Vol. 616, pp. 94–109.

¹⁵"People's Republic of China Efforts to Amplify the Kremlin's Voice on Ukraine," May 4, 2022, U.S. Mission China, U.S. Department of State, <https://china.usembassy-china.org.cn/peoples-republic-of-china-efforts-to-amplify-the-kremlins-voice-on-ukraine/>.

of these cases are public. Beijing used economic coercion to target Canada over the potential extradition of Huawei's Meng Wanzhou, Australia over Canberra's call to investigate the COVID-19 pandemic origins, Lithuania over its Taiwan office, South Korea over the THAAD missile defense system, and the Philippines over its actions to assert its rights in the South China Sea. Some cases are never publicized, because the threatened nation backs down in response to Beijing's economic coercion threats.

The State Department is ideally placed to push back—not only after coercion has already occurred, but beforehand, when nations are facing economic coercion threats. During the Biden administration, the Department launched an internal unit to provide support to nations facing Chinese economic coercion.¹⁶ That effort was wildly successful. Over a dozen nations engaged the Department for support, and State Department support enabled those nations to stand firm in the face of PRC coercion.

(5) Congress should empower the State Department for full-spectrum competition. We are battling to determine which system—ours or Beijing's—prevails. The stakes are astronomical. This is not the time to keep major levers of U.S. national power on the sidelines.

- *Re-authorize the Global Engagement Center (GEC) to empower the United States to engage in effective public diplomacy and information competition.* Due to the recent lack of re-authorization, there is currently no U.S. Government entity with both the capability and the credibility to effectively combat PRC disinformation. GEC grants to third-party entities in the United States and other nations were critical for exposing and neutralizing PRC disinformation efforts, which are key to the covert nature of PRC malign influence. According to a recent Congressional Research Service report, the State Department inspector general found GEC to be “generally effective” in achieving these objectives.¹⁷ That effectiveness is why the Chinese government referred to GEC as Washington's “information warfare” unit and the “command center of perception warfare.”¹⁸ Shutting GEC—and keeping these counter-influence warriors off the global battlefield—boosts Beijing at U.S. expense.

- *Provide the funding and personnel resources needed to directly—and rapidly—counter PRC economic coercion.* At present, there is no single FTE or office at the Department with authorization and appropriations to counter Chinese economic coercion. During the Biden administration, the internal counter-coercion unit neared case capacity due to the number of nations coming in seeking assistance. Congress should empower the Department to counter PRC economic coercion by providing dedicated resources and FTE for this effort. In particular, it should fund the Office of the Chief Economist (OCE), which is a critical first step in coercion response. [Note: OCE also plays a key role in mapping PRC sanctions evasion, which is a complementary effort.]

- *Empower U.S. State and local governments to make informed decisions about the PRC.* Across the United States, most State and City governments do not have a single person dedicated to international affairs. (Some larger cities have a single person dedicated to both international affairs—with all countries—and immigration.) State and local governments do not have the capacity to track Beijing's influence tactics and do full due diligence on what may be involved in economic offers from Chinese companies. The State Department Special Representative for City and State Diplomacy and the Subnational Diplomacy Unit can fill this gap. Instead of seeking to staff all city and State governments across the nation with China experts, the Subnational Diplomacy Unit can serve as their gateway to existing expertise. During the Biden Administration, the Subnational Diplomacy Unit served that role; it also provided targeted China briefings to Governors and mayors offices that requested them. This office enables the Department to efficiently fill Chinese influence analysis and push-back needs across the nation, without requiring every mayor

¹⁶ Peter Martin and James Mayger, “US Creates Team to Counter China's Trade ‘Coercion’ Tactics,” April 28, 2024, Bloomberg News, <https://www.bloomberg.com/news/articles/2024-04-28/us-firm-steps-in-when-china-is-seen-as-a-bully-not-a-partner>.

¹⁷ Matthew C. Weed, “Termination of the State Department's Global Engagement Center,” December 26, 2024, Congressional Research Service, [chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://crsreports.congress.gov/product/pdf/IN/IN12475](https://crsreports.congress.gov/product/pdf/IN/IN12475).

¹⁸ For example, see: Foreign Ministry Spokesperson Zhao Lijian's Regular Press Conference on August 29, 2022, in Chinese at https://www.mfa.gov.cn/fyrbt_673021/202208/t20220829_10757191.shtml, and Foreign Ministry Spokesperson's Remarks on the US State Department's Report Targeting China,” September 30, 2023, in English at http://us.china-embassy.gov.cn/eng/zmgx/zxxx/202310/t20231005_11154911.htm.

and Governor nationwide to hire their own experts.¹⁹ Running these engagements through a single office also enables the Department to track Chinese influence trends and tactics, which it can then use to warn local officials what to expect and watch out for. Congress should strengthen the Subnational Diplomacy Unit to make its counter-China efforts more robust.

- *Provide the authorization and appropriations for the Department to proactively engage partner nation officials and scientists in strategic technology sectors.* At present, the majority of funded science and technology partnerships run through the NSF, NIH, DOE, NASA, or DOD. DOE and DOD bring a national security nexus to that engagement, but DOE is limited by its energy focus and DOD by its warfighting capability focus. Congress should empower the State Department to actively engage partner nations in sectors critical for U.S.-China competition.²⁰ Many of the most critical advancements are occurring in the commercial space, e.g., in quantum, artificial intelligence, cyber security, 6G development, and biotech. There is a need for proactive engagement among U.S. and allied researchers to build trusted research ecosystems that promote collaboration in ways that exclude the PRC. State is well-positioned to do the horizon-scanning engagement needed to promote science and technology collaboration, working with key allies to identify leading-edge researchers among allied nations and bring them together to help the U.S. and its allies compete effectively with China.

- *Support U.S. students to study China and the Mandarin language, developing specific capabilities that fill gaps in needed U.S. Government China expertise.* The number of U.S. students studying in China has fallen dramatically in recent years. That is partly due to the growing difficulties of traveling to and studying in China (which include detention risks and an increasingly draconian security environment). The students who still pursue China analysis also recognize that their best job prospects may be with the U.S. Government, which will require a security clearance, and many fear China travel will make them ineligible. Congress should provide authorization and appropriations for the Department to launch a China studies fellowship program aimed at building the bench the United States will need for U.S.-China competition. That program should identify key functional needs (e.g., science and technology or public diplomacy) and offer a three-step program to fill them: 1 year of funded language study at an approved language/exchange program in China or Taiwan, followed by continuing study at the Foreign Service Institute during the second half of the fellowship; a paid 12-month fellowship during which cleared students work in State Department China programs, which could include DC-based offices (sanctions, export controls, etc.) or field offices (supporting Regional China Officers or U.S. embassies/consulates in China); language testing at the end of the fellowship to provide verified scores for U.S. Federal Government jobs. This program should run at a post-graduate level and aim to provide Federal Government on-ramps for rising China experts in their mid-20's. Students participating in this program should receive a waiver for residency requirements that disqualify U.S. Government job applicants who have lived in foreign destinations (such as China) prior to submitting their application; other U.S. fellowship recipients (e.g., Boren Fellowships and Critical Language Scholarships) should receive similar waivers.

Senator RISCH. Thank you, Dr. Hart.

We will now hear from Dr. Jennifer Lind. She is an associate professor of government at Dartmouth College. She also is a faculty associate at Harvard University and the author of a forthcoming book on the rise of China and the future of great power competition.

So with that, Dr. Lind, the floor is yours.

**STATEMENT OF DR. JENNIFER LIND, ASSOCIATE PROFESSOR
OF GOVERNMENT, DARTMOUTH COLLEGE, HANOVER, NEW
HAMPSHIRE**

Dr. LIND. Thank you, Chairman Risch.

¹⁹Kristen Edgreen Kaufman, "Why The Next Trump Administration May Prioritize City-Level Diplomacy," December 18, 2024, Forbes, <https://www.forbes.com/sites/kristenkaufman/2024/12/18/why-the-next-trump-administration-may-prioritize-city-level-diplomacy/>.

²⁰"NSTC: Biennial Report to Congress on International Science & Technology Cooperation," February 29, 2024, The White House, <https://bidenwhitehouse.archives.gov/ostp/news-updates/2024/02/29/biennial-report-to-congress-on-international-science-technology-cooperation/>.

Chairman, Ranking Member Shaheen, and distinguished members of the committee, thank you for having me today.

What I would like to talk about is China's malign influence operations and influence operations more broadly, and let me talk about what these operations are and what makes them malign.

Although all countries seek to build their influence through a range of policies that we call public diplomacy, malign influence operations are a very different matter. The CCP conducts extensive influence operations that are malign both in terms of goals and methods.

Such operations seek to bolster authoritarianism, discredit democratic governance, reshape global norms in China's interest, and silence China's critics.

In these operations proxy organizations obscure ties to the CCP while they buy media companies and fund research and think tanks.

Cyber units employ illegal cyber espionage and hacking operations, and Chinese agents coerce American citizens into promoting Beijing's interests by threatening their family back in China.

China's influence operations are thus threatening because their goals run counter to U.S. interests and because of the covert and illegal methods on which they rely.

Furthermore, they are threatening because they are massive in scope. They are run through a huge government bureaucracy consisting of numerous different agencies at all levels of society.

The budget for these operations is said to exceed the budget of China's Ministry of Foreign Affairs. This is not geopolitics as usual. This is an unusually aggressive and well funded effort.

Now, how should the U.S. respond to these malign operations? In my written statement I introduced a framework for thinking about U.S. policy.

Its goal is not only to defend the United States from hostile Chinese operations, but also to convince Beijing to rein in its activities and thus to establish some rules of the road to stabilize our strategic competition.

The first step toward creating those rules is for U.S. leaders to identify which of China's activities are regrettable but normal great power competition.

For example, although we do not like it, and although we should maintain as good a defense as possible, we can probably tolerate cyber attacks, pro-CCP fake accounts on social media.

But the second category of activities is different. These are the policies or behaviors that U.S. leaders decide are intolerable.

Such activities might include election interference, abductions, and operations that coerce American citizens. So step one is to distinguish between regrettable but tolerable operations versus intolerable ones.

Step two is to develop a tool kit that we are willing to use to shape Chinese behavior, actions that the CCP would view as intolerable.

The U.S. Government would convey privately to Beijing that if it violated the bounds of acceptable activities we would respond in kind. That is, we would cross some of Beijing's red lines.

This is not an escalation. It is how great powers establish the rules of the game. Beijing's bright red lines—the absolutely “intolerables”—relate to China's domestic stability. Specific policies would have to be figured out at the classified level.

But once again, the core idea is not only to play defense, but to make the CCP feel the costs of its aggression and to encourage it to moderate its behavior. This sounds delicate and dangerous and hard, and it is actually harder.

Let me conclude by noting that not only do we have to manage this challenging strategic competition with Beijing, but in that competition lurk potential dangers to the rights of millions of Americans, Chinese Americans in particular.

Our adversary is already—at this early stage and in peacetime—coercing good Americans to work against their country on its behalf.

As we formulate our responses to Chinese malign influence operations U.S. leaders should think about previous situations such as World War II, Japanese internment, and cold war McCarthyism, and think about when our institutions protected our people versus failed them.

In other words, U.S. leaders should think not only about this important strategic interaction with Beijing, but whether our policies in that interaction uphold our values.

Thank you very much.

[The prepared statement of Dr. Lind follows:]

Prepared Statement of Dr. Jennifer Lind

Chairman Risch, Ranking Member Shaheen, and distinguished members of the committee: thank you for the invitation to testify before you today. My name is Jennifer Lind: I'm a professor at Dartmouth College in New Hampshire where I teach courses on great power politics, East Asian international security, and U.S. foreign policy toward the region. My recent research and forthcoming book focus on China's rise to become a great power and technological leader.

In my testimony today I will briefly cover four topics. First I will discuss what are influence operations and when are they malign. Second, I will comment on how threatening we should view Chinese operations. Third, I will offer a framework for thinking about U.S. responses: one that relies not only on defense but on more assertive measures as well. Finally, I conclude with thoughts about responding to Chinese influence operations in ways consistent with U.S. values.

(MALIGN) INFLUENCE OPERATIONS

Every country to some extent engages in activities to communicate its views, frame its actions in the best light, and shape policy outcomes to reflect its interests. China is no exception in pursuing what we call public diplomacy or soft power. The Chinese Communist Party (CCP), like other governments, engages in numerous mundane influence activities: it extends aid and loans to other countries; it promotes a positive narrative of China overseas; China's government sponsors educational and cultural activities abroad; Chinese diplomats write op-eds in foreign newspapers and promote the national interest within international organizations. In the United States, Chinese firms hire lobbyists to influence U.S. policy; China's government hires PR firms and offers all-expense-paid trips to China to influential Americans. All of these activities are routine in international relations. To be clear, we don't like these Chinese activities because of the agenda they advance. But they are standard public diplomacy: business as usual in international politics.

However, malign influence operations are a different matter. The CCP conducts extensive influence operations against the United States and the broader international order that are malign in terms of goals and methods. Such operations seek to bolster authoritarianism, discredit democratic governance, and reshape global norms in China's interests. China exploits its economic leverage, such as market access and investment, to coerce businesses and governments to behave in accordance

with Beijing's wishes. The CCP employs propaganda and disinformation campaigns, relying on social media manipulation to sow division and weaken democratic resilience. Cyber-enabled espionage and intellectual property theft bolster China's military and technological power. CCP co-optation—of NGO's, academics, political and other leaders—seeks to silence criticism of China. In many of its influence operations, the Chinese government coerces Chinese citizens living abroad as well as Chinese Americans.

THE THREAT OF CHINESE MALIGN INFLUENCE OPERATIONS TO THE UNITED STATES

The CCP clearly conducts a mixture of mundane and malign influence operations. Is China's level of activity in this domain unusual or unexpected? Are its operations particularly malign? Such context is important because if China's actions seem unusually aggressive, that's an important threat indicator.

A look at Chinese influence operations suggests their extent is vast. The CCP conducts such operations through a massive government bureaucracy that includes agencies such as the United Work Front Department, the Propaganda Department, the Ministry of State Security, the Ministry of Foreign Affairs, and the Chinese People's Association for Friendship with Foreign Countries. The CCP also directs influence operations that recruit Chinese businesspeople from both the State and private sectors.

The annual budget for such activities is understandably hard to assess but estimates range from about \$3 billion to \$8 billion. The Jamestown Foundation's Ryan Fedasiuk reports that this exceeds China's budget for the Ministry of Foreign Affairs.¹ From the extent of China's influence operations we can infer the CCP's high level of ambition and commitment to advance China's interests and undermine the United States.

What can we learn from the types of influence operations that China pursues? As noted, the CCP engages in operations that depart from mundane public diplomacy activities, or even from the espionage common to great power rivalries. First, many Chinese operations are malign because they are covert rather than transparent. Proxy organizations that obscure their connections to the CCP fund political contributions, think tanks, and academic research. The Hoover Institution reports that the CCP gained control of the Chinese-language media in the United States as well as in other countries; "Over the course of the last decade, most of the independent Chinese language media outlets in the United States have been taken over by businessmen sympathetic to the PRC."² China's government also seeks to shape public opinion through social media operations that rely on fake accounts and "hashtag storms" to flood sites with pro-CCP content while burying dissenting opinions and encouraging abuse of people who offer them. Other examples of covert activities abound.

Second, many Chinese influence operations are malign because they violate U.S. law and the rights of American citizens. Chinese cyber units engage in operations to steal U.S. technology, gather intelligence, and disrupt activities critical of the CCP. Such operations rely on cyberespionage, identity theft, and hacking operations that use malware and spear phishing techniques. Targets include the U.S. Government, think tanks, NGO's, researchers, activists, dissidents, and journalists.

Chinese agents also operate in the United States in violation of the Foreign Agents Registration Act. They engage in surveillance and intimidation campaigns against Chinese citizens (e.g., tourists, students, businesspeople, and researchers) as well as U.S. citizens of Chinese descent. The CCP harasses and pressures people to promote Beijing's interests by threatening their families in China. In 2020, the U.S. Department of Justice charged eight individuals who stalked and pressured a Chinese dissident and his family in New Jersey, as part of China's "Operation Fox Hunt": a program ostensibly aimed at apprehending Chinese fugitives abroad, which has been turned against dissidents and other ethnic Chinese.

In sum, this is not geopolitics as usual. China's influence operations do seem unusually expansive, unusually well-funded, and frequently conducted using covert and illegal methods that undermine not only U.S. interests but the rights of American citizens and the rule of law in our country. Although the United States previously engaged in this kind of shadow conflict with the Soviet Union, this is not your father's cold war. As a rich, economically central, and technologically advanced

¹Ryan Fedasiuk, "Putting Money in the Party's Mouth: How China Mobilizes Funding for United Front Work," China Brief 20, no. 16 (2020), <https://jamestown.org/program/putting-money-in-the-partys-mouth-how-china-mobilizes-funding-for-united-front-work/>

²Larry Diamond and Orville Schell, eds., *China's Influence & American Interests: Promoting Constructive Vigilance* (Stanford, Calif: Hoover Institution Press, 2020), p. 214.

country, China has a powerful toolkit to exploit as it engages in influence operations in the United States and around the world.

RESPONSES TO CHINESE MALIGN INFLUENCE OPERATIONS

How should the United States respond to Chinese malign influence operations? Scholars and think tanks have produced many articles and reports that detail the numerous U.S. Government agencies and programs that monitor and counter Chinese activities. Such studies generally emphasize defensive U.S. responses to blunt Chinese operations.

I would like to build on the valuable tools recommended in those studies to introduce a broader framework for thinking about U.S. policy. The goal of this framework is not only to consider how the U.S. should defend itself from hostile Chinese operations, but how to convince Beijing to rein in its activities. The United States is in a great power competition with a very capable adversary; this is going to be a long haul with a serious risk of crises and war. In the shadow conflict of influence operations, the two countries—as the two superpowers did in the cold war—should create some rules of the road in order to stabilize their relationship.

The first step toward creating those rules is for U.S. leaders to identify which of China's activities are regrettable but normal great power competition. After all, China is a great power with its own interests; China is allowed to do things even if we don't like those things. So we should ask ourselves, which Chinese behaviors and activities fall into that "regrettable but acceptable" category—versus which activities do we view as intolerable? That's our first challenge: to distinguish between the two.

Examples of "regrettable but acceptable" activities might include pro-CCP fake accounts on social media, Chinese efforts to set agendas in key international institutions, and Chinese aid for brutal authoritarian leaders. To be clear, we disapprove of such activities; we would keep playing defense and try to thwart them. But we would understand that such operations are commonplace and, from our standpoint, bearable.

The second category of activities are different: they are the Chinese policies or behaviors that U.S. leaders view as intolerable. Such activities might include election interference, abductions, and operations that harass, coerce, or blackmail American citizens (of Chinese descent or otherwise). These operations undermine the rule of law in the United States and our responsibilities to protect our citizens from direct harm by foreign adversaries.

Step two is to develop a toolkit that we are willing to use to shape Chinese behavior: activities and policies that the CCP would view as intolerable. The U.S. Government would convey privately to Beijing that if their influence operations violated the bounds of acceptable behavior, we would respond in kind: in other words, we might cross some of Beijing's red lines. This is not an escalation—it's a negotiation. This is how great powers establish the rules of the game—about what's going to be normal conduct versus what's going to be out of bounds.

What are the CCP's red lines? Beijing would prefer that we wage the shadow conflict far afield—in the United States, in third countries, and no closer than Taiwan, Tibet, and so on. But Beijing's bright red lines—the absolutely intolerables—relate to China's domestic stability. The CCP worries about its people mobilizing, getting ideas about democracy, and about economic and financial crises delegitimizing the regime. If the United States were to push ideas about democracy, or to take steps that undermine the stability of the Chinese economy—for example, its real estate or banking sectors—that would be intolerable to the CCP.

Identifying specific policy tools would have to be done by experts doing very sensitive work at the classified level. At an unclassified level we can't even talk about what are current U.S. operations, let alone how one might want to shift them or scale them up. So today I can't give you specific recommendations but rather offer this general framework for thinking about U.S. responses.

Once again, that frame is: first, figure out what we view as garden-variety great-power competition versus unacceptable Chinese behavior. And second, figure out how we might respond using both defense and offense—defense to protect ourselves from China's run-of-the-mill activities, and more assertive steps designed to make the CCP feel the costs of its aggression and to encourage it to moderate its behavior. And over time the two countries would forge an equilibrium in which hopefully both sides stay within the bounds of that agreement in order to maintain stable relations.

LIVING UP TO OUR OWN VALUES

Let me conclude by noting that as we formulate our responses to Chinese malign influence operations, U.S. leaders should be thinking not only about this negotiation

with Beijing, but also about whether our responses uphold our own values. Among our people number millions of Chinese American citizens. We find ourselves in a complex situation in that our adversary is already—at this early stage and in peacetime—harassing and coercing good Americans to work against their country on its behalf.

As U.S. leaders evaluate policy responses to Chinese operations, it's helpful to think about similar situations in the history of U.S. national security policy, and to ask ourselves what we got right and wrong. U.S. leaders should have this conversation (as indeed the Committee is doing today) with members of America's free and vibrant civil society: which sets us apart from authoritarian rivals and indeed is one of our country's strengths.

In World War II, the U.S. Government imprisoned Japanese American citizens in camps in violation of the U.S. Constitution. In the cold war, the Red Scare of McCarthyism violated the rights and ruined the lives of many people. The aftermath of September 11, 2001 in some ways offers a more optimistic example. President George W. Bush made it crystal clear to Americans that we were not fighting a war against Islam, but against a terrorist group that had twisted Islam's teachings. This kind of strong leadership was essential then and is essential today.

It is important for Americans to recognize that in the security competition with China lurk not only geopolitical dangers, but dangers to our people and values. As that competition becomes more intense, and as we get frustrated that an authoritarian society is exploiting our free one, while we protect ourselves against Chinese influence operations in the ways recommended here, we must also honor our own values.

Thank you.

Senator RISCH. Well, thank you.

First of all, I want to commend the panel. We get panels through here all the time but this is probably as good a presentation as we have had on an issue in a long, long time.

Part of this whole problem is the fact that convincing America and different segments of America how dangerous of a situation this is, and one of the ones I have been focused on over the years and have been somewhat successful but not completely successful is to get a better handle on what colleges and universities are doing.

The colleges and universities, as all of you know, are a really target rich place for the Chinese. They show up with money, and as was pointed out here, colleges and universities respond to money whether it is from their donors, from their alumni, or from the Chinese showing up with money.

And most Americans are shocked to hear that we have hundreds of thousands—hundreds of thousands—of Chinese students studying here in the United States with only a tiny, tiny fraction of U.S. students studying in China, and there is a huge difference.

The Chinese students here are not studying ancient Greek history. They are here with the STEMs and the national security issues and everything else, and each and every one of them, whether they like it or not, is an agent of the Chinese Communist Party.

When they go back, we all know they get debriefed, and any information that they have garnered here in the United States becomes the property of the Chinese Communist Party.

So we have seen example after example of the Chinese showing up at a university, coming up with millions of dollars, and they get a chair—they get an endowed chair. They get an entire institution within the institution focused on what they want to have focused on.

So I guess the question I would have for all of you is—and first of all, admittedly universities have an entirely different view than we that work in the national security lane do of this.

When you sit down and talk with them, they believe, and a lot of them, I think, are very sincere in their belief that, oh, in academia we are all together.

This is one big world and we should all use this knowledge that we have and share it with each other regardless of the national security implications of it, whether it is designing computer chips or designing factories that manufacture arms.

So give me some thoughts. How do we bring the universities on board to have a better understanding of, number one, how dangerous China is, and number two, how they are exploiting us even without our knowledge in a lot of instances in taking what we have?

Mr. Mattis, let us start with you.

Mr. MATTIS. Well, one thing I can tell you is that 10 years ago this was a completely different problem than it is today. There are actually resources, there are companies, there are more experts, there are journalists, there are plenty of places where universities can go.

So a dearth of expertise or a lack of information is no longer the problem that they once faced, or it was not as severe.

The second, as I think my friend Jeff has said, that the grant reporting requirements from the Federal Government actually have to be rigorously pursued and adhered to.

We would not—we would consider it corruption if it were a defense contractor or others that were not providing the correct reporting requirements, and because, as I think you have heard from every single witness, the problem here is the corruption of the rules and the corruption of the process, and as long as that process is clear and has rigor, then it will provide the basic level of protection.

I think the other piece that is there is to go back into your home States and to talk to the public universities and engage them on and ask, well, what have you done for compliance? What do you do about these things? Because I know from my time on Capitol Hill that those conversations actually did bear fruit, and they did drive public universities to think about this.

Senator RISCH. That is a good suggestion. Thank you.

Mr. Stoff.

Mr. STOFF. Thank you for the question.

Yes, a lot of it—I agree, a lot of it has to do with raising a level of understanding and awareness, and one of the challenges is that the U.S. Government needs to share a lot more information on the kind of investigations.

For example, the OIGs do a lot of interesting things that are at civil and administrative levels that do not reach—that are just simply not public record, right, because they are not a criminal indictment, and that is not a bad thing.

But what happens is the universities are not seeing and they are not really incentivized to see what is happening on their campuses and the type of malign influence and the way China can come in and divert and influence the research that is going on.

There is some information that the government has that I think needs to do a much better job in sharing that. There also needs to be much more scholarship on the topic itself where we demonstrate

activities, and behaviors, that China exerts that are fundamentally against the principles and values of academic freedom, transparency, reciprocity, and integrity, which are core to what universities talk about of their mission, and there needs to be a lot more effort looking at where and how this is being done to show this is affecting us all, including on your campus, so that we take more collective action.

Thank you.

Senator RISCH. Dr. Hart.

Dr. HART. Thank you.

I endorse the comments that have come before and would like to just add one point. We need a scalpel for this, not a sledge hammer. It is in U.S. national interest to keep the student pipeline open.

We are in a pitched battle for global tech supremacy. For decades Beijing stole our IP. Let us steal their best engineers.

You know, China's national engineers developed the DeepSeek AI model that surprised the world this week. You know, we would be better off if the engineers behind that were working here in the U.S. and U.S. universities and U.S. companies. So it is important to keep that in mind.

Those student exchanges are a way that we can siphon off some of Beijing's top talent. So we want to make sure that for the students that are here, for the researchers that we want, that they feel they are safe in the United States, they understand how to follow the rules, and they feel their civil rights will be protected. We can beat Beijing at making Chinese scientists feel safe.

Senator RISCH. Well, thank you, Dr. Hart. There is a flaw, however, in your suggestion, and I think probably everyone in the room knows it.

When a student comes over here, they got to go back. If they do not go back, there is a family there, and we all know what the Chinese government does to families. They do it across the oceans, and they do it even here in the United States.

So that is a great idea. The problem is we are dealing with a malign institution here. We are not dealing with people like Americans who say, oh yes, you are free to move and do whatever you want to do.

They will take it out on the families. We have all heard stories of that. But you know, your thoughts are well taken, that it would be good if we could reverse the tables. I am not so sure that we can do it in the same manner.

My time is up, and Dr. Lind, we will get to you too again. We are going to do a 5 minute round, and if we have got time we will back up.

So, Senator Shaheen.

Senator SHAHEEN. Well, thank you all.

Let me echo the Chairman on his appreciation for the presentation from everyone and give a special shout out to Dr. Lind from Dartmouth College in New Hampshire.

We just have to get that in, Dr. Lind.

Senator RISCH. Look at the time.

[Laughter.]

Senator SHAHEEN. Senator Rubio, Secretary Rubio now, introduced a bill back in July of the last session that would have required the Secretary of State to work with the Ukrainian government to establish a mechanism for reviewing PRC investments in Ukraine.

Now, sadly, one of the results of this foreign assistance freeze is that it is cutting off some essential services to Ukraine at a time when we know not only is Russia looking at how they can undermine Ukraine, but the PRC is starting to invest there.

So, if our goal is to prevent Ukraine from accepting that PRC investment, how does cutting off our own assistance move us toward that goal? And are there incentives for Beijing to play a productive role in trying to get to peace talks in that conflict?

The President has raised that as a potential role for the PRC. Do we think that is likely, Dr. Lind?

Dr. LIND. Thank you for your question.

On the broader issue of pausing U.S. foreign aid, I agree with the sentiments that we have heard today so far that talk about foreign aid as a really important arrow in the quiver of U.S. national security, along with other tools such as diplomacy, military assistance, and so on.

And so ideally we would want to be using all of our different tools in a coordinated fashion to achieve our objectives. So for that reason I think it is understandable if the Administration wants to take a short pause and assess, are we using the right tools in the right way, should we be using some tools more than others, and so on.

But we should not be taking this important arrow out of our quiver, and we should recognize the many areas across the globe where it does so much good. We have talked today about medicines going to waste on ports, talked about children dying, right? So there are such implications to think about here.

So because of that, it is really important that we remember there is important development assistance that this pause will affect, and there are also strategic realms that we may not have appreciated how consequential this aid pause would be such as the conflict in Ukraine, for example.

Senator SHAHEEN. So, is there any incentive for the PRC to help move negotiations around the war in Ukraine? Does anybody on the panel think that there is a way that would encourage them to do that?

Mr. Mattis.

Mr. MATTIS. So, as president of the Jamestown Foundation, I oversee a large network of analysts that are not just covering China but focus on Russia as well, and it is hard to see that the PRC has played any kind of neutral role, and even their positioning in peace talks has not been neutral—it has been reinforcing Russia's positions.

And I cannot help but think that at best getting them to neutrality would require a lot of pressure and a lot of threats to their system that we can still apply, and the question is whether or not we would want to escalate in that way.

But barring some massive change Beijing is not neutral, and they have put their support behind Moscow. So, anything there

they will try to bring pressure on Ukraine and to get Ukraine to surrender.

Senator SHAHEEN. Thank you.

Dr. Hart, as you pointed out in your comments, and I referenced in my opening statement, the PRC spends over a billion dollars a year in promoting their messaging. The state backed media outlets are found in every major hotel in the world.

Chinese firms purchase local media outlets, and yet we are woefully behind. You mentioned the Global Engagement Center, also appropriations for U.S. Agency for Global Media entities and networks including Radio Free Asia, Voice of America, Radio Free Europe.

Those have declined by almost 12 percent in real terms over the past decade, and as we all know America has a better story to tell, but we need to be a lot better at telling it.

So what should we think about other than those two arenas in terms of competing with China on their propaganda campaign?

Dr. HART. Sure. I will make two points.

You know, China, as you said, is spending over a billion dollars in getting its message out to the world. That is very difficult to combat directly.

But one brilliant element of the former Global Engagement Center is that it provided grants to third parties in the United States and in other agencies to empower NGOs around the world to do their own investigations and their own exposure of what Beijing was actually up to.

So it was a massive force multiplier. It enabled the United States to leverage voices around the world to combat Chinese disinformation, and that third party element is really critical.

And I would just add one other point, which is our online spaces. Unfortunately, we are seeing quite a bit of disinformation in social media and in other online spaces, which again, the U.S. Government can be a bit slow in tackling those spaces.

But there are third party agencies that are great at it. The Atlanta Council has the digital forensic research lab, for example, which is actively tracking Chinese and Russian disinformation in U.S. and other social media domains. We want to empower not just the U.S. Government but also every ally we have in the field.

Senator SHAHEEN. Thank you.

Senator RISCH. Thank you, Senator Shaheen.

Senator Ricketts.

Senator RICKETTS. Thank you very much, Mr. Chairman, and thank you to our panelists for being here today.

Communist China is the single biggest external existential threat we have to our nation. I believe that you are all making the case for that, that this needs to be what we focus on, and we have not been focusing on it.

And during his confirmation hearing, Secretary Rubio warned that, quote, "If we stay on the road we are on right now, in less than 10 years virtually everything that matters to us in life will depend on whether Communist China will allow us to have it or not."

Folks, right now we are facing that first real test of whether or not we are willing to get off that road that we have been on that

has allowed Communist China to take advantage of the world system and seeks to—and a country that seeks to displace us, and that test is TikTok.

This app is just not another social media platform. It is one of the apps that Communist China uses in its web of diplomacy to push its propaganda, spy on Americans, and control the narrative of why they think they are better than we are.

That is why we passed with bipartisan support a law that required ByteDance to sell within 270 days, and the Supreme Court, by the way, upheld that law unanimously.

The law is now moved or is in effect, and so what you are seeing is TikTok has been removed from app stores, meaning that not only can new users not download it, but you cannot get updates, so effectively it will mean that the existing users will see their experience degrade as well.

And as long as Communist China governed ByteDance controls the app it is going to be a tool for the Communist Party in China to try to exercise its malign influence here in the United States.

TikTok has 170 million users. Fifty-two percent of them get their news from it. That is over 88 million Americans that rely on the app, and after October 7 we saw that there were 50 times more views that were more pro-Hamas, pro-Palestine than pro-Israel, despite the fact that polls show that Americans overwhelmingly supported Israel.

And TikTok is—we talked about controlling the narrative—China suppresses the information on there. So, for example, I have seen different studies that show that, for example, if you compare TikTok and Instagram, there is 80 times more mentions of Tiananmen Square on Instagram versus TikTok, 180 times more mention of the Hong Kong protests when that was going on on Instagram versus TikTok, 400 times the amount of content talking about Communist China being responsible for COVID on Instagram versus TikTok, and when it comes to Uighurs about 10 times more information on Instagram versus TikTok.

This is part of how they are shaping the narrative, and it is just the start. We see this in other applications as well, obviously, with the announcement of a law going into effect on TikTok RedNote saw a bunch of users, and of course, Dr. Hart, you just talked about DeepSeek as well. China is lining up the next apps to be able to control our things.

And by the way, folks, we do not allow foreign adversaries or foreign companies to own our TV stations and radio stations. You are limited to 20 percent of a direct foreign ownership in a TV or radio station. We do not have such laws for streaming services. That is one of the things, perhaps, we can take up.

So these applications are where people are getting news in America. We have laws to block them in TV and radio stations, but not for applications like TikTok.

Mr. Mattis, how relevant are these apps like TikTok to Communist China's strategy to control the narrative, to be in competition with us, to undermine us?

Mr. MATTIS. So one of the points that I alluded to in my statement, and that Melanie has spoken about, said this narrative fight is actually not just a narrative on narrative, but it is a competition

for the platforms and the pipes, if you will, that allow narratives to move and allow them to be pushed out.

So if we go back, let us say, 40 years to the Soviet disinformation effort to say that the United States was harvesting organs from babies in Latin America or was the source of AIDS as a biological weapon in Africa, those were things that took years and years of effort, and now those stories can be disseminated to 170 million people, essentially, instantly and overnight.

This is the biggest change, and I think we have to keep our eye focused on what those platforms are so that they can be free flowing, that they are not distorted.

Because to me, I know it is easy to understand the privacy issue of some of these apps, but it is the ability to distort the messages that people hear that are the most important, and everything that we have learned about cognitive psychology—the way that we take in information, the way our biases become anchored—the more closed off or the more you are sucked into a particular information source, the easier it is to plant something that will stick and that will be harder to pull apart.

So we have to keep our eye—I focus less on the narratives themselves and much more on the groups and the platforms. It is first the medium, then the message is what the party is doing.

Senator RICKETTS. And if I may, Mr. Chairman.

Just real briefly, what should we do about RedNote and DeepSeek and other platforms like that?

Mr. MATTIS. I think for those kinds of platforms you have to adopt the same approach that was applied to TikTok, that it either is sort of removed from their control, or it is no longer available in the app stores.

Senator RICKETTS. Great. Thank you very much, Mr. Mattis.

Thank you, Mr. Chairman.

Senator RISCH. Thank you.

Senator Schatz.

Senator SCHATZ. Thank you, Chairman.

Thank you to our panelists.

And I agree with the Chairman, this is an excellent group to inform us.

Mr. Mattis, I want to just start with the Philippines. As you know, they are one of our closest allies. We have economic assistance arrangements. We have lifesaving support that we provide, and of course, we have a security partnership that has lasted generations.

If you were a senior CCP official, how would you view this freeze in foreign aid coming from the United States?

Mr. MATTIS. Frankly, I would be looking to exploit the opportunity that is there, and over the years the political fluctuations in the Philippines have offered those opportunities.

They have disrupted the relationship. They have disrupted partnership, and anything from Beijing's perspective, or if I were in the senior official in the united front work department I would be doing everything I can to exploit whatever chaos is there in the U.S.-Philippine relationship.

Senator SCHATZ. What would that look like?

Mr. MATTIS. Either/or sort of the traditional tools of sort of corruption. I would be looking also to mobilize groups, to lobby politicians to say, well, look, the U.S. is an unreliable ally, and that you need to move in this other direction.

I would be looking to creating pressure about escalation risks if the Philippines chooses to defend itself on Second Thomas Shoal and other territories. It could go on a range of things like that.

Senator SCHATZ. Sure.

Do you think this moment is particularly important? I mean, it seems to me like tactically that if I were a senior CCP official, I would be mobilizing this week to be making some moves that are specific to the opportunity presented this week. Not just as a general proposition in terms of great power competition in the Asia Pacific region, but specifically to seize this opportunity of us looking like an unreliable partner.

Is that fair to say?

Mr. MATTIS. When I look at the CCP, what I was alluding to was a long term set of ambitions and clarity, and we may be talking about this more, but it does not mean that 10 years ago we did not know or we did not see these. It is just that we were not looking.

Senator SCHATZ. No.

Mr. MATTIS. So there are always opportunities to exploit.

Senator SCHATZ. So let us go to Papua New Guinea. A lot of natural resources, but it is at risk of becoming a foothold for PRC military expansion.

But right now it has the highest HIV incidence in the Pacific, and it is rising. It also has a lot of unexploded ordnance, and last year the Department of Defense signed an \$864 million defense deal with Port Moresby.

So it seems to me that the Philippines is one question. We have a bilateral relationship that spans generations and is sturdy. Like, under Duterte less sturdy but still solid, even when we have a President who is an unreliable partner.

But in places like PNG where, to use the domestic equivalent, they are sort of swing states. They are open for business to being aligned with China, to being aligned with the United States, to playing both sides against the middle.

I am particularly concerned about smaller countries for whom withholding of economic or military or lifesaving support is not something they can sort of weather, and so I am wondering if you can talk about PNG in particular.

Mr. MATTIS. I do not know specifically about this, and I think it is the Secretary's job to determine how the priorities go, because we cannot be everything to every country, and I would hope that there is some systematic view of where do we prioritize, what is important, where can we intervene effectively, and where does an intervention simply sort of pour bad money after bad.

Senator SCHATZ. Yes.

Ms. Hart, did you want to just comment just generally speaking on the opportunity we are presenting to the CCP? And I do not mean generally. I mean this week.

Dr. HART. Sure. Basically, we have given Beijing a blank check and kneecapped the United States and the entire global pro-democracy movement.

If you want to talk about PNG and their need for medicines, there is a very clear pattern that during the COVID crisis Beijing forced nations around the world to carry out its political edicts in exchange for COVID vaccines.

I have no doubt that Beijing is already showing up in capitals where the United States is pulling back and saying, here is your HIV medicine, and guess what? Here is the three things you need to do for me today to get it.

Senator SCHATZ. Thank you.

Senator RISCH. Thank you, Senator Schatz.

Senator McCormick.

Senator MCCORMICK. Thank you, Mr. Chairman, and thank you. What a great and sobering panel.

Mr. Stoff, I would like to start with you and talk about the CCP's IP theft in research security. I ran the Commerce Department's export controls about 20 years ago, and even then there were warning signs of the CCP's infiltration.

I remember giving a speech that talked about 90 percent of Chinese software being stolen or acquired from—mostly from the United States. Here we are two decades later, and that risk seems more extreme and pervasive than ever.

When it comes to the CCP theft of U.S. research and IP, where are we most vulnerable and are research security requirements for sensitive dual use technologies, in particular, keeping up?

Mr. STOFF. Thank you for that question, Senator.

First, I think we need to understand and frame the current regulatory landscape that we operate in. Where we are most vulnerable is in fundamental research domains as defined by National Security Decision Directive 189. And basically, as you probably know, Senator, export controls, largely, do not apply in any case to any academic research that is designated as fundamental.

And so that means that outside of a few appropriations restrictions that have been put in place, particularly the NASA Wolf amendment, there really is not any restriction of any kind, and so this allows basically just a free for all—and this was set up by design but now has become a much bigger problem, and I think the problem that you are raising goes beyond how we traditionally define and view IP theft at least with the way our legal statutes are designed.

Particularly, 1831 and 1832 of the U.S. criminal code have very specific requirements to prove that it is theft, and most of the time a lot of what is happening in academia because of the open nature of our system is not actually theft the way our statutes define it.

As such, the entire early stage of our research and innovation ecosystem is basically rife for complete penetration, influence, and diversion of all of that technology and research for China's benefit.

And as was pointed out earlier, I think Chairman Risch had mentioned, when China comes in with lots of money, this is irresistible, and the combination of those two things makes it very difficult for U.S. policy to effect change because—originally by design—there is not enough regulatory oversight to do anything about it.

Quickly, I would say that, and in my recommendations in my written testimony, I do think that we need to apply some of the re-

strictions in our export control regimes—the Entity Lists, or the BIS List, or the OFAC lists—those are already established. The U.S. Government has already determined that there are a number of entities, both research institutions and companies, that conduct research that are a threat to our national security.

Well, we should put restrictions in place if you are dealing with those entities because the Government has already decided that those entities are a problem. So a kind of harmonizing our export control regime with our ecosystem will help.

Senator MCCORMICK. Yes. That makes a lot of sense.

Along those same lines, in December the Biden administration signed a 5 year extension of the U.S.-China science and technology agreement.

Was this a good idea? Is this part of the big gap in our regulatory framework that you are referring to?

Mr. STOFF. To be honest, Senator, I am not familiar enough with the details of that agreement to opine on whether this is effective or not.

But the sense I get is most of the policy apparatus and how universities and the government interact with each other, with grant making agencies, et cetera, the things that I recommend I do not think would have any bearing or effect on this larger government-to-government science and technology agreement. I think the things that I recommend would not necessarily conflict with that agreement.

Senator MCCORMICK. Thank you.

Mr. Mattis, just very quickly, we saw all the announcements this week around DeepSeek-R1. Does the proliferation of open source AI models that are trained to push the CCP's propaganda advance the party's efforts to shape public discourse in the United States, and how can this open source approach enable future influence operations?

Mr. MATTIS. So very quickly, I think there are two dangers of platforms like this coming out of the PRC.

The first is that it is a data collection effort that the more people interact with these systems the more that is brought in, and this is something that is—you know, goes back to, you know, sort of the back end software that are on Huawei telecommunications and conference equipment—many other areas where you can see the PRC putting things kind of astride those pipes and platforms that allow them to benefit from the flow of information. So that is the other piece.

The second is that the more that those models are trained on an international set of data, the more we are able to see things like the effectiveness of automated disinformation systems or propaganda systems that we have seen the PRC use, and the better those are, the harder it is to deal with, the harder it is to recognize them, the harder it is to shut it off.

Senator MCCORMICK. Thank you.

Senator RISCH. Thank you.

Senator Coons has yielded to Senator Kaine, as I understand it. Senator Kaine.

Senator KAINE. Thank you, Mr. Chair, and thanks to my Delaware colleague, Senator Coons.

Thank you for being here.

I am interested in all of this topic. I am particularly interested in Chinese influence in the Americas. I have maintained during my now 12+ years here under Presidents of both parties, and under Senates controlled by both parties, that we do not spend enough time or attention in the military space through SOUTHCOM or in the foreign assistance space; we are not focusing enough on the Americas.

And China sees that as a huge opportunity area for them, and my other colleagues who travel in the Americas, we see this all the time. Investments in Panama, offers of, you know, 5G systems to nations like Costa Rica, and we appropriately warn allies in the region about the dangers of these, and we usually hear the same thing—yes, we understand, but do you guys have anything on the table for us?

And what we tend to say then is we kind of diplomatically stumble over our tongues because we do not really invest.

I am very nervous about a recent statement of President Trump's reported last week. We do not need Latin America—that was widely reported. And then the foreign aid pause last week, which did not just affect programs in Latin America. It affected them everywhere.

But even setting those things aside, talk a little bit about what you are seeing in terms of Chinese influence in the Americas and how worried we ought to be about it.

Dr. HART. So the Americas is currently our primary battleground with Beijing. China sees our weaknesses there. They see an opening. They are showing up across the hemisphere.

I think the recent port opened in Peru is a perfect example. When we show up, we win, and one example—I would like to thank Congress and this committee for authorizing and appropriating the CHIPS Act which included \$500 million for the State Department to show up in Latin America and elsewhere and partner with nations to support U.S. based semiconductor manufacturing.

Senator KAINE. And just to use as an example, there was a chips plant in Costa Rica that had closed, relocated to China, but it is now back up and running in Costa Rica, and the chips portion of the CHIPS Act that involved incentives for allied nations to produce chips near shore if not onshore was a factor in that decision.

Dr. HART. And I would also like to add that that was a factor in Costa Rica saying no to Huawei and going with Western alternatives, because you cannot be a CHIPS recipient and have Huawei as your 5G provider. I am quite confident that this committee would rule as such.

And I would be remiss in my duty if I did not add there is substantial amount of counter PRC malign influence activities across the hemisphere that is currently frozen.

Senator KAINE. Please, Dr. Lind.

Dr. LIND. Thanks so much.

It is a really important question, and important to remind us of how vital the Latin American region is and is going to be in coming years.

We are in a superpower competition, and we remember the last superpower competition that we were in, the number of times that the United States was engaged in various activities in Latin America, and the number of times the Soviets were as well.

I mean, think about the Cuban missile crisis. So just the fact that we are in a superpower competition again should cue us to be thinking that Latin America and South America are going to play a much larger role.

I would say that from China's perspective, it sees the United States as very much operating in its back yard. We have bases there. We have strong alliances. We have the U.S. military flowing throughout the region, and so on.

So China has the perception that it wants to push the U.S. out and a very keen way to do that—a very clever way to do that is to start pressuring us in our back yard as, indeed, it is already doing.

Senator KAINE. What is the Chinese assessment of our response? I mean, they are pushing in our back yard, but to me it does not look like we are really responding in a forceful way. Is that how China sees it?

Dr. LIND. I could not tell you how China sees it, unfortunately, but I think that when China looks at our efforts, it sees both a very powerful adversary, capable, technologically advanced, an adversary that has tremendous assets around the globe and tremendous goodwill across the globe and in the region that we are talking about, in many ways.

So China sees that but it also sees vulnerabilities. And the vulnerabilities are many of which we have been pointing out today, and the vulnerability of the pause in foreign aid, for example, that is a—

Senator KAINE. Or a refusal to confirm ambassadors in the region. These are all kind of part of a fabric.

My time is over, so I yield back, Mr. Chair.

Senator RISCH. Thank you.

Senator Scott.

Senator SCOTT OF FLORIDA. Thank you, Chairman.

Let me continue with what Senator Kaine was talking about.

I am from Florida, so what goes on in Latin America is a big deal. We have a lot of people in my State that came from Latin America, and so they are following what is going on down there.

Not just—for sure the last 4 years but for quite a while the United States did not put a lot of effort into what goes on in Latin America, and as we have seen, whether it is Russia, China, even Iran, you know, they have—they have actions down there.

So it has been frustrating to get the Administrations to really focus on what is going on in Latin America, and hopefully, the next 4 years with Marco Rubio as the Secretary of State and Michael Waltz, because he is from Florida and he cares about it, as National Security Advisor we are going to see a change. Hopefully, that is what will happen.

I do not believe China is our friend. I believe the government of China has, clearly, decided to be our enemy. They want to destroy our way of life, and I think if we do not wake up it is going to be too late.

Mr. Mattis, in 2021 you wrote a piece in War on the Rocks explaining Communist China's long-term strategy and ambition. Giving that it is now 2025 4 years ago—4 years since, has your interpretation changed of Xi Jinping's emphasis on the great rejuvenation of the Chinese nation?

Mr. MATTIS. I would say, if anything, my appreciation for the clarity and long term thinking of the CCP and its focus on these objectives has, I would say, gotten sharper than I put in that piece.

Senator SCOTT OF FLORIDA. Do you think their ambitions are regional or global?

Mr. MATTIS. They are global. They have always been global. I mean, if you look at the way that Mao launched the Great Leap Forward, he was not talking about China becoming or the PRC becoming the world's or Asia's largest steel producer.

He was talking about it becoming the world's largest steel producer, and you can see from every leader from the CCP's beginning to the present that they have always seen themselves on the world stage and not simply a regional one.

Senator SCOTT OF FLORIDA. Mr. Mattis, the CCP has invested heavily in military capabilities to challenge U.S. influence in the Indo-Pacific.

I had the opportunity to go to the Philippines last year, I think it was, to see what they are doing in the shoals down there. How should the United States respond to these developments to preserve the ability to operate in this region?

Mr. MATTIS. Ultimately, this is a place where the—sort of the tyranny of geography and time requires us to work with allies and partners, and it requires us to make a greater investment in the number of platforms and ships and planes and drones that can be able to operate over those kind of large geographical distances.

Senator SCOTT OF FLORIDA. There has been a lot of written that China does not have the ability to execute, and so a lot of people say, oh, do not take them seriously because, you know, they are not very good at what they attempt to try to do.

Has that hurt us? Do you think there is a thought process out there that they cannot do what they are trying to do?

Mr. MATTIS. We have a logical fallacy in the way that we have analyzed the PRC, which is that we use what we think their capabilities are today to dismiss their ambitions for tomorrow, and in 1993 when the new strategic military guidelines were set out by Jiang Zemin in talking about fighting this kind of precision warfare in an information rich environment and being able to exploit that, it looked like science fiction for where the PLA was.

No one is laughing now about where that is. And what I find troubling is that when you look at a lot of analysis of the shortcomings of the PLA, is that we are quoting them talking about themselves.

I do not like that the PLA is a self-conscious and self-aware actor that is seeing its problems and trying to fix them, and they are talking about some of these problems in a way that we do not actually know what their level of capability is.

So just to take an analogy and say we are talking about a gymnast, every gymnast has some trouble with sticking the landing. But the difference with sticking the landing between a 13 year old

and with an Olympian medalist is a completely different physics problem, and it is something completely different. But it would still show up as there is trouble sticking the landing. We do not know where the PLA's actual capability in some of these things are.

Senator SCOTT OF FLORIDA. So, do you buy Chinese products and services and do you think Americans should?

I can start with you, Dr. Lind. Do you buy Chinese products and services?

Dr. LIND. I think nearly everything I am wearing and carrying is probably from China, and I think that is the case for many people here.

Senator SCOTT OF FLORIDA. Do you try not to?

Dr. LIND. No, not consciously.

Senator SCOTT OF FLORIDA. Dr. Hart.

Dr. HART. I have young kids, and so I pay a lot of attention to where things are made and what the quality is, and that means that we tend to buy more from the U.S., and that means, unfortunately, we pay more for it as well.

Senator SCOTT OF FLORIDA. Mr. Stoff.

Mr. STOFF. I echo Dr. Hart. I make great pains to try to avoid when I can, but it is quite a big challenge. But I take efforts to, yes.

Senator SCOTT OF FLORIDA. Mr. Mattis.

Mr. MATTIS. I am in the same situation as Dr. Hart, and I think it is important to pay attention to what you buy and where it comes from. We should not care more about where our coffee comes from than we care about where our T-shirt comes from.

Senator SCOTT OF FLORIDA. Thank you, Chairman.

Senator RISCH. Thank you, Senator.

Senator Coons.

Senator COONS. Thank you, Chairman.

Thank you to all four witnesses, and I apologize for my lateness in arriving to question. There is another confirmation—there is a confirmation going on in another committee.

I am particularly concerned about the possible expansion of China's influence both at home and abroad as a result of a freeze on our foreign assistance, and in particular the way it is being implemented and its cascading effect.

There is nothing China wants to do more than limit the reach of our global influence, than to reinforce their impression that we are an unreliable partner with countries throughout the world and particularly in the Global South, and my concern is that we put our security, our economic, and our diplomatic interests in danger with an abrupt pause that puts a halt to actions to counter malign activity by the PRC, to advance democracy, to invest in infrastructure.

Dr. Hart, you referenced in response to a question from Senator Kaine the importance of our showing up in the CHIPS Act. A bill that came out of this committee that President Trump signed into law—the BUILD Act—helped create the Development Finance Corporation. It has received robust funding and support from both President Trump, President Biden. I am hopeful that that will be part of our efforts to engage in infrastructure and in showing our influence.

In the previous decade the Belt and Road Initiative spent more than a trillion dollars on infrastructure projects to try and buy influence and curry favor for the PRC.

But this suspension of our aid so broadly implemented actually will not save money because the cost of shutting down and restarting programs often exceeds the cost of a careful review and then pivoting to more effective delivery.

And it may not be temporary. For many small contractors and organizations, many run by foreign nationals, they will not be around in 90 days. So I just want to ask you a few quick questions, if I could.

Dr. Hart, how do you think the PRC would be viewing this pause in our foreign assistance, and what impact do you think it would have for our pro-democracy work, both the IRI, the International Republican Institute, and the NDI, the National Democratic Institute, to have a 90 day freeze on their spending that would require them to lay off their employees, their contractors, and cease all activity?

Dr. HART. Thank you for the question.

You know, Beijing is viewing this as a blank check, a blank check to take the space that we are vacating to pursue their interests at America's expense, and frankly, this kneecaps the global human rights and pro-democracy movement.

I can share that, you know, frontline rights defenders and pro-democracy groups are closing their doors. NDI and IRI are shutting down globally. The U.S. has effectively abandoned the Hong Kong pro-democracy movement as the NGOs supporting that movement have all ground to a halt.

We have basically put a blindfold over the global apparatus that we use to track Beijing's rights abuses and hold them accountable. This is a blank check, and I am quite sure Beijing will seek to cash it.

Senator COONS. Mr. Stoff, one of the impacts of the domestic funding freeze was to put at question research—university research, medical research, research by literally tens of thousands of different doctors and scientists across the United States.

It has been temporarily paused, but it may well come back. What is the impact in terms of our credibility domestically and globally to have an across the board pause in Federal funding for research?

Mr. STOFF. Well, I think just to echo Dr. Hart's comments, whenever we do things like that, that provides more opportunity for China to come in, and this is already a problem set in terms of Chinese money and influence and a research ecosystem that is not really systematically tracked or understood at all.

And so if we are kind of stopping this effort, it does give China a lot more opportunity to come in and it also may give the opportunity to message around the world to our allies and partners that, oh, well, China has got the money. China can support this R&D. Maybe the U.S. is not as serious about it now.

So there can be secondary effects to this that we need to very carefully consider.

Senator COONS. I will say I appreciate Secretary Rubio reinterpreting the initial guidance so that it is broader. As some of my colleagues have pointed out, the actual impact on the ground in terms

of its impact—who is being laid off, what is being shut down—is broad and will echo.

When an organization like Freedom House that has long enjoyed bipartisan support, that has long been on the front lines of advocating for human rights and democracy, shuts its doors. when the IRI and the NDI shut their doors, I think China advances and we recede, and I think it is profoundly unwise.

Thank you.

Thank you, Mr. Chair.

Senator RISCH. Thank you, Senator Coons.

Senator BARRASSO.

Senator BARRASSO. Thanks so much, Mr. Chairman.

Mr. Mattis, if I could—for you, I want to talk about undersea cables. I mean, it is happening around the world, the threats and the sabotage.

We know that on January 3 Taiwan's coast guard intercepted a Hong Kong owned freighter after damage to an international undersea cable was reported. Taiwan alleges that the Chinese vessel cut the fiber optic cable by dragging its anchor across the seabed.

It is not an isolated incident there. According to Taiwan's national security bureau, over the past 3 years there have been seven or eight of these undersea cable disruptions. Most of the incidents can be held to the responsibility of vessels from China.

We are also seeing it in the Baltic. Our NATO friends and allies have had increased patrols to protect critical infrastructure felt to be related to Russia's activities in that area.

So while cable damage is not uncommon, heightened geopolitical tensions have raised suspicion of sabotage, and that is what I believe it is. So, what is China attempting to accomplish through these efforts?

Mr. MATTIS. So, if we are able to lay responsibility at Beijing's door, or in the—and probably that they were cooperating with Moscow on some of these operations, I think we should understand these as trying to right now test the response time of different actors to see what they can do, how long does it take to become repaired.

In some sense, I think this is an area where we should be looking at what is the state of the undersea cable industry—who repairs, who maintains, who can lay this cable, and what is the structure of their companies, what are those interactions. Because this is probably an area to keep the PRC out.

And then with respect to Taiwan specifically, it is a question of can they isolate Taiwan—can they cut it off from the rest of the world, can they create what they would call an information blockade so that Taiwan cannot function, cannot interact.

Senator BARRASSO. So, you detect, respond, and repair. And is there something technologically that can help us do that more actively or quickly? You know, how can countries better protect their underseas communication infrastructure from this potential sabotage?

Mr. MATTIS. I am honestly not sure what the technological solution is. I do know that this operates in kind of a legal lacuna in the way that international law functions, as you can see in the Baltic, when countries were having trouble figuring out what is the

justification to seize and search a vessel that had clearly done something.

Senator BARRASSO. Which leads to say what would be the role then of international organizations in investigating and trying to prevent these incidents?

Mr. MATTIS. I think it is a country level investigation. It is in international cooperation, and to the extent that there is any international organization that has a role, they should they should be involved.

And I think it is an important recognition for us that we have to understand that such an investigation only works when that organization has the integrity of its own processes, and I think everyone here could give you an example of an international organization where that has not kept that integrity, and it has led to problems.

Senator BARRASSO. Can I ask you a separate topic, which is IP protection, because some of the nation's strategic advantages that we have here come from our innovation, our technology, as well as our research and development.

And in about 2019 America's intellectual property was valued at almost \$8 trillion. China poses, I believe, a serious threat to our businesses and our academic institutions. The Chinese Communist Party consistently steals intellectual property, patents, other data.

In 2018 Chinese intellectual property theft was estimated to cost our economy over \$600 billion a year. No telling how much these numbers have gone up since then.

Is there leverage that we have here in the United States to help deter that threat?

Mr. MATTIS. I think one of the most powerful tools that we have is to deny the PRC a market because in some cases they are stealing the intellectual property, they are turning around, driving U.S. companies or other companies out of business, and then they are able to sell it on our market. And this is one of the key features that they are—that they need access to in the world.

This is what allows them to have the over capacity is the knowledge—the sure knowledge that they can sell those products from sort of ill gotten methods on a U.S. market, on a European market, and elsewhere.

Senator BARRASSO. And a similar topic, are there things that we can do better here at home to safeguard our intellectual property and our research from China?

Mr. MATTIS. There are many things that could do. As Mr. Stoff alluded to, we have whole categories of research that are not covered. We do not necessarily rigorously enforce some of the reporting and guidelines that are there and we do not necessarily require, for example, security training or awareness for people that are involved in potentially sensitive projects. I mean, we could go down a very, very long list of potential options.

Senator BARRASSO. One last question—I am running out of time.

Can you talk about any recent actions by China? What we have seen in their use of tactics against Taiwan that have taught us about China's capabilities and objectives that we might not have known?

Mr. MATTIS. I think if you look at the military exercises that have been launched around Taiwan, that you see an ability to operate more ships and more planes with less of a lead off time, which is sort of reducing our warning time, which when we think about the geography of East Asia, we have much further to go.

A second thing is that the National Security Bureau and the Ministry of Justice investigation bureau have made a number of arrests recently exposing sort of networks of CCP agents that are actually there to stir up trouble, to be in place for sabotage, and in some cases to instigate violence. And this is something that has been there, but if they are making arrests, this is a change in the scope and scale of that problem inside Taiwan.

Senator BARRASSO. Thank you, Mr. Chair.

Senator RISCH. Thank you.

Senator Shaheen, did you have a comment?

Senator SHAHEEN. I did.

Senator Barrasso, I wanted to point out that the only U.S. company that makes undersea cables is SubCom in New Hampshire, and I would bet they would be happy to come down and brief us on some of the challenges that Mr. Mattis identified and how they would encourage us to respond to those.

Senator BARRASSO. Thank you.

Senator SHAHEEN. So, I am happy to help arrange that.

Senator BARRASSO. Thank—no, I appreciate it. Thanks.

Senator RISCH. Senator Barrasso, you pointed out a brand new problem with China. I mean, we never heard of undersea cables being disrupted. Now all of a sudden we get one right after the other, and the finger always goes back to Moscow and China combining to do it. So, somebody is going to have to hold them accountable somewhere.

With that, Senator Van Hollen.

Senator VAN HOLLEN. Thank you, Mr. Chairman.

I thank all of you for your testimony.

I think you are hearing a common theme, at least from this side of the dais, that the Trump administration's freeze on security assistance and many other forms of assistance is a gift to Beijing.

And I have been listening by C-SPAN, and I think it is fair to say that we would agree that if we want to compete with the PRC for influence, we need to make sure that countries have a clear alternative based on our values and our competitive advantage as a nation.

You cannot beat something with nothing, and we have to be a reliable partner. But this freeze, which we do not know how long it is going to last, is already sending a terrible message to our partners around the world who are standing up for their countries' sovereignty against China's influence campaign. These are civil society partners.

It has also been noted that putting a hold and disrupting our security assistance sends a terrible message to our partners, whether they are Taiwan, Vietnam, Indonesia, the Philippines, Pacific Island nations, others in the east Indo-Pacific region.

These countries rely on that ongoing support, and cutting it off without notice, without a clear idea when it is going to resume, clearly puts us falling into China's hands.

Then there are the human rights defenders that people have talked about. We know about PRC's transnational repression of dissidents and how it has expanded, reaching dozens of countries. Both the State Department and AID provide urgent, lifesaving assistance to human rights defenders.

There is also the decision of the Trump administration to withdraw from the World Health Organization which, again, is a space that China will be happy to fill the void.

And we are also learning about this purge over at USAID, where dozens and dozens of civil servants who have qualifications in these areas are being summarily sent home and sometimes with pay—contractors without pay.

So I guess my question is as I sort of listen to the testimony so far, Ms. Hart, is—and I know Senator Schatz asked a version of this question—but if you are President Xi, right, are you looking to exploit this moment, and what would you be doing to exploit the moment?

And do you agree that what we have seen is really an unforced error and gift to President Xi and the PRC?

Dr. HART. Absolutely.

So, first, I would like to acknowledge and thank Secretary Rubio for the measures he has taken thus far. I would hope to see them extended to cover other programs including the counter China programs.

Basically, this across the board freeze has kneecapped America in the global competition with China. We have talked about how this silences and blindfolds our human rights watchers, giving Beijing a blank check to commit human rights abuses including forced labor abuses.

We have talked about, you know, the Taiwan military financing freeze, which gives Beijing a blank check to ramp up the coercion around Taiwan.

There are two others I would like to mention. Cyber assistance is frozen. We are giving Beijing a blank check to commit cyber attacks against some of our partner nations. State's CDP—the Cyber-space Digital Connectivity and Related Technology Fund—provides rapid foreign assistance to small countries that are being targeted with Chinese and Russian cyber attacks.

That is turned off. Beijing has a golden opportunity to go after networks.

And another one that has not been mentioned thus far is, you know, DFC over the past few years has been finally chipping in in outbidding Chinese companies, even Chinese state owned enterprises, in global infrastructure projects including ports and telecom infrastructure.

That is where we want to put Beijing on our back foot. But DFC is impacted by the freeze, and EXIM may not be directly impacted, but any company has to look at U.S. financing vehicles—any country has to look at EXIM and DFC and question how reliable they are.

So it not just kneecaps us in human rights, in protecting Taiwan, in resisting cyber attacks, it also undercuts our ability to outbid Beijing in ports and telecom infrastructure.

Senator VAN HOLLEN. Well, I appreciate that, and I know that there have been lots of discussions with Secretary Rubio, who was supported unanimously in the Senate.

There has been some clarification on the humanitarian aid front, that it is not just limited to emergency food assistance, other areas. But the rest of this freeze is still in place, and you have described the really terrible consequences.

So I hope we can end this sort of self—this forced error—our own goal here and get back on track.

Thank you, Mr. Chairman.

Senator RISCH. Thank you.

Senator Curtis.

Senator CURTIS. Thank you, Mr. Chairman, Ranking Member. It is great to be with you.

Before I begin my remarks, it is important to me to lay down some foundational principles that I believe all of us operate on, and I will just tell you personally I have great respect for the Chinese people, the Chinese culture, the Chinese history.

I just want to make sure none of this this morning is about any of that, but rather a dictatorship that is as hard on their own people as they are on other people.

So let me jump in. Today, I introduced a bill aimed at increasing pressure on Chinese—the way they address the theft of our IP.

IP theft is one of the top issues I hear back about in my district, small businesses to big businesses across the top, and I understand it is estimated that we lose about \$600 billion annually to this.

So, Mr. Mattis, to what extent is China's IP theft explicitly backed by the government as a state sponsored initiative?

Is it actively pursued by the government as a strategy, or does the government simply turn a blind eye as long as it targets Americans?

Mr. MATTIS. It is a policy that is backed both by the party and the state, and that party and state organizations are both involved in actively organizing people to conduct that theft, in creating—for example, one of the latest innovations is overseas innovation centers to fund partnerships, and this is a constantly sort of morphing problem that we cut off one avenue and another one pops up.

They are a creative and prolific adversary, if you will, in terms of finding the holes and trying to keep those things going, especially when they can exploit third countries that may not care as much about the protection of U.S. intellectual property and U.S. technology.

Senator CURTIS. Thank you.

Now, if I might, I would actually like to speak to my CCP handlers.

I know you are listening. I know you try to read my emails. I know you try to read my texts. I know you try to influence me back in my home State and my staff here in Washington, DC.

So I have a word for you. [Speaks in Chinese.] is not working. I am not intimidated, and I will continue to fight for freedom and democracy around the world, especially in Hong Kong and Taiwan.

Now, Mr. Mattis, can you help us describe a little bit what subnational influence operations are and the influence that targets people within a State, and how much of the goal is it to influence

State and local government, and how much it is to influence Federal officials?

Mr. MATTIS. The answer of whether or not it is also to influence the Federal Government as well as State and local is yes, because, I mean, think how many people in this chamber and in the Senate at large began their careers as town council members, as State legislators and others, because there is a natural progression and a natural career path that people hold.

And when you look at, you know, the attempt that was widely reported—a House member in the Bay Area, right—the Chinese consulate was targeting a number of different politicians in that area, and in your home State of Utah they have certainly looked for specific connections back to the PRC and looked for ways to shape government decisions.

And one of the other things that you can see there is it can be regulatory. You know, some States required a change in their laws to allow a Confucius Institute at those universities. That has occurred.

You can see it in terms of trying to push government procurement so that PRC products rather than from Huawei, from Lenovo, from others, rather than others that might be safer are put into government.

And I think anything that you can describe or that you have heard reported as being directed at a national government has been directed at a State and local, and the biggest difference is they lack access to the staff resources and oftentimes the knowledge to be able to push back effectively, although I think your State has the most robust private sector in trying to identify and push back on these threats.

Senator CURTIS. Good. Thank you.

I would like to kind of end where I began and just double down on this. Like, my goal is that we have a strong, productive relationship with China. We do not need to be at odds, but it has to be a relationship that is on the equal.

You cannot steal our intellectual property. You cannot take advantage of our businesses and expect us to have the type of relationship that we need to have for not just us, for them and for the entire world.

And so, thank you all. Thank you for this hearing, and I yield my time.

Senator RISCH. Thank you, Senator Curtis.

Senator Rosen.

Senator ROSEN. Thank you, Chairman Risch, Ranking Member Shaheen, for holding today's important hearing.

Thank you to all the witnesses for joining us today.

You know, with this Administration's disastrous decision to freeze almost all foreign assistance, we all know this hearing is a critical opportunity for us to highlight not just China's harmful influence but also the opening this freeze gives to the PRC to expand its foothold around the world, as many of my colleagues have already spoken about.

We would be naive to think that desperate countries will not turn to China to fill the gaps that our assistance has left behind. And so, with that in mind, I am going to move on to my first ques-

tion which is PRC investment in the Middle East, because in recent years China has deepened its ties with the Middle East.

For example, the PRC has spent billions on projects in the region including for infrastructure initiatives such as a high speed rail line linking the Gulf Cooperation Council countries, desalinization, solar plants, port modernization projects.

Meanwhile, the current Administration's foreign assistance freeze, which already has broad reaching impacts throughout the Middle East, threatens to leave a vacuum that the PRC can exploit for further influence in this critical region.

So, Dr. Lind, what are the practical—practical implications, practical effects, of Chinese investment in the Middle East? Specifically, I would like to hear more about how the PRC can leverage or might leverage its economic ties to advance its regional interests.

Dr. LIND. Thank you for this great question.

I think it is clear from Chinese activities in the Middle East that you describe—that we can see in China in its behavior there as well as in other areas of the world—it does have global aims.

It recognizes that this is an essential region for energy security, and for influence, and so China wants to have influence within that key region. So its actions tell us that pretty clearly.

Getting to the practical implications of this, obviously this is letting the United States know we need to be engaged in this region if we want to maintain the influence that we have had.

And then also on the theme of today's hearing, I think this is a region where we particularly see the risk of China's support for global authoritarianism. China is probably the world leader in technologies of authoritarian repression, and this is one realm in which it practices tremendous influence around the world, and in this region in particular, there is so much demand for what China is selling.

And by that I do not mean just Chinese technologies. I mean, certainly, Chinese firms but also Chinese government influence or Chinese government partnerships.

These are relationships that it seems to be sort of pushing on an open door between like minded societies in many ways: That some of these governments have an interest in acquiring technologies and methods and expertise in repression, and China holds that expertise and technologies and so on.

And so, those are, I think, among the biggest practical implications of its involvement there.

Senator ROSEN. Well, we have a lot of threats from China, the threat of—countering the threat of opioids, countering the threat of other types of competition.

But I want to move on to something in my last moment that has a Nevada connection. It is the lithium competition, because given the dual use potential economic importance of lithium ion batteries, securing a reliable lithium supply is a national security imperative.

Nevada is poised to be a global leader in this issue. We are home to the highest proven lithium reserves in the United States.

So, Dr. Hart, I am concerned that Chinese battery exporters—you think about other ways they can influence us, and we all like our phones. You know, people know about lithium from that.

But deliberately lowering the price of lithium ion batteries to undercut U.S. and allied manufacturers is a tactic the PRC has employed in the past.

So, can you talk to us about how we can weather this unfair practice and ultimately win the lithium ion battery race with China?

Dr. HART. Sure. So, where we have sectors that Beijing controls global supply chains—and we are working very hard to get alternatives online such as the projects in Nevada—getting those alternatives online is step one.

Step two, I suspect we are going to need something like a buyers club for these critical products, whereby the United States and key allies and partners agree to buy from each other, recognizing that we will not cut each other off.

Otherwise, if we have a completely open market, China will do what China has done before, which is dump product on the market to put these really important alternatives out of business.

So, getting them online is step one. For step two we are going to have to have some kind of multilateral arrangements or buyers clubs to encourage and incentivize companies to buy from Nevada instead of buying from Beijing.

Senator ROSEN. And would you think it is a good idea for the Department of Energy and the Department of Commerce to continue to fund the lithium loop that is in Nevada as a tech hub that will help us fight China?

Dr. HART. I think our national security may depend on it.

Senator ROSEN. Thank you.

Senator RISCH. Well, thank you very much.

I want to thank our panel.

Dr. Lind, you know, as we closed here you hit on a point that I think really deserves underscoring, and that is the fact between our cultures, and that is you were talking about the technology they produce for, really, controlling populations, and there is a real difference between autocracies and democracies in that here—we in the United States and other democracies we, the people, want to control our government, and those autocracies are in the exact opposite business, and they have a government that wants to control their people.

And it is a very, very different view of life from the time you get up in the morning until the time you go to bed at night, and that is the world we live in, and we are going to have to figure out how we continue to live in a world where we have such differences in our view of the importance of an individual human being.

So, with that, thank you for the panel. This has been a great panel that we have heard from today. We hear a lot of them over the years. We have probably as good an expertise here as I have seen on any issue that we have. So thank you all for participating today.

I am going to leave the record open for 24 hours to submit questions for the record. If we have some, I hope you will take the opportunity to include answers to those in the record.

So, with that, Ranking Member Shaheen, any final thoughts or—thank you.

Senator SHAHEEN. Just thank you to all of you.

Senator RISCH. Thank you so much. With that, the hearing is adjourned.
[Whereupon, at 12:24 p.m. the hearing was adjourned.]

