Center for Strategic and International Studies Holds China Initiative Conference

CQ Transcriptions

February 6, 2020 Thursday

Body

Center For Strategic And International Studies Holds China Initiative Conference

February 06, 2020 08:00 A.M.

SPEAKERS:

ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY JOHN DEMERS

DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION CHRISTOPHER WRAY

NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER DIRECTOR WILLIAM EVANINA

ATTORNEY GENERAL WILLIAM P. BARR

CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES TECHNOLOGY POLICY PROGRAM DIRECTOR JAMES LEWIS

DEPARTMENT OF JUSTICE NATIONAL SECURITY DIVISION DEPUTY ASSISTANT ATTORNEY GENERAL ADAM S. HICKEY

FBI COUNTER INTELLIGENCE ASSISTANT DIRECTOR JOHN BROWN

CSIS FREEMAN CHAIR IN CHINA STUDIES JUDE BLANCHETTE

KANSAS UNIVERSITY CHANCELLOR DR. DOUG GIROD,

UNIVERSITY OF TEXAS AT AUSTIN PRESIDENT DR. GREG FENVES

ASSOCIATION OF AMERICAN UNIVERSITIES PRESIDENT DR. MARY SUE COLEMAN

NIH DEPUTY DIRECTOR FOR EXTRAMURAL RESEARCH DR. MICHAEL LAUER

[*]LEWIS: Good morning. Welcome to CSIS. We have a very full schedule today and one thing we didn't know is that it's also National Prayer Day so the director is caught in the motorcade. He'll be here shortly. We're going to address the schedule slightly. First, the break is gone, sorry, but feel free to go out and get coffee whenever you

want. Second, I'm going to introduce John Demers who will tell you what the revised schedule is. The director should be here in about 15 minutes.

John has been the Assistant Attorney General for National Security since 2018, so it's been almost two years, right? He's the attorney general's lead on the China Initiative since November of 2018 and previously he was the Vice President and Assistant General Counsel at the Boeing Corporation. So--and also long experience at Justice, which I'm not going to read because it's too long. But John, please come up. Thank you.

DEMERS: Thanks. All right, thank you. Good morning everybody, thanks Jim, thanks to CSIS for hosting this and thanks for your patience. So we're going to flip things up a little bit. I think we're going to do Bill Evanina first as the threat briefing and the directors on his way. There's some blockades we didn't realize today, it's also National Prayer Day and so he got sort of caught up in the traffic.

It's actually consoling to realize that even the FBI director gets caught up in D.C. traffic, so--

(LAUGHTER)

--that's kind of nice. Well thanks a lot for being here this morning. As I think most of you know, we launched this China Initiative at the end of 2018 in response to a lot of the intelligence that we were seeing about Chinese malign activity; both on the foreign influence front and on the economic and political espionage front in our daily intelligence briefings. And the question from Attorney General Sessions, at the time, was what more can we do and how can we set this up? And the response was, this China Initiative.

When we set it up, we suspected that there would be many more cases for us to work and a lot more we would learn about the threat as we went along and, of course, we're going to hear a lot about that today starting with Bill Evanina who's going to describe the threat itself and then from our U.S. attorney panel, we'll talk about a lot of the cases and their activity within their district.

Now, despite the sobering nature of the threat, I hope you'll also take away some good news and that is, the significant steps that we're taking as part of a whole of government effort to hold the PRC accountable for its criminal activities and to push back against this economic aggression.

As you'll hear in our case overview, we're prosecuting a number of significant trade secrets theft in other criminal cases charged over the past year or so and as always, there are more in the pipeline. And while prosecuting criminal cases is our bread and butter, we've also leveraged a number of other national security tools including conducting outreach to educated colleges, universities and industry about the threats, applying the Foreign Agents Registration Act to unregister Chinese agents here in the U.S., reviewing and mitigating national security risks as part of the foreign investment review process and identifying and addressing supply chain risks through our participation in the inner agency team telecom process.

But even as we review our accomplishments, we should acknowledge that our work is far from done. We must settle in for the long-haul against the government that proposes a very different set of social, political and economic values from those of us in the West with Western liberal democracy and free markets.

The PRC is certainly settling in for this long haul in explaining Beijing's long-term ambitions, the parties policies highlight the year 2049 which you should all recognize as, of course, the hundred year anniversary of the--the PRC and the party as the time when China will, "Regain its might and re-ascend to the top of the world."

Based on the learns we've learned--best based on the lessons we've learned from the China Initiative, it's clear that protecting our technology is in our values. We'll require instituting a more aggressive and holistic approach. The approach will need to include our private sector, and I'm pleased that we have representatives of the private sector here today, our academia and we have folks from academia here today, our research institution and of course our allies around the world; I'd like to welcome those of you who are here from some of our nations allies, or our allies including the U.K., Canada, Australia and Italy.

At the end of the day, I hope you come away with a greater understanding of the challenges China poses. The departments approach to tackling this problem and a clearer sense of the way forward. Make no mistake on both the espionage, traditional espionage and economic espionage front, and on the foreign influence front, the threat from China is real, it's persistent, it's well orchestrated, it's well resourced and it's not going away any time soon. So with that, let me introduce Bill Evanina. Bill has been a wonderful partner. He's in the DNI's Office in the National Counterintelligence and Security Center. We have spoken together on this topic many times. He is one of the nations experts on the threat posed by Chinese covert activity here in the U.S. and so I'm very pleased to introduce my fellow Alexandria resident and friend, Bill Evanina. Thank you.

(APPLAUSE)

EVANINA: Good morning. Good morning. So I work for the government so we have to have a good morning. So thanks for the introduction. Again, thank you for CSIS and the team for being so gracious to host what I believe to be a transformational panel where we get to address threats and ideas in the construct of fairness, laws, morals that affect our nation not only now but in the future.

And let's start by saying I have never been so thankful to a prayer breakfast ever before. The fact that I get to speak before the FBI director makes me much more comfortable in this situation. Going after the FBI director and before the attorney general was not a good situation for me; so I'm excited now so hopefully you'll have more energy and I have to hurry up before the director gets here.

(LAUGHTER)

So, I think John talked about the solemn nature for which we are here to talk about and I want to just step back a little bit and explain the context a little bit from my perspective from a global threat ideology. So the president, on January 8, signed a National Counterintelligence Strategy for America. It's important to note that's the National Counterintelligence Strategy for America. It's not just for the government, it's not just for the intelligence and law enforcement community; it's for America. We're going to roll that out on a Monday so I'm not going to steel too much of that but I want to talk about the linear scope of that strategy which will now entail a whole society, whole nation approach defending what we believe to be our core values of America.

From supply chain to critical infrastructure all the way to foreign influence, one of the main pillars of that strategy is economic security and that's what we're going to talk about today and I'm really excited about--to bring a global perspective of what that economic security is and why it's so important to us as a nation.

That key pillar of economic security, before we get into it, I want to just level-set where we are. And you're going to hear a lot of comments today about the ethos of America and how it's different from the rest of the world; specifically with some of our adversaries; Russia, People's Republic of China, Iran, North Korea who are not democratic nations. We grew up, and if you're an American or you're a Western civilized nation, you grew up with a clear bifurcation between the government, the private sector and the criminal element. It's part of our growing up, our posture of a republic and a democratic society. That is not the case with the Communist Party in China. That is not the case with the Federation of Russia. It's not the case with Iran. So it's important to remember when we hear all through the day the concept of fairness, rule of law, morals and values; so keep that in mind.

So you're also going to hear about the threat, how it's permeated itself in the economic sector, the academic sector, research and development sector which we pride ourselves on with the concept of fairness; open sharing, collaboration, specifically in the economic environment. Let's move ahead. If I can figure this out here.

All right, so next slide, in reference to economic espionage in perspective of fairness. I'd like you to read this quote, and remember that Xi Jinping has one goal, to be the global leader geopolitically, militarily and economically and he and his Communist Party will stop at nothing to get there. We have an opportunity where I work to see the most classified intelligence that the world has ever seen and that is his senior most important intent.

So why does it matter? Why does it matter to America? Why should it matter to you this economic espionage, this economic security threat that we face? You see the official numbers up there but we're in the government, we're

probably closer to the FBI's numbers and White House's numbers with, let's just say, $400 billion a year in economic loss just from the theft, the proprietary data and trade secrets; just what we know, not including the existential loss that we see when technology, emerging thoughts and ideas or patented first in China and then sold around the globe at $0.30 on the dollar. We can't calculate that loss and that cost but it's mesmerizing.

We look at this slide, you ask yourself, does it matter? When the secretary of the Navy has concerns about a weapon systems performing because the supply chain penetration by the Communist Party of China, it's concerning. And when you look at the million, billons of dollars and you say, well what does it matter, if it's $4000 for each of us in here and our families per year after taxes, should it matter to America, should it matter to the American families the threat that we face economically from the People's Republic of China.

So you're going to hear today the China 20--25 plan. You're going to hear today about the theft of the intellectual property and trade secrets. This is jus a small graph laying out the paradox of the China 2025 plan and a listing of the investigational context with the FBI and DOJ and the priorities of the ministry of state security to acquire this technology and these buckets and the prioritization they have for obtaining this around the globe. You're going to hear today from the FBI and DOJ about cases that involve a lot of these key sectors. I will (INAUDIBLE) to you back to my original remarks; is this a governmental problem? Is this an FBI problem? Is this an intelligence community problem? This is an American problem. This is a CEO problem, this is an academic problem, the research and development problem, this is a whole society approach to what the People's Republic of China will do, stop at nothing, to steal. Stop at nothing.

This is a really important slide. I know we have a little technical difficulties here but if you say why does it matter, and you look at the prospect of if you were and American company, if you're a Western civilization company, a European company and you're working in joint ventureship or partnership with a Chinese company, you need to know and be aware of these laws that were enacted by the People's Republic of China last November. Just take a look at them, read through them, the red--you shall, shall. If you were a citizen, if you are a business entity, you shall cooperate with the intelligence services of the People's Republic of China. You don't have a choice; no choice. If you are, we're talking about technical, it's like a CISO, CIO position, you shall provide all your data, have all your data available for the Communist Party of China, (INAUDIBLE) state security. And we'll talk a little bit more later about how that manifests itself in joint ventures and sharing. In some of the cases you're going to hear from the FBI, not only are germane to the theft of intellectual property, outright theft either from a cyber perspective or an insider threat but oftentimes they're subsequent to an honest to goodness, believed to be fair, joint venture. Look no further than the Sinovel case; the semiconductors and the wind turbines. It's a very sophisticated concept that they use. But when you think about this, and if you're a Chinese national and you're sent abroad on--you're legitimately abroad working or educating yourself in the United States or Western civilization and you're called up in this aspect, what are you going to do? The law is the law.

So how does it work? Social credit score. Raise your hand if you're familiar with this? Okay, is this going to have an impact on the globalization of the economic world? I'd say it is. I'd say it is. Take a moment and understand here what this means. We've already seen impact, so we call it in the intelligence community, apology diplomacy, it starts with. When you have legitimate businesses in the U.S., Marriott, GAP, Delta who want to drive new global business with China and they do the right thing in their marketing campaign, for some reason it doesn't have the country of Taiwan on the map. Historically there's been an apologetic letter written by the CEO to apologize for the unbelievable infraction posed against Xi Jinping. Now it's becoming in a situation where it's going to be an impact on your ability to have business in China and be part of the China global economic engine.

I think all CEO's should be aware of this. All general counsels should be aware of this. All individuals who are tech startups who want to have a future in the economic prospects of dealing with, and investing in, and with people from the People's Republic of China.

So how do they do it? You're going to hear a lot about this from Director Wray and the FBI but we call this the wheel of doom, right? This is the unclassified version of what we see in the comprehensive strategic efforts by the Communist Party of China to obtain, legally and illegally, our proprietary data and trade secrets. If you look around that wheel you're going to see all kinds of legitimate and illegitimate opportunities to do that and you're going to

hear about that later today so I'm not going to get too in depth on how they do it. And the key word you're going to have to listen today, or phrase, is a non-traditional collector. You're going to hear that later. So it's really important to understand the complexity and the thoughtfulness that the People's Republic of China will utilize to facilitate your goals and needs.

We're going to talk about just about a few of these in a moment to give you a context but as we do, just keep remembering the colors of the wheel and what they look like and how they facilitate the--their work.

Some of the prioritization, oops, let me go back. Electrical vehicle technology. So there's probably 40 of these that we could talk about but I just want to pose a few with you to understand where we are globally. So the chart here on the right basically looks at, in 2040, the amount of electrical and autonomous vehicles in the world. You're going to hear me say this multiple times; they have a long-term view. If you ask yourselves, where does Tesla sell most of their cars? If you look down here, the FBI and DOJ, two Chinese nationals; Apple. Anybody here drive an Apple electrical vehicle? Just imagine if we did. Just imagine if that didn't occur? Not to put this on Apple but just imagine if Apple rolled out the electrical vehicle that did their iPhone. But because they haven't, think about all the manufacturing facilities in the U.S. that haven't been built and all the tens of thousands of jobs that haven't been developed, procured and filled to build these vehicles. That is the existential cost that we have with economic security.

If you look at this chart. If you're in the academic field, if you're in the research and development field, if you're a tech startup on the East Coast, West Coast, Silicon Valley, you need to be aware not only of what they've done historically but how they do it. The non-traditional collector. If you look on the left-hand side, you're going to hear more about this later from the FBI and DOJ. Harvard, Los Alamos but I want to be candid here for a second. We hear a lot of pushback in the government about this is a racial issue. Totally disagree. This is a fact-based issue of the theft of intellectual property, trade secrets and ideas by a communist country. On the left-hand side, two cases, Harvard, Los Alamos, are they Chinese nationals? Check your head this way; they were not. They were not.

So I don't want to really get into this discussion but I think we have to be able to be in a posture to have an honest discussion about what happens with the Thousand Talent Program and who they seek to recruit in our research and development academic institutions.

Let's take a look at this chart. We call this, how to steal an airplane. Read through the chart, understand from the first chart, aerospace, aeronautics is one of the priorities of the People's Republic of China to steal. Another word to say (PH), steal around the globe. This plane, as they built, the Comac C919 was their attempt to build their own airliner. With the long-term proposition, which I give them credit for to compete with Airbus and Boeing. But because they don't invest in a long-term or real organic research and development posture with the Communist Party in China, they seek to acquire the technology in other ways. And this chart lays out where they got all the parts of that airplane. So this is not just an American issue. This is a Western democratic issue, it's a world issue because a lot of countries on here have been victimized and a lot of these thefts have occurred in legitimate partnerships with the People's Republic of China that they believe to be honest, true and fair and either via an insider threat or supply chain penetration or a combination, the Chinese have left. Now, fortunately they rolled out this airplane in 2017, they're still having technical difficulties, but when you talk about the existential threat from an economic security perspective, eventually this is going to be rolled out. And for everyone of these planes they sell at half the price of a Boeing and Airbus airplane, 15 years from now, how many Boeing airplanes are we going to be able to sell around the globe when we're being undercut not dissimilar to the current Huawei situation. This is the long-term existential theft resulting in economic, I would say, unfairness and chaos moving forward.

Again, why does it matter? Take a minute to look at this chart. This is a chart we use a lot in the community for the CEO's. They say, why does it matter? I would--I would point you to 2010 and we're all in the business of having global equality with respect to development and trade and--and the globalization of market economy. But if you are a CEO and you look at the last ten years of growth with the Chinese economy and the top ten largest companies in the world, it's got to be disturbing to you. If you're an American entrepreneur, I know the Chamber of Commerce is not happy about this, U.S. Trade Rep, Economic Council, just take a look at the last decade and then extrapolate

that the next decade. In 2030, what does this map look like? We all have children, grandchildren, should be concerned. The long-term existential threat to the economic security of our nation is real.

So for you, if you're thinking about entering into a joint venture or partnering with any one of the Chinese companies or a company in China, remember back to the Chinese laws. But take a look at this map. Top 15 countries, companies in each country. Why are the ones highlighted in yellow? Because these are owned or operated by the People's Republic of China. Nine of the 15 there are banks in China. So if you merge this concept of government backed financing with the chart we saw before with the national security laws and you're going to merge or have a joint venture with a Chinese company, what advantages do they have that you don't have? They have state-backed funding to protect you and you have the opportunity to have the MSS, the PLA provide you all the intelligence you want on the--on your company. It's an unfair playing field.

We talk about Huawei all the time; 5G, why does it matter? This is a granular perspective of why it matters. When the People's Republic of China controls 50 percent of the global smartphone market, 50 percent currently. That's up 10 percent in the last two years. I'll ask a rhetorical question, does the People's Republic of China that administrate state security do--do they need a FISA or a court authorized warrant to get into those phones? Shake your head this way.

(LAUGHTER)

So 5G matters. I want to finish in my last minute to say the stakes are high and why are the stakes high? The economic security portfolio of our nation is on the presidents new strategy is not just about the great work the Department of Justice and FBI are doing; they are really putting the pedal down and the Department of Justice Task Force is really facilitating and providing the network for the FBI globally to do their job. But there's more too it than this. This to me is about ethos and culture, values and norms of the dem--democratic world that we live in. It's an unfair playing field that we are taking part in and you get to see that everyday but this is also a call to arms for all of society. If we are going to be able to be put in a position where we can effectively compete on a global market long-term, we have to look at our economic security as part of national security.

Thank you for your time and enjoy the day.

(APPLAUSE)

DEMERS: All right, thank you very much, Bill, and with thanks for his flexibility. I'd next like to introduce the director of the Federal Bureau of Investigations, Chris Wray. Director Wray has been the Director since 2017. He--I won't read his speech for him, he--look I--and I've been in this job for two years and in that capacity can attest to his utter dedication to the mission, to his thoughtfulness, to his dedication of the rule of law and to all that is best within the FBI.

And he has been a forceful voice at explaining and discussing the threat emanating from China. So without anything further, I'd like to thank him for coming and welcome him to the podium. Chris Wray.

WRAY: Well thanks, John, and I want to add my thanks to those of others (PH) to CSIS for hosting this event and for all you do to educate policymakers and the public. You just heard a pretty sobering presentation from Bill about some of the costs and the impact of this threat. I will tell you, from my lens, having been FBI director for over two years now, and having had to confront what I would argue is a wider than ever array of challenging threats. This one to me really stands out as the greatest long-term threat to our nations information and intellectual property and to our economic vitality and this is a threat, as I think you heard from Bill, not just to our economic security but by extension to our national security and I believe that to respond to the China threat more effectively, we need to better understand several key aspects of it. So what I thought I'd try to do is help further set the table for today's presentations and give you a little bit of a window into how the FBI sees the threat and how we're dealing with it.

The first thing I think we need to understand about the threat from China is just how diverse and multilayered it is. And I say that in terms of its techniques, its actors and in its targets. China is using a wide range of methods and techniques, and I'm talking about everything from cyber intrusions to corrupting trusted insiders. They've even

engaged in outright physical theft. And they've pioneered an expansive approach to stealing innovation through a wide range of actors including not just Chinese intelligence services but state-owned enterprises, extensively private companies, certain kinds of graduate students and researchers and a whole variety of other actors all working on their behalf. But it's also a diverse threat when it comes to the sectors and sizes of China's targets here in the U.S. We're talking about everything from Fortune 100 companies to Silicon Valley startups, from government and academia to high tech and even agriculture.

Even as I stand here talking with you today, the FBI has about a thousand investigations involving China's attempted theft of U.S.-based technology in all 56 of our field offices and spanning just about every industry and sector.

They're not just targeting defense sector companies, the Chinese have targeted companies producing everything from proprietary rice and corn seeds to software from wind turbines to high-end medical devices. And they're not just targeting innovation and R&D, they're going after cost and pricing data, internal strategy documents, bulk PAI, really just about anything that can that give them a competitive advantage.

They're also targeting cutting edge research at our universities. Just last week, for example, we announced charges against the chairman of Harvard's chemistry department for false statements related to a Chinese Talent Plan and a PLA officer at Boston University for concealing her military ties. In December, we arrested a Chinese researcher for smuggling vials of stolen biological research. Now, all three of those cases were just investigated by one of our field officers, one of our 56 field officers, the Boston field office, in about a month. So that gives you a taste of what we're dealing with. And you'll hear more about some of these cases later this morning but in sum, the Chinese government is taking an all-tools and all-sectors approach and that demands on our end our own all-tools and all-sectors approach in response.

The second thing I think we really need to understand about this threat is the scope of China's ambitions which are no secret. You heard a little bit about that from Bill already. To be clear, this is not about the Chinese people as a whole and it sure as heck is not about Chinese American's as a group but it is about the Chinese government and the Chinese Communist Party. The Chinese government is fighting a generational fight to surpass our country in economic and technological leadership. But not through legitimate innovation, not through fair and lawful competition and not by giving their citizens the freedom of thought and speech and creativity that we treasure here in the United States.

Instead, they've shown that they're willing to steal their way up the economic ladder at our expense. In recent decades, China has grown its economy rapidly by combining low cost Chinese labor with Western capital and technology but China's leaders know they can't rely on that model forever. To surpass America, they need to make leaps in cutting edge technologies.

Last March, at a Communist Party gathering, Chinese Premier Li made that understanding pretty clear. He said, and I quote, "Our capacity for innovation is not strong and our weakness in terms of core technologies for key fields remains a salient problem.

To accomplish the breakthroughs they seek, China is acquiring intellectual property from America and innovation by any means necessary. We see Chinese companies stealing American intellectual property to avoid the hard slog of innovation and then using it to compete against the very American companies they victims. In effect, cheating twice over. Part of what makes this threat so challenging is that the Chinese are using an expanding set of nontraditional methods; both lawful and unlawful. So blending things on the one hand like foreign investments and corporate acquisitions, with on the other hand things like cyber intrusions and espionage by corporate insiders.

Their intelligence services also increasingly higher hacking contractors who do the governments biding to try to obfuscate the connection between the Chinese government and the theft of our data. The Chinese government is clearly taking the long view here and in many ways that's an understatement. I would argue they've made the long view an art form. They're calculating, they're persistent, they're patient.

The third thing we need to remember about this threat is that China has a fundamentally different system than ours and they're doing all they can to exploit the openness of ours. Many of the distinctions that we hold dear and that are so engrained in the way we operate in this country are blurred if they exist at all in China. I'm talking about distinctions between the Chinese government and the Chinese Communist Party. Distinctions between civilian and military sectors or uses. Distinctions between the state and their business sector. For one thing, many large Chinese businesses are state-owned enterprises; literally owned by the government and thus the party. And even where not formally owned, they are legally and practically beholden to the government in a very tangible way. You've heard a little bit about that from Bill just a few minutes ago. And you don't have to take my word for it, you can take theirs. China, as you heard, has national security laws that compel Chinese companies to provide their government with information and access at their governments request.

And virtually all Chinese companies, of any size, are required to have Communist Party cells inside them to make sure that those companies stay in line with the parties principles and policies.

Try to wrap your brain around something like that happening in our system; you can't. Unfortunately, it's a similar story in the academics sphere. The Chinese government doesn't play by the same rules of academic integrity and freedom that the U.S. does. We know they use some Chinese students in the U.S. as non-traditional collectors of our intellectual property. We know that through their Thousand Talents Plans and similar programs they try to entice scientists at our universities to bring their knowledge back to China, even if that means, even if that means, stealing proprietary information or violating export controls or conflict of interest policies to do so.

And we know they support the establishment of institutes on our campuses that are more concerned with promoting Communist Party ideology then independent scholarship. We also know that they pressure Chinese students to self-senor their views while studying here and that they use campus proxies to monitor both U.S. and foreign students and staff. And last, we know that they use financial donations as leverage to discourage American universities from hosting speakers with views the Chinese government doesn't like.

So whether we're talking about the business world or the academic world, it is crucial that we acknowledge and understand these differences between our two systems because China is doing everything they can to turn those differences to their advantage. Obviously, they're exploiting our open academic environment for research and development. They're exploiting American companies openness for foreign investment and partnership and they're acquiring U.S. firms to gain ownership of what those firms have created.

Meanwhile, they take advantage of their own system being closed. They often require our businesses to put their trade secrets and our customers personal data at risk as the cost of gaining access to China's huge market. And they make American joint ventures operating in China establish those Communist Party cells within their companies.

This government control over our joint ventures has become so common that a lot of American companies don't even really stop to think about it. But if these companies want to protect their information, they sure better be thinking about it. They should also be thinking about what it means to operate in an environment where a major IT provider, like Huawei, with broad access into so much that U.S. companies do in China has been charged with fraud, obstruction of justice and theft of trade secrets. There's no reason for any U.S. company working in China to think that it's safely off limits.

So understanding the Chinese cal--counterintelligence threat better will help us respond to it more effectively. As I described, China is taking a multifaceted response so we've got to have a multifaceted response on our end. Our folks at the FBI and DOJ are working their tails off everyday to protect our nations companies, our universities, our computer networks and our ideas and innovation. To do that, we're using a broad set of techniques from our traditional law enforcement authorities for our intelligence capabilities. And you'll hear more about that in the panels later this morning but I'll briefly note that we're having real success and real impact.

With the help of so many of our foreign partners, we've arrested targets all over the globe. Our investigations and prosecutions have exposed the trade craft and techniques the Chinese are using raising awareness of the threat

and our industries defenses. They also show our resolve and our ability to attribute these crimes to those responsible. We've seen how our criminal indictments have rallied other nations to our cause which is crucial to persuading the Chinese government to change its behavior.

We're also working more closely than ever with partner agencies here in the U.S. and with our partners abroad. We've got a whole host of tools we can use from criminal charges and civil injunctions to thinks like economic sanctions, entity listings, visa revocations. We're also working with CFIUS, the Committee on Foreign Investment in the United States and its review of foreign investments and American companies that produce critical technologies or collect sensitive personal data of U.S. citizens. Bu we can't do it on our own. We need a whole of society response with government and the private sector and the academic sector all working together. That's why we, in the intelligence and law enforcement communities are working harder than ever to give companies an universities the information they need to make informed decisions on their own to protect their most valuable assets.

Through our Office of Private Sector, the FBI has stepped up our national outreach to spread awareness of this threat. For example, we're holding conferences for members of our DSAC, our Domestic Security Alliance Council where we share information with Fortune 1000 companies about China's continued efforts to steal intellectual property. We also now have private sector coordinators in each of the FBI's 56 field offices who lead our engagement with local businesses and universities.

We're meeting with these partners frequently, providing threat awareness briefings and helping connect them to the right people in the FBI on any concern. Our Office of the Private Sector also engages with a variety of academic associations on the China threat including the American Council on Education, the Association of American Universities and the Association of Public and Land Grant Universities.

Just last October at FBI headquarters we hosted an academia summit where more than one hundred attendees discussed how the academic community can continue to work with the FBI and other federal agencies to tackle national security threats on our campuses. All of this outreach is geared towards helping our partners take the long view and preventing our openness from being exploited.

In this country we value our open free market system including the way it attracts international investment and talent to our country. In this country we value academic freedom including international collaboration and the benefit we gain from having talented students from abroad, including China, come here to study. We're not going to change the way we are or who we are but at the same time, we've got to be clear-eyed and thoughtful about the threat from China and do everything possible to ensure a level playing field between our two countries.

So the FBI is encouraging our business and academic partners to keep that long view in mind when engaging with China. We're asking executives and boards of directors to carefully consider who they choose to do business with and who they make part of their supply chains. A decision to enter into a joint venture or contract with a particular vendor might look good to them in the near-term, it might make a lot of money today, might sound great on the next earnings call but it might not look so hot a few years down the road when they find themselves bleeding intellectual property or hemorrhaging some of their most sensitive data.

We're also encouraging universities to take steps to protect their students from intimidation or control by foreign governments and to give them ways to report such incidents. We're urging universities to seek transparency and reciprocity in their agreements with foreign institutions and to do their due diligence on the foreign nationals they allow to work and study on their campuses.

Finally, we're asking our private sector and academic partners to reach out to us if they see something that concerns them. And we're going to keep working to build trusted relationships with them so that they know, with confidence, that we're here to help.

Let me close by making one thing clear. Confronting this threat effectively does not mean we shouldn't do business with the Chinese, it does not mean we shouldn't host Chinese visitors, does not mean we shouldn't welcome Chinese students or coexist with China on the world's stage, but what it does mean is that when China violates our criminal laws and well established international norms, we are not going to tolerate it much less enable it.

The Department of Justice and the FBI are going to hold people accountable for that and protect our nations innovation and ideas. Thanks for having me here today.

(APPLAUSE)

DEMERS: All right, thank you very much. And--so next up we have Adam Hickey who's a Deputy in the National Security Division and oversees a lot of the cases that we have been talking about and that we will continue to talk about today and John Brown who's the Assistant Director for Counterintelligence and the Acting Executive Assistant Director for National Security at the FBI and a great partner in everything we've been doing and everything we're talking about today. So welcome them up to the stage. Thank you.

(APPLAUSE)

BROWN: Thanks Bill, I get to follow the director, so thanks, appreciate that. So--go ahead and start? All right. Good morning ladies and gentlemen, my name is John Brown and that is my name.

(LAUGHTER)

A little FBI humor to start the morning, right? So I'm the assistant director for the FBI's Counterintelligence Division and as you heard from the director and from Bill Evanina, we believe that no country posts a long--no country poses a greater threat than Communist China. Now, I'll tell you that I think the question before us is simple, over the next 30 years does the world go through Communist China or the United States? Who sets the standards? Fairness, justice, over the next 30 years. It's a simple question but each of us as America's have to be asking ourselves that.

As you heard the director say, the goal of Communist China is simple and to the point. It desires to be the world's leading super power by 2049 and do whatever it takes to get there. At the great expense of the United States and the American people. From our vantage point, the United States has not faced a similar threat like this since the Soviet Union and the Cold W--Cold War.

So therefore be--before we discuss the individual cases, I'll need a clicker here, before we discuss the individual case I'd like to give you an overview of the FBI's heightened commitment to defeating this threat. During my first year, I've got it right here-- During my first year as the assistant director we had witnessed an ever-growing caseload related to Communist China's efforts to conduct hostile intelligence activities targeting the United States. Today investigations related to the government of China make up a greater percentage of our counterintelligence workload then at any other time in the FBI's history.

Right now, as the director has mentioned, the FBI has approximately a thousand cases on economic espionage and technology theft and trying (PH) to benefit the Chinese government, Chinese companies and other entities in China. This graph shows a steady rise in such cases as shown in orange. Some of those cases involve talent recruitment plans, which as you heard the director, our Chinese government programs that often incentivize people to steal proprietary technology for the benefit of Communist China.

Technology theft cases are a critical segment within our China program but we investigate many other types of activity as well including traditional collection of my intelligence officers and co-optee's (SP).

With that, the FBI's devoting a significant number of agents and analysts to our counterintelligence investigations. We're also partnering closely with academia and the private sector. Of course with our increased case load we are achieving more disruptions than ever. This past fiscal year we arrested 24 people in counterintelligence cases and you'll hear some of that from Adam here shortly. Cases where the government of China was involved. The comparable number from five years earlier, it was 15 so the rise has been dramatic.

Right now we're only a third of a way through the fiscal year of 2020 and we've already made 19 China related arrests. So we're on pace to exceed last years number by a wide margin. Of course we're not seeking cases or arrests for the sake of numbers. The rising cases and arrest reflects a real-world rise in the threat, the threat from Communist China.

As the director mentioned though, we want to be clear about one thing. Our investigations are based on the facts, the law and proper predication and are usually concentrated on those intelligence officers, agents, co-optees, hackers and a variety of other actors working for the government of China; Communist China.

We are not focused on the Chinese people as a whole, as the director mentioned, we're focused on those committing crimes and conducting intelligence activities for Communist China. The mission of the FBI is simple; to protect the American people and uphold the constitution. We remain steadfast in our effort to protect all Americans from every walk of life. We welcome visitors, students and researchers from all over the world. We're committed protecting their ideas, their innovations, their patents. Our nations economic security is unequivocally linked to our national security.

We must protect those who come to the United States to make a better world for themselves, their families and all of us. We recognize that many people from China living in the United States face growing threats, intimidation and coercion at the hands of the Chinese government. Please know, the FBI is here to protect you. We are heard--here--here to ensure you can live the life you want to lead in the United States free from the watching eyes of the Chinese government, of the Communist Party. So with that being said, I will now turn it over to Adam. Thank you.

(APPLAUSE)

HICKEY: Thanks, John, and good morning everyone. So, when then Attorney General Sessions took the podium in November 2018 and launched the China Initiative, part of what he was doing was sending a call to action to federal prosecutors around the country and sending a signal that cases related to threats from China are a priority; that they're worth spending your nights and weekends on because the stakes of those cases are very high and the prosecutors and the Department of Justice did not disappoint. What I'm going to cover in the next few moments is just a sample of the cases that our prosecutors have brought in the last year and change and some of the lessons they have to teach us about the goals and methods of the Chinese government.

Before I touch on particular cases though, I want to make two points, or offer two caveats. The first, as you've heard both from Director Wray and Assistant Director Brown, the China Initiative is targeting the behavior of a foreign state; behavior that writ large poses a strategic threat to the United States. Individual cases are based on individual behavior. We begin with what someone does and from there a criminal investigation starts and often that behavior is brought to our attention by a victim in the private sector. The second point, many of the cases I'm going to discuss are pending and so the facts, as I described them to you, are allegations in our charging instruments at this point therefore they are just allegations. It is our burden to prove them beyond a reasonable doubt; we certainly intend to do so; that's why we brought the case but at this point they are allegations and the defendants are entitled to the presumption of innocence until we carry our burden in court.

All right, the first lesson I think we've learn from our cases is that there's a pattern that we see. There's a demand signal that starts in China that translates into an act of theft here in the United States. Three examples of that; one is the indictment against Huawei in Seattle. There, according to the allegations in the indictment, company executives were determined to obtain technology related to the testing of mobile phones, I this case, a robot that was used to automate that testing and so they determined that U.S. employees should steal it and if they couldn't do it, they would send individuals from China to do so.

At or around the time that this was happening, a memo goes out company-wide offering bonuses to Huawei employees for obtaining proprietary information and sending it to a secure email account. Second example involves two companies, state owned enterprise, Chinese student, state owned enterprise known as Fujian Jinhua and a Taiwan semiconductor company, UMC.

So in 2016 the Chinese government determines that there's a particular type of computer memory, DRAM, dynamic random-access memory that they need to become self-sufficient in and so they invest a great deal of money in that state-owned enterprise, Fujian Jinhua and establish a joint venture between those two firms.

The plan they have is that Fujian Jinhua is going to be the chef. It's going to actually cook the memory, it's going to create the memory chips and UMC is going to be responsible for providing the IP, the recipe that the chef follows.

The problem is that neither of those entities had the IP. So according to the allegations in the indictment in San Francisco, they set out to recruit employees of an American firm, Micron, poach them to the joint venture and have them bring and steal IP with them worth, we allege, $8.75 billion.

Third example involves a technology known as syntactic foam. Syntactic foam is a substance that has critical buoyancy properties, it has both civil and military applications. Again, China determines that it's a national priority to become self-sufficient in creating syntactic foam. So, a PRC company, CBMF (SP), establishes a U.S. subsidiary and sends someone who is also a professor, (INAUDIBLE) to the U.S. to run that subsidiary which, coincidently, is very close in space to an American company--oops, can we get back to whatever, wherever I was, if someone could make that happen, that would be great because there are a lot of buttons on here and I don't know what the other ones do.

(INAUDIBLE) sets up the subsidiary. It's funded entirely by the foreign parent company and he proceeds, according to the evidence produced at trial where he was convicted, he proceeds to poach employees from the U.S. competitor and as CBMI, the U.S. sub stands up its work, he begins to pitch the PRC military on what he's doing.

Second lesson, our private sector is in the crosshairs of intelligence services. They are using the same techniques they would use to target the U.S. government and that includes a mix of both recruiting insiders and computer intrusions. So beginning at the top right and moving clockwise, the allegations in the AP10 indictment are that hackers associated with the MSS targeted managed service providers for the purpose of breaching hundreds of their clients around the world and obtaining IP in breach of the 2015 commitment by China not to do so.

Second case, there were hackers on the outside of company networks but the MSS officers--I really have to stop that. There we go, are accused of using company insiders not only to get the malware on the victim network but also to monitor the companies remediation efforts so that the outside hackers were able to pull down tools and avoid detection.

Continuing over, we have another case in which an MSS officer is accused of recruiting employees to travel to China, grooming them under the guise of delivering a university presentation with the ultimate objective of obtaining IP from their employees down the road and the fourth case in the top left, an employee at an international airlines company working at JFK persuaded by PLA officers who leveraged her patriotism to smuggle packages on board commercial jets that would evade, therefore, diplomatic protocols and the like; other screening mechanisms.

Third lesson, there are certainly a lot of cases where we don't have evidence beyond a reasonable doubt that the Chinese government has procured or sponsored the theft but we see patterns where the theft is rewarded after the fact. There's a structure set up to encourage it. So you don't need the state to sponsor it at the frontend if the state rewards you at the end. A lot of those cases involve talent plans, plans established to recruit technical experts from around the world to come work in China and fill gaps they have in their capabilities, which, of course, by itself is not a problem except that, in a number of our cases, talent plan members are citing the information they've stolen, the trade secrets they have access to and claiming they should be rewarded for it or otherwise getting rewards on the backend for bringing the IP to China for the purpose of supporting a business there.

So, what are some of the lessons from the last two slides? Well, one is when you think about security in a company you have to be thinking both about cyber security and detecting insider threats. You have to have a holistic approach to it and second, if the PLA or the MSS is willing to leverage company employees for the purposes of theft, what would they be willing to do if the objective changes to something more disruptive? That has to be a concern and that is implications when we think about who providers should be, in say, critical infrastructure like telecommunications networks.

Second, with respect to the talent plans, that's a reason why companies need to have mechanisms in place to detect and have transparency when company employees who have access to sensitive information may have conflicts of interest; financial incentives to steal.

Now I've broken it. There we go. I think we're up to Lesson 4. Private sector is not the only target. Academia presents an attractive target as well because it is open in a way the private sector is not. Now, of course,

universities aren't in it for the money and they're not looking to profit, necessarily or primarily from their innovations but the cutting edge research done at universities, potentially has national security implications down the road and universities do care about getting proper credit for the innovative research that they do; attracting talented students, applying for funding based on the research that they did, preventing someone else from taking credit for it.

So this is a reason why the academic community needs to detect conflicts of commitment, conflicts of interest and protect against theft, not the same way that maybe the private sector does but in an analogous and an important way.

Lesson 5, is that the PRC is covertly attempting to influence public opinion and policy. One example of that is through what I'll call state media. CGTN America is the subsidiary of a Chinese media company. They recently registered under the Foreign Agents Registration Act. We approached them because we believe that they were under the editorial direction and control of the Chinese state and we based that decision, in part, on style guides and other guidance given to reporters as well as statements, some of which are quoted here, by Chinese officials directly to the media enterprise on what their responsibilities are.

My problem is not that Chinese television or CGTN has a message that comes from the Chinese government, the problem is if they are not transparent about the fact that they are related to the Chinese government or that that messaging is coming from a state, a foreign state, as opposed to say the reporters and editors here in the United States.

(OFF-MIC)

BROWN: So a--and I apologize, we're tag teaming this, we should have told you this upfront, right? So I apologize. In this slide I'd like to remind you that traditional collection of--by intelligence officers and their co-optee's is still a threat. For example, last year three people were sentenced to long prison terms for espionage-related crimes on behalf of the Chinese government. Even traditional espionage is evolving including the use of social media by Chinese intelligence services and so we continue to look hard at this threat and the thing I would say, and I'm--Adam will close it here, but one thing, my last comment is this, and I go back to what I said at the beginning, right, does the world go through China--Communist China or the United States in the next 30 years? We have been deceived too long. We have been deceived too long. I think we have woken up, I think we're taking the initiative, being aggressive, and I want to thank the DOJ in particular for--for doing that but we have been deceived too long.

Now, is the time for action. That action is together. As the director mentioned, a whole of society effort against this threat.

HICKEY: And so what that means is a concrete matter; it's--there we go. And I'll close quickly on this. Some best practices we recommend to the private sector. First among them, understanding what your assets are, what your intellectual property is. If you don't define it and tell your employees or others what it is and that they should protect it, it's going to be harder for them to do so. And I want to close with an anecdotes which I think sets forth what your goal is in the private sector. What you want in your company.

This is a story related to me during one of my outreach events. And it involved a Chinese national who was an employee of an American firm who was approached by someone, the intimation (PH) was that they worked for the government. And the request from that person was that that employee take a thumb drive and just put it in his computer at work at a certain point. The suggestion was that if he didn't do that, there would be negative ramifications for individuals at home.

Now, at that moment I think that employee faced a very difficult choice. This stranger had asked him to do something that seemed, you know, he could pretend not to know what it was, it was a simple matter, just plugging a thumb drive in and the consequences, much more concrete potentially for his family. So he could have just done it. He doesn't do it. He goes to IT and the firm, he tells them what he was asked to do and the company is in a position to take steps so that when the thumb drive is plugged in, there's no actual damage. The stranger thinks the employee did what he was supposed to do and it just didn't work.

I love that story because it exemplifies what your goal is. Your goal is to ensure that every employee in the company, or professors, understand the importance of security that we are protecting a shared asset and you want to generate the trust in your employees that they trust you, that they're willing to come to you when they see something, or approached, because they know you're going to do the right thing.

So as you establish policies and principles and protocols, remember that the most important asset that you have are the trust of the people who work with and for you and you need to be concerned about that, first and foremost. Thank you very much for your time.

(APPLAUSE)

DEMERS: All right, great. Thank you Adam and John. All right, next up we have our panel of distinguished U.S. attorneys who have been leading the China Initiative along with myself and Brian Benczkowski who is the Assistant Attorney General of National Security. I'll just introduce Brian briefly and then he will introduce the rest of the panel here. But I'd like to thank the U.S. attorneys, you know, unlike those of us who live in D.C. and just got off at a different metro stop today, they did come in from all around the country to be here. So I'd like to thank them for that.

Brian's been the Assistant Attorney General for the Criminal Division and my partner in crime for now almost the last two years. We were also partners in crime in prior administrations and with prior attorney generals. So, it's been a great pleasure for me to work together with him and with all the fantastic work that the Criminal Division is doing in partnership with the U.S. attorneys around the country on the threats we've been hearing about. So thanks very much, Brian.

(APPLAUSE)

BENCZKOWSKI: Thank you, John. It's a--it's been a pleasure to be your partner in crime as well and thank you for your leadership on this. And for all of you, thank you for joining us for our first panel this morning on the China Initiative.

As you've heard, the department launched this initiative in November of 2018 under the leadership of then Attorney General Jeff Sessions and it has been carried forward with great vigor and intensity under Attorney General Barr's leadership as well. And the Criminal Division has been proud to stand shoulder to shoulder with our partners in NSD a well as our partners in the United States attorneys offices around the country. And we have a great panel of very distinguished United States attorneys from around the country today. I dare say there aren't four more accomplished United States attorneys in the country then the four you all have in front of you here today.

Let me briefly introduce all four although they don't need much introduction and I'm not going to go into their bio so that we can get into the details quickly. But immediately to my right is Rich--is Andrew Lelling, the United States Attorney for the District of Massachusetts. Next to him is Jay Town, the United States Attorney for the Northern District of Alabama. Next to Jay is Erin Nealy Cox, the United States Attorney for the Northern District of Texas and at the end is Rich Donoghue, the United States Attorney for the Eastern District of New York. All four of these United States attorneys have been key players in the China Initiative and--and I wanted to give each of them an opportunity to give you all a summary of--of what their districts have been doing, to date, to achieve the primary goals of this important initiative and we'll do this a little bit out of order; we'll go ladies first and let Erin start.

NEALY COX: Well thank you. Appreciate that Brian. Thanks for having us here. So just to talk with you a little bit about what we're doing, I mean, as U.S. attorneys we were certainly charged by Attorney General Sessions at the time to start working on these cases with our counterparts in the Criminal Division and the National Security Division and to really partner very cohesively and effectively with the FBI to--on the investigations and in the counterintelligence realm.

In addition to that, I would say in particular in my district and elsewhere across the Southwest, we have been partnering with academic institutions and universities as well as corporate America to conduct talks and sessions in big cities and in small cities just to talk about the threat as we're seeing it which is something that the department hasn't been as much out front on until the China Initiative was launched and to really work with them to make them

more aware of the problem, which I think awareness, although simple as a concept, is a really important factor coming out of the China Initiative.

LELLING: Excuse me--good morning, I'm the U.S. attorney in Boston and so in Boston we have a high concentration of both academic institutions and sort of biotech startup type activity. So the China Initiative was very important to us from an enforcement perspective up there and we've sort of conceived of this as proceeding on two tracks which is, as Erin noted, the outreach side and then the enforcement side and these two compliment each other; meaning what we have found is that we do a tremendous amount of outreach to major academic institutions up there, we have Harvard, MIT, Boston University, others and it won't surprise any of you that there's something of a cultural divide between academia and law enforcement and so convincing academic institutions that there really is a problem has sometimes been difficult. The enforcement side helps us. Actually doing cases where you are publically announcing charges and you're prepared to prove them helps you convince the relevant organizations or schools that this really is an issue.

And we have found over time that we've been able to generate momentum this way and so it's important to us to do the cases, unearth this kind of activity, prosecute it, have a deterrent effect. It's more important to us, ultimately on the outreach side, to convince the schools to do their own--take their own internal steps to look at this issue, sensitize them to the problem so that going forward they educate their own staff, they're sensitized to the issue and so we don't have to do as many of these cases in the future.

BENCZKOWSKI: Jay?

TOWN: So, the five U.S. attorneys that are on the China Initiative, Boston, Dallas, New York, San Francisco, Silicon Valley, your economic sec--sectors of the United States, insurance industries, oil, energy and then--and then there's a guy from Alabama, right? Naturally you would--you would insert someone from--from the great state and--but--but what you don't know is that all around this country you get out of your major population centers and there is a great deal of R&D and development going on at universities in the private sector. Huntsville, Alabama, which is where I live, is in the Northern District of Alabama. It has every Fortune 100 aerospace company you can think of inside of Huntsville working on R&D, working on our natural defense systems, our propulsion systems to get to Mars, to get to the moon, to, you know launch drones and hellfire missiles at folks. I mean, we do all of that in Huntsville, Alabama. We have NASA and--and so it's important, and it's one of the reasons why I was asked to be on this initiative is because it does sort of ex--exemplify that that perfect soybean (PH) is being developed in--in Iowa or--or that thing is being developed in New Mexico or in Montana. And so, it--it's important in our outreach, it's important when we're talking to universities and to the private sector that we all understand, that we all have a great deal of proprietary information in our districts and our cities and our states. It's not just in those population centers.

And the point of that is, is that the targets then for the PRC are not just in our big cities, they're everywhere. And so that's--that's been part of our outreach, that's one of the things I've been working on a great deal with this initiative and--and--and it's great to be with my colleagues here today and with you too Brian.

BENCZKOWSKI: Thanks, Jay. Rich?

DONOGHUE: Okay, so similar to our colleagues, we're in the Eastern District of New York are primarily taking a two-pronged approach to the China Initiative. First is we're continuing and greatly expanding our traditional investigations of criminal prosecutions and with regard to any of the pending cases, obviously I would adopt Adam's caveat, about pending cases and--and the limitations in the caveats to keep in mind but we have, for instance, a Huawei case, not the one that Adam mentioned, the case they had mentioned is the Western District of Washington, Seattle case which is incredibly important, that's a good example of IT or, I'm sorry, IP theft prosecution. We have a related Huawei case in the Eastern District of New York dealing with a variety of things including bank fraud relating underlying to sanctions violations. And then we have things like Aventura case we announced recently which relates to supply chain security and cameras that were actually being manufactured in the PRC, mislabeled manufactured in the United States, shipped to New York and then sold to the government including some very sensitive installations within DOD and Department of Energy.

So it's sort of a reverse example of some of the things that we focus on. So instead of them taking IP and brining it to China, we see them bringing technology from China and the weeding it into our infrastructure to give them insight and advantage. We have other cases, I think Ying Lin was one of the cases mentioned as well. The handler at JFK who was putting packages on commercial aircraft, circumventing TSA and other procedures.

So we see a variety of criminal cases across the spectrum that we're prosecuting and our colleagues are prosecuting in the U.S. attorney's offices, we also have a significant amount of outreach through (INAUDIBLE) as well as DSAC, Domestic Security Alliance Council. We do that in conjunction with the FBI. I spent six years in a technology company before I had the opportunity to return to the U.S. attorney's office and I--I see the importance of that to those companies in academic institutions to have some insight into what is actually going on here so they can assess the risk that they are taking. So, a lot of things going on and I think going forward our efforts and the efforts across the department will only expand.

BENCZKOWSKI: Rich, let me--let me stay with you for a minute here. The initiatives top priority clearly is to prosecute economic espionage cases when--and where we find them (PH). Can you talk a little bit about how the investigation and prosecution of cases under the Economic Espionage Act differ from other types of national security and white collar crime and while economic espionage is, of course the focus, there are other tools that we have in our toolkits; so we can talk a little bit about both of those?

DONOGHUE: Sure. So, we have a lot of national security matters, investigations, etc., in the Eastern District of New York. We've had them for a long period of time as all our colleagues do. I think this differs from those more traditional national security cases because the threat is not eminent in the same way and it's therefore not as obvious, right? So if you take a more traditional national security case that we work, say a terrorist cell is planning an attack in New York. Everyone understands very quickly what that threat is and how to respond to it and you understand how the players fit into, perhaps, a larger plan or conspiracy and you're able to react to that. So you see kind of the whole threat at one point in time that you're able to react to that. Here because the threat is very different and very incremental, you don't necessarily focus on it and how it fits into a bigger picture and I think that's why A.G. Sessions really came forward with the China Initiative in November of 20--2018 to get us, as a department, to look more broadly at the threat and to understand what's actually going in to these efforts over decades, right? You heard about China 2025, the importance of the hundred year anniversary that's going to come up in 2049 and Chinese Ob--stated goals over these milestones and so it does differ from national security cases in that way.

In terms of white collar cases; you know, many of which are very significant and sophisticated and complex, the white collar cases you can usually follow the money. So there is a trail there to be followed and then you understand the scope of the conspiracy and the scope of the criminal conduct. Here, very often the perpetrators are taking things that are much more valuable than money. They're taking software code or perhaps hardware that they then use to dominate markets going forward. So while there's a lot of money at stake and we've heard about some of the--the estimates, $600 billion a year, it's not as easy to follow that because there's not necessarily money trail when someone puts software code on a thumb drive and walks it out of a company.

So, it is different from the white collar cases in that regard and it is more challenging. I would say the--the broad nature of the threat also creates challenges but also opportunities. We see PRC coming up in things like opioid, the opioid epidemic because so much Fentanyl is manufactured in the PRC and they have done some things recently to help with that in terms of scheduling (PH), but you see this threat manifest across the spectrum of the offices, cases and investigations and I know that's the same for all our colleagues.

BENCZKOWSKI: Andrew--thank you, Rich. Andrew, your office is very high profile case just last week charged a trio of China related cases; one of which is, folks have noted here today, involved a senior professor at Harvard. Can you describe what these soft-power influence efforts look like on college campuses today given the cluster of universities that you have in Boston then--and what should academic institutions be on the lookout for and how can they protect themselves from this kind of conduct?

LELLING: Sure, first these three cases last week I think illustrate a point that both Director Wray and A.G. Demers made which is the scope of the problem. So we charged three cases last week; one involving Professor Charles

Lieber at Harvard who is the chair of the chemistry department at Harvard and a pioneer in nanotechnology, which is not an irrelevant detail to his dealings with the Chinese. And he is not a Chinese national nor is he of Chinese decent. The second case involved a cancer research at a major hospital in Boston, was a Chinese national, stealing cancer research from that hospital, taking it back to China. The third, what we would call a traditional intelligence collector, as opposed to a non-traditional one, was a women employed at Boston University in polymer studies as a researcher who happened to also be a lieutenant in the People's Liberation Army but allegedly managed to leave that off of her visa application and her paperwork with BU.

And so these three cases, which are sort of three different flavors, give you a sense of how broad a spectrum there is in this area. Of these three cases, the Lieber case I think got the most attention and caused a certain amount of consternation in the academic community. And essentially the allegation against Dr. Lieber is that he had been recruited by the Thousand Talents Program, a program sponsored by the Chinese government, which is kind of brilliant in its simplicity and what it essentially does is attempts to induce researchers in the United States, whether they are Chinese nationals or whether they are not, to work with the Chinese and so instigate a flow of technology and know-how from the United States to China.

So Dr. Lieber was recruited by Wuhan University of Technology and then recruited by the Thousand Talents Program and, what we've alleged, is that he was being paid $50,000 a month to work with the Chinese and essentially transfer to them his know-how on nanotechnology on the atomic level which is obviously a cutting edge science. The core of the allegation against him is that he lied about this to federal authorities, including investigators from NIH and DOD when they asked him about it and that--that is a crime.

And so in light of that case a lot of questions we've gotten revolve around, well, is it illegal for academics in the United States to collaborate with their counterparts in foreign countries? And the answer to that is, no. And, again, this has caused some confusion because while that is allowed, lying about that activity to federal authorities when you're required not to is not allowed. And so the upshot here is that on university campuses what we have seen is that cases like this have generated a need for better guidelines for academia.

Even the members of academia who are not opposed to this form of enforcement ask not unreasonably, okay, well going forward, how do we avoid this problem? And that's a lot of the outreach that I've been doing in the last few months and now on an accelerated basis since we charged Dr. Lieber.

And so there are a few answers to this--this question, one, the primary goal of the China Initiative is to sensitize private industry and academic institutions to this problem. That's 80 percent of the battle. So, if the administration at Harvard, or whatever other major university institution we're talking about is aware of this issue and is disseminating that concern to its faculty, right there you've done a lot to deter this issue in the future. Maybe next time an academic does not lie about his connections to a Chinese program or maybe next time an academic or that institution thinks twice or thinks a little bit harder about heir collaboration with a Chinese institution and what the motivations of the Chinese institution might be. That's most of it. Beyond that, on the more nuts and bolts level, it will ultimately be up to the institutions to develop their own internal controls for keeping track of, if they choose to do this, what their faculty are doing on Chinese projects.

Now some will complain that this might have a chilling effect on collaboration with the Chinese. The answer to that is, for good and bad reasons, yes; it will. We are in the midst of a situation in which China has launched a massive nationwide effort to kill for U.S. technology and know-how and transfer it to China for its own uses and so unfortunately this kind of response is needed.

But to your point about other soft power influences, another aspect of the problem, and one that Director Wray touched on, is the Chinese governments very determined effort to control discussion of China on U.S. college campuses and increasingly even in K-12 education in U.S. schools. So there are Confucius Institutes on many U.S. campuses which are Chinese funded sort of Chinese cultural centers and the people who work there are under extremely strict controls about what they can and cannot say about the Chinese government.

More concerning to us, and we--we have leads on these kinds of cases in Boston, is agents of the Chinese government, and I--I mean, literally agents of the Chinese government, come to the United States to exercise sort of ideological control over Chinese nationals who may be operating completely in good faith who are here to study, to learn at our schools or work at our institutions and we have seen indications of Chinese agents coming to the United States to cajole or intimidate other Chinese nationals who are here to make sure that their targets do not say negative things about the Chinese government and, in fact, only say positive things about the Chinese government. And so what you see is the Chinese government taking advantage of the openness of U.S. society to make this kind of propaganda headway on our own soil; which is extremely concerning and has led us to try and think of creative ways to, frankly, prosecute some of these people who have come over here with that intention in mind.

So, I'll pass it back to you.

BENCZKOWSKI: Thanks, Andrew. Jay, as you mentioned in your opening remarks, you and your office have been active in conducting outreach to industries and institutions, companies, that are potential targets. What have you seen in terms of the challenges that we face in getting our message out to universities and companies in Alabama? What's working and--and--and where have we faced headwinds?

TOWN: Well, one of the things that we identified early on, we--the China Initiative is that it was important that we develop sort of a suite of things for all of the U.S. attorney community, all 93 of us, to be able to go out into our universities and private sectors and--and give some sort of overview of the threat that the PRC poses to their district. Every district is a little bit different, every--but every district probably has a military base, has--has a university of some sort and some sort of economic sector. And so the--and the technology that drives that sector. And so we developed not only, you know, PowerPoint presentations, you've seen a lot of those slides today, already, but also the talking points and making sure we get the word out with--with op-eds, with--with the sort of appearances in the media, in--in one form or another; one platform or another.

And so that was important that it wasn't just the--the--well, the four of us, but the five of us, AAG Benczkowski and Demers, it can't just be us doing all the lift. The--the whole of government approach has to include all of our United States attorneys, of course General Barr and General Sessions have been leading the way on that as well.

And, you know, one of--I have--I have a friend who is the general counsel at a major pharmaceutical company and we--we often sort of quip about how that first pill costs $10 billion to--to create and manufacture and to be efficacious. The second one costs $0.02 and the--the--the illustration is that the Chinese government only wants to pay $0.02. And that is sort of--sort of the message when you put it in sort of those terms, that is exactly what the China Initiative is countering but that is also the threat, the national security threat, that the PRC is posing to the variety of our economic sectors. You saw the--I think it was the wheel of death that you referred to. It--it--it is every--it's agriculture, it's--it's IT, it's not just national security and aerospace and the things that we typically think of when we talk about national security. It's every sort of aspect of our--of our economy. And so what we've done is I've--I've gone out and personally, and I know that--that these folks have too, gone out and done major sort of CEO summits for a multitude of--of CEO's and CFO's and COO's in my--in my community both in Birmingham and Huntsville and from around my district.

I have done it for university systems, in my district, as well. And then we have done some private outreaches that, you know, that a company might not want to show up at the big thing and ask a question in front of all of the other CEOs.

But, hey, could you come and sit with my C suite folks and give us the same briefing? And, we are happy to do that. And, we usually bring the FBI, we have some intelligence community folks, down in Alabama, as well. Naturally, right? And so, we, you know, we bring them along so that we--we remind our corporate sector and our academia that frankly, we can keep bigger secrets then there has been some sort of cyber intrusion into your company.

And so, if you enlist our help and our resources, we can be of great benefit. To one, ensuring that that does not happen again, to you or to others. But, two, perhaps getting into the criminal prosecution business that my colleague was just speaking about. And by the way, Andy Lelling has never had a case that was not high profile.

(LAUGHTER)

I have known him for three years, and that is pretty much so-- yeah, yeah.

BENCZKOWSKI: Thanks, Jay. Erin, as folks have noticed here these China-related cases arise in a surprisingly wide range of districts. We have, who--as Jay said, who would have thought we would have northern Alabama here. But what kind of resources, are you available? We are grateful that you are here.

(LAUGHTER)

Now, it gives a sort of a gee-whiz moment, not a, why are you here moment? Erin, what kind of resources are available for your fellow U.S. attorneys to prepare for cases involving Chinese economic aggression? And, what do you think that we could be doing better, to equip our prosecutors, to handle these cases?

COX: Well, you know, I think that we have really focused on working with our counterparts, our National Security Division, Crim Division, all of the U.S. attorneys across the country, like Jay said, the 93 of us. To number one, make sure that we are aware of the research and counterintelligence out there, to make sure that we have the latest briefings. But also, to make sure that we are aware about the enforcement cases that are going on across the country.

And to be able to use those cases in some of our outreach efforts. I mean, I think that that is something unique that we need to be able to do. We need to be able to point to cases and talk about factual situations, that are applicable to companies and to citizens that are in every district.

And, I think that we have really had a good opportunity to do that, collect those cases, talk about them. And, a lot-- you know, there is a great deal of interest across the U.S. attorney community, not only for the enforcement nature of the case but also in being able to better arm their counterparts and colleagues and big companies and across academia, just to give them, sort of, some hard factual data, so that they could be aware of it.

It is not, you know, we are certainly not talking about the what if's, this could be, and engaging in hyperbole when you hear about some of these cases. There is a distinct and stark realization, that what the FBI has been saying for some time now, is actually happening in the country. We are going to be prosecuting it vigorously.

So, we have been arming them with a lot of good information. Certainly, you have seen, likely some U.S. attorneys across the country that have written some opinion pieces and have gotten those published in papers, so that we can effectively talk about it, on a larger basis, as well.

And then, you know, the National Security Division and Crim Division have been working with our offices to, to give them, you know, speaking materials and intelligence briefings, from the FBI. Just to be better equipped to talk about the latest things. So, I think, you know, we have taken, you know, we certainly, consistent with director Ray's admonitions, we have taken a whole U.S. attorney community approach, to this threat.

It is that important to us. It is that significant to us, to talk about it. And, to engage in pretty vigorous prosecution of these cases.

BENCZKOWSKI: Thanks, Erin. There are a couple of additional questions. I will throw it open to any of the panelists who have thoughts. One question is, are there additional legislative or regulatory steps that we would recommend that the United States should consider, to allow us to more effectively address, these particular issues?

LELLING: I have one thought on that, which is on the academic side, which my office has been focusing on a lot. I do think that it would be in the public interest for grant-making bodies, that give a lot of money to academia, DOD, NIH and there are others, to establish their own kinds of guidelines and guidance, for the academic community, to sort of, alleviate some of the concern about not knowing where the navigational buoys are anymore.

If you are in academia, there is that feeling. And so, I think that would probably be a helpful step, for the government to take.

TOWN: I think that, so--we have all heard, in this town anyway, of the Foreign Agents Registration Act, and that really only applies to political activities, as it relates to foreign governments. And, with the billions of dollars that we are, as Andy was talking about, you know, granting to academia, and investing into R&D in the private sector, through DOD and other departments.

I do think that it would be important to at least have, sort of a point 1, where it does apply to not just political activity but perhaps it would apply to research activity and some other things. And give some real teeth to what we--what the President and what this Justice Department is trying to accomplish, with prosecuting these individuals that are taking these grant monies and perhaps using it for nefarious purposes.

BENCZKOWSKI: Do any of our panelists have any thoughts about what we might do, in terms of additional, international outreach efforts, to strengthen our hand here? Obviously, our outreach to China, is probably unlikely to serve much in the way of that purpose but are there other, in your views, things that we can be doing internationally to help with this problem?

DONOGHUE: Brian, there are a number of things underway already and they will continue to expand as we go forward. As Andy indicated earlier, we have one of the Huawei cases currently pending and that case will continue but you could do an entire conference on Huawei, right?

As an example of how this operates in the real world. But I think that we need to continue to have very frank discussions with our partners around the world, about the nature of this threat. I think that is ongoing now. Obviously, you know, almost not a day goes by when you don't look in the Wall Street Journal, the New York Times, Washington Post, whatever, and see articles about Huawei, consideration, and discussions around the world, about the role that that company should play.

Particularly, as we go forward into a 5G environment. But it is good that we have discussions and it is good that we are given the opportunity, around the issue, to discuss what is really going on here. I think that, in addition, we should have very frank discussions with China. We have been very clear with them about our perceptions of their efforts and how we are going to respond to it.

And, how we are simply not going to enabling their efforts to undermine our national security. So, it is important that we have these discussions, both with allies and with adversaries around the world. And, I think that you could see that continue and expand, as we go forward.

BENCZKOWSKI: Several questions from the audience, many of which we will not be able to get to, but I think that this is a good one. And based on your--each of your experience in outreach to the business community, in your particular districts. The question from the audience is; what would it take and what do we think that it will take to get U.S. businesses and their trade associations and others, to be willing to speck--to step up and speak a little bit more publicly, on their own behalf, about the threat that they face?

There is a perception, at least by the questioner in the audience, but I think that it is probably accurate, that many are in the business community are unwilling to speak out and discuss this threat openly because of fears about retribution. But do you have any thoughts about what we might be able to do to encourage that discussion and encourage the business community, in particular, to acknowledge the threat?

COX: Well, you know, this comes up quite often in the discussions that I have had with those that are C level executives, as well as, you know, those that are working in important aspects of their businesses. There is a general disinclination to; number one, believe that this is actually going on at the level that it is going on. And two, that they would actually be a target of this kind of state-sponsored economic espionage.

That is why it is helpful to have the cases to talk about. I mean, ranging from, it is not just obviously technology, telecom industry or defense industry, it is almost every industry in America, the idea is in any way and in every way that they can gain a competitive advantage, they will.

And I do think that the cases make a difference. It is reminiscent of, you know, when we started seeing a lot of cyber intrusions and a lot of media exposure to data breaches. Where people were not thinking that they would ever be a victim of a cyber intrusion and now that is in our common, everyday vernacular.

I think that those cases really exhibit to them this could be me and I really need to start paying attention to it. Also, I do think that in our discussions, one thing that may make them more comfortable and has made them more comfortable, the business executive or the employee, is knowing that they do have, you know, someone in the FBI who is very sensitive to these things, understands the threats, understands the inclination of the employee to be fearful about retribution, the inclination of the company executive to be fearful of retribution.

And we do not approach it in a sort of storm in and take over the type of situation. We are sensitive to these things. We understand the ramifications, the real-world implications of these kinds of things. And I think, from my part--my point of view, that really makes a difference when you can walk through specific examples of how the FBI and the United States government has dealt with these things. Sometimes very quietly, and sometimes very loudly.

BENCZKOWSKI: Another good question from the audience, and a related question. In your outreach to universities, have you sensed resistance to cooperation, particularly if the University is engaged with China, Chinese entities, or receives funding for their graduate students? Have you felt that resistance? And what have we been doing to try to overcome it?

LELLING: I can give you a quick example from Boston. I think that, and I alluded to this earlier, one of the very important aspects of actually bringing cases, actually putting points on the board, is that when you go and talk to the universities, the more likely they are to believe you that there is actually a threat.

And so, what I have experienced in the Boston area, is that initially, there is resistance from the universities, from the viewpoint of whether they believe that there is actually a problem. Once you are able to get them over that hurdle, they are actually quite responsive. And so, we have gone to universities and we have initiated conversations and their concerns are not unreasonable ones.

Their concerns are, you know, are you just being paranoid because you are in the federal law enforcement? Is this actually a problem? Are you racial profiling? These are all questions that come up. We deal with them. Once we are able to convince them that this is an existing threat that impacts their campus, then that is fine. Then I have found that the universities are quite responsive, very responsible.

They are willing to convey information to us to help us along in our investigations. There are things that they need on their end. A certain degree of discretion. A certain degree of input on how these things proceed. But I have actually not seen a problem.

DONOGHUE: Yeah, just to echo what Andy said. I think that that is absolutely right. You mentioned earlier that there was a bit of a cultural divide between academia and law enforcement. And that is certainly true. But that's an initial reaction. If we can get past that and explain to them what is really going on, I think that they are appreciative and responsive. You know, in a lot of ways, part of the cultural divide is because academia flourishes on collaboration, as it should.

And so, when you look at technology development and you look at people trying to take advantage of other's technology development, what becomes the weak link here? It is academia. Because people coming in and out of labs at universities, they want professors and students to come from other countries and that is beneficial for everyone.

But they don't have the same type of safeguards in place that say, a technology company would, that's invested millions or billions of dollars, in this research. And, has an infrastructure to secure that research. Academia is much more loose in how it secures these things. And, that emphasis on collaboration tends to leave them vulnerable.

But when you explain the vulnerabilities to them, I think they are very receptive. And I think, particularly, with regards to the grant process, academia is very interested in this and should be. If you are in an academic institution,

and you are not thoroughly scrutinizing the grant applications you are putting in and the grant that you've already received, you are committing administrative malpractice.

They really need to take the time to look at their representations that they are making to the U.S. government and other grant agencies to ensure that their own personnel professors and otherwise, are accurately reporting what financial or other support they are receiving, from other entities. So, they really need to focus on the grants right now, and as we have seen recently, with the work in Andy's district and elsewhere, that is an incredibly important component of this effort.

BENCZKOWSKI: I was told that we have until 10:00. We may have a little bit longer than that. But I wondered if each of you could give us a sense of where we go from here, from your perspective? What do you see on the horizon, heading into your offices in the coming year? I imagine you may have similar views about what we are going to do next. But if you guys each want to offer a few thoughts about how you think the initiative will continue to operate and flourish and grow in the next year or so.

LELLING: I can say from the Boston perspective, my hope is that my prediction is that, these cases will spike at some point and then begin to trail off. Hopefully, as industry and academia become more sensitized to the problem. I can tell you that for the coming year in Boston, what I anticipate, frankly, is prosecuting more people. Which I think will help to deter this kind of conduct in the private and academic sectors.

And, I think that we will couple that with outreach. Later in the year, we anticipate doing some kind of national conference, on the China issue, to sort of try and raise the profile even more and take advantage of the publicity of recent cases, in this area. I guess this is what I see, in my neck of the woods.

TOWN: Just like anything else, that is incredibly complex and sort of involves a holistic approach, for solutions, the situation with the PRC and the China initiative, is no different. And so, I think the more that we talk about it, you are all here at CSIS, today, to hear some wonderful speakers and talk about the issue but also, to engage with us on these panels. So clearly, you have the interest, as well. I think our goal is to swell audiences and have more audiences like this one, so that this does sort of, enter our common lexicon when we are talking about, not just economy, but also national security.

And it is just sort of repetitive in our national lexicon such that we can continue to have conversations like this, five, ten, twenty years from now. As Rich said earlier, you know, China's goals with their, you know, their 2025 and 2049, you know, they are not going to quit just because we have had a successful year prosecuting folks or when we see that spike and it starts to go down. The Chinese are playing a long game and so we need to match that with our own wits.

COX: Well, I, of course, echo those sentiments. The only thing that I would add is really that I see us cooperating with some of our other government agencies, such as Commerce and Treasury, and really kind of ramping up a holistic approach, from the federal government, so that we can address the cases that we already have, more effectively, and address the threat more effectively, from an outreach point of view.

DONOGHUE: And I think that as Andy said, you will see an increase in prosecutions, not just of individuals, but of companies. And that opens a whole new avenue of discussion, right? Because as with any company prosecution, you cannot incarcerate a corporation. And so, what is the right result, to a company prosecution?

You may want to punish them; you may want to deter them. But particularly when you are looking at a threat that is going forward, really for decades, the right resolution to those types of criminal prosecutions has to do with mitigating a threat and it has to address mitigating that threat. So, I think that you are going to see some very interesting prosecutions coming forward across the department, across the U.S. attorney community.

And, I think that it will challenge our international relationships and structures and norms and I think we will get to a period where there will be a new normal; that would be based upon a more thorough understanding of what is going on and a more clear-eyed assessment of the interest in conflicting interests of different parties. And, I think that that is good.

Because I think that the backside of that, is that it will actually lessen the chance for conflict going forward, because what has been going on for the last few years is something that I think that John Brown noted, we have been late to become aware of.

It has put us on the road to conflict. And if we address it now, and we address it effectively, through prosecutions of individuals, prosecutions of companies, outreach to academia and the technology industry, I think in the long term, that lessens the chance for conflict between the United States and the PRC. And that is actually, a good thing for all of us.

BENCZKOWSKI: I think that we have reached the end of our time. I hope you all appreciate and found this panel informative. These are four United States attorneys among many, but certainly, four of the key leaders in the department, who are really at the forefront and the tip of the spear, on this initiative. So, I want to thank you all for coming in from your various districts, around the country, to participate here today. I think that this was very informative and very helpful. So, thank you very much for all of it.

(APPLAUSE)

LEWIS: Okay, are we set? Well, good morning. Thanks for staying and for what has been so far a really good session. I suppose our next speaker needs no introduction-boy, there's an old one for you. But I will say that William Barr was confirmed as the 85th Attorney General, by the Senate in February of last year, so it has been almost a year.

We are doing this on your anniversary, great. He is one of the only two people in U.S. history to serve twice as the Attorney General. Previously in the George H.W. Bush administration, he was the Executive Vice President and General Counsel for GTE and then Verizon. So, very knowledgeable on telecom issues. And prior to serving as an attorney--as Attorney General, he was at one of the law firms here in D.C., one of the big ones. So, without further ado, Mr. Attorney General.

(APPLAUSE)

BARR: Thank you, Jim, and thanks for the introduction. And thank you for hosting this event. I appreciate all of you taking the time to come here and participate. It is good to see my coll--so many of my colleagues from the department participating. You know, my original career goal was to go into the CIA as a China specialist and therefore I spent six years at Columbia getting a B.A. and M.A. focusing on Chinese studies.

And I remember in one of my government classes, we were having a debate, and this was in the early '70s, and we were having a debate as to which of our foreign adversaries would pose the greatest long-term threat, to the United States. And the question was whether it was Russia or China. And I recall the observation of one of my classmates, who was arguing that China posed the greatest long-term challenge to the United States.

He said, Russia wants to conquer the world, we can deal with that. China wants to own the world, that is more difficult to deal with. And there is a certain truth in that. In 1972, our hope was that integrating China into the international economic system would encourage the PRC to liberalize its economy and that a freer market and economic growth would gradually lead to greater political freedom for its citizens.

Unfortunately, economic liberalization has only gone so far. While individuals have been permitted some degree of economic freedom, the Communist Party remains in firm control of the economy. It is an architecture of state power, whose principal features are central planning, state-owned enterprises, and government subsidies.

Politically, the PRC remains a dictatorship under which the Communist Party elite, jealously guard their monopoly on power. Marxist-Leninism and Maoism linger on, primarily as a justification for communist rule. Which is authoritarian through and through.

The Communist Party is willing to resort to harsh measures to repress any challenge to its one-party rule. Whether it is suppressing religion, rounding up and reeducating Uighurs, resisting efforts at self-determination in Hong Kong or using the great firewall to limit access to ideas and penalize their expression.

For a brief time after the Cold War, we had indulged the illusion of--that democratic capitalism had triumphed and was now unchallenged by any competing ideology. That was nice--that was nice while it lasted. But we are now in a new era of global tension and competition. And China has emerged as the United States' top geopolitical adversary, based on competing political and economic philosophies.

Centuries before communism, China regarded itself as the central kingdom, 'Zhongguo' (SP). And, it was not central to the region, it was central to the world. And its ambition today is not to be a regional power, but to be a global one. For China, success is a zero-sum game. In the words of then General Secretary Xi, Communist Party members should concentrate their efforts on building a socialism that is superior to capitalism.

Such efforts, Xi claimed, would require party members to concentrate their entire spirit, their entire life, for the socialist ideal. And the reward for this sacrifice would be the eventual demise of capitalism. I mentioned my classmate's comment about China wanting to own the world because today I would like to focus on the challenge of China's drive for economic and technological supremacy.

But I am not suggesting that China's ambitions are merely economic, or that our competition with China is, at bottom, merely an economic rivalry. The Chinese have long been a commercial people. But for China, purely economic success is not an end in itself. It is a means to a wider political and strategic set of objectives.

Throughout its long history, China has always used its economic strength as a tool to achieve its political and strategic objectives. In 2015, the Chinese leadership launched its Made in China 2025 plan. A sustained, highly coordinated campaign, to replace the United States as the dominant technological superpower.

The dictatorship has mobilized all elements of Chinese society, all government, all corporations, all academia, and all of his industrious people, to execute seamlessly on an ambitious plan to dominate the core technologies of the future. This drive is backed by industrial policy, involving huge investments in key technologies, massive financing, and subsidies in the hundreds of billions of dollars.

Unfortunately, it also involves industrial espionage and theft of technology and intellectual property. As well as, forced technology transfers, predatory pricing, leveraging China's foreign direct investment and strong-armed sales tactics in target markets. Including, the use of corruption. Make no mistake about it, China's current technological thrusts pose an unprecedented challenge to the United States.

The stakes for our country, could not be higher. Since the 19th century, the United States has been the world's leaders in innovation and technology. It has been America's technological prowess that has made us prosperous and secure. Our standard of living, our expanding economic opportunities for our young people and for future generations, and our national security, all depend on our continued technological leadership.

In the past, prior administrations and many in the private sector, have too often been willing to countenance China's hardball tactics. And it has been this administration that has finally moved to confront and counteract China's playbook.

(APPLAUSE)

Today, I want to focus on two aspects of the challenge that we face. The first is how China jump-starts its techno--technology initiatives by stealing our technology. And second, I want to explain why China's current focus on dominating 5G technology is of central concern.

The ability of totalitarian countries to engage in central economic planning can at times appear to be an advantage. Especially, when mobilizing the kind of technological blitzkrieg that we see unfolding today. The downside is that

central planning suppresses technological innovation. Breakthrough ideas arise in free societies like ours, which have long led the way in cutting-edge technological development.

The Chinese are trying to have it both ways. While they are orchestrating a centrally planned campaign to dominate key technologies, they are attempting to capture the benefit of our free society, by the outright stealing of our technology. The stealing of technology is not a sideshow, it undergirds and propels their efforts.

As my colleague, John Demers, the Assistant Attorney General for our National Security Division observed, China wants the fruits of America's brainpower to harvest the seeds of its planned economic dominance. In 2018, as you have been hearing, the department launched its China Initiative to confront China's malign behaviors, and to protect U.S. technology.

As the presentations earlier this morning and throughout the day will demonstrate, investigations during our initiative have repeatedly shown how the PRC is using intelligence services and tradecraft to target valuable scientific and technical information held by the private sector in the academy. This covers a wide range of technologies, from those applicable to commercial airplane engines, to renewable energy, to new materials, to high-tech agriculture.

Since the announcement of Made in China 2025, the Department has brought trade secret theft cases, in eight of the tech--ten technologies, that China is aspiring to dominate. In targeting these sectors, the PRC employs a multi-prong approach. Engaging in cyber intrusions, co-opting private-sector insiders through its intelligence services, and using non-traditional collectors, such as graduate students participating in university research projects.

Chinese theft by hacking has been prominent, and I am sure you have discussed some of the more recent cases. Those actions by China are continuing, and you should expect more indictments and prosecutions, in the future. Outside cyberspace, defendants pose as U.S. customers to avoid export controls and recruit U.S. employees or co-opt insiders to steal trade secrets.

And at academic and other research institutions, China uses talent programs to encourage the theft of intellectual property. And finally, China complements its plainly illicit activities with facially legal but predatory behavior: the acquisition of U.S. companies and other investments in the United States.

The department confronts these threats through the Committee on Foreign Investment in the United States and Team Telecom. As one example, earlier this year, based on the recommendation from the Justice Department and other agencies, the Federal Communications Commission denied a license to China Mobile on national security grounds.

The PRC's economic aggression and theft of intellectual property come with immense costs. It has been estimated that the annual cost to the U.S. economy could be as high as $600 billion. The department will continue to use our full suite of national security tools to combat the threat posed by theft directed and encouraged by the PRC.

But as I am sure that the FBI director stressed, our ability to protect American technology will ultimately depend on the partnership and working in collaboration with industry in the academy. Now let me turn to a very concrete problem that confronts us today. It is the pivotal nature of 5G technology and the threat arising from China's drive to dominate this field.

5G technology lies at the center of the technological and industrial world that is taking shape. In essence, communications networks are not just for communications anymore. They are evolving into the central nervous system of the next generation of Internet. The industrial Internet. And the next generation of the industrial systems that will depend on that infrastructure.

China has built up a lead in 5G, capturing 40 percent of the global infrastructure market. And for the first time in history, the United States is not leading the next technological era. Now much of the discussion on the dangers of allowing China to establish dominance in 5G, have been focused on the immediate security concerns of using communications networks that China can monitor and surveil.

That is, in fact, a monumental danger, and for that reason alone we should mobilize to surmount China's drive to dominate 5G. But the stakes are far higher than this. It has been estimated that the industrial Internet powered by 5G could generate new economic opportunities in the range of $23 trillion, by 2025. If China establishes sold dominance over 5G, it will be able to dominate the opportunities arising from a stunning range of emerging technologies that will be dependent upon and interwoven with the 5G platform.

From a national security standpoint, if the industrial Internet becomes dependent on Chinese technology, China would have the ability to shut countries off from technology and equipment upon which their consumers and industry depend. The power that the United States has today, to use economic sanctions would pale by comparison to the unprecedented leverage we would be surrendering into the hands of China.

It is important to understand how 5G will enable a revolution in industrial processes. Some Americans think that all we are talking about is analogous to the shift from 3G to 4G in our wireless networks. But we are talking about change that is far more fundamental, then merely increasing download speeds for iTunes and websites and movies. The move from 3G to 4G meant moving from download speeds of about 1 Mb per second to about 20 Mb per second. And this increase made it possible to move the storage of data and some modest processing power off of the devices and onto the cloud.

But even this modest evolution of the wireless business spawned wide new fields of innovation, applications, and businesses. And because the United States was the country that developed 4G, we were the country that captured most of the economic opportunity that flowed from that technology. The jump to 5G is a quantum leap beyond this. We are now talking about multi-gigabyte-per-second peak rates for both download and upload.

These fiber-like speeds, coupled with placing Edge computing facilities closer to the users, means 5G is capable of extremely low latency, under 10 milliseconds. With this capacity, the tiniest devices can have virtually instantaneous connectivity and access infinite commuting--computing power. With these characteristics, 5G becomes a real-time, precise system of command and control.

Devices of all kinds, some smart, some sensors collecting and transmitting data, some actuators carrying out remote commands, can be dispersed and embedded in business and industrial equipment across a wide array of businesses, such as; transportation, energy, finance, healthcare, agriculture, heavy construction, and so forth.

5G provides the command and control function for managing all of these industrial processes. As the world of 5G unfolds, we will be seeing not just smart homes, smart thermostats, but smart farms, smart factories, smart heavy construction projects, smart transportation systems, and so forth, and a host of new emerging technologies.

In addition to artificial intelligence, we will become interwoven with and dependent on 5G and the industrial Internet; for example, robotics, the Internet of things, autonomous vehicles, 3-D printing, nanotechnology, biotechnology, material silent--science, energy, storage, and quantum computing. China has stolen a march and is now leading in 5G.

5G is an infrastructure business, it relies on radio access network, RAN, facilities. China has two of the leading RAN infrastructure suppliers, Huawei and ZTE. Together, as I have said, they have already captured 40 percent of the market and are aggressively pursuing the balance. Huawei is now the leading supplier on every continent, except North America.

The United States does not have an equipment supplier. China's principal competitors are the Finnish firm Nokia, with a 17 percent share, and the Swedish firm, Ericsson, with a 14 percent share. The Chinese are using every lever of power to expand their 5G market share around the globe. It is estimated that the total market for 5G infrastructure is $76 billion.

China is offering over $100 billion in incentives to finance customer purchases of its equipment. That means that China can offer its customers to build their 5G networks for no money down. And they have a salesforce and technicians of 50,000 around the globe to push the acceptance of Huawei infrastructure.

In an infrastructure business like 5G, and I say this as someone who has spent 15 years in the telecommunications business, scale is critical. The business requires huge investments in R&D, as well as, very high capital costs. The larger the company's market share, the better it can afford these costs. Competitors facing a shrinking addressable market, find it harder to sustain the levels of investment required to stay competitive.

Chinese companies start with the advantage of the largest domestic market, giving them instant scale. And as they add this around the world, they will be able to invest more in their technology. The more China gains ground as a supplier of 5G infrastructure, the more it will also gain ground in all of the constituent technologies that undergird 5G infrastructure.

5G rests on a stack of technologies including; semiconductors, fiber optics, and rare-earth and materials. China has moved to domesticate all of these elements so that it will now-- it will not be dependent on foreign suppliers. Semiconductors provide a good example of the ripple effect of Chinese leadership in 5G. China now consumes over half of the world's semiconductors.

China has now started to replace U.S. semiconductors with its own. Its scale in this field will permit it to make the investments needed to close the current quality gap. As China builds its scale in the semiconductor industry, it will replace substantial pressure on alternative semiconductor suppliers.

And of course, semiconductors are indispensable to a wide range of technology and industries, apart from 5G. China's success in 5G infrastructure is also translating into advantages in a range of new technologies associated with 5G. Artificial intelligence is a good example. It is interwoven with the industrial Internet. As China captures more and more of the data generated by its 5G infrastructure, it can produce better artificial intelligence because that is what artificial intelligence learns from.

The more data, the better the AI. It is a virtuous cycle. Within the next five years, 5G global territory and application dominance will be determined. The question is whether, within this window, the United States and our allies can mount sufficient competition to Huawei, to retain and capture enough market share to sustain the kind of long-term and robust competitive position necessary to avoid surrendering dominance to China.

The time is very short, and we and our allies have to act quickly. While much has to be done, it is imperative to make two decisions right away. First, we have to deploy the spectrum necessary for a robust 5G system in the United States. We have not done this. This is the mid-brand--mid-band spectrum called the C-block or the C-band.

The FCC has been working hard to get the C-band spectrum out into the market through an auction. And it is critical to get this done within the next very few months. Even then, the United States will need 400,000 base stations to cover the nation if we rely solely on C-band. This could take a decade or more to build out. Just, by comparison, today's wireless system runs on 70 to 80,000 base stations.

China has already installed approximately 100,000 base stations for 5G. We will have to build 400,000 base stations for nationwide 5G coverage after the C-band is put out. Now, recently there have been some interesting proposals to jumpstart U.S. 5G by also making available L-band spectrum, for use in tandem, with C-band. By using and L-band uplink, we could dramatically reduce the number of base stations required to complete national coverage. It has been suggested that this could cut the time for U.S. 5G deployment from a decade to 18 months.

And save, approximately $80 million. While some technical issues about using the L-band are being debated, it is imperative that the FCC resolves these questions. Make its decision on spectrum and move forward. The bottom line is that we have to move decisively to auction the C-band and bring resolution on the L-band.

Our economic future is at stake. We have to bear in mind in making these spectrum decisions, that given the narrow window we face the risk of losing the 5G struggle with China should vastly outweigh all other considerations. Second, we have to make a decision on the horse we are going to write in this race. Who is the 5G equipment supplier or suppliers, that we will rely on to compete against Huawei, around the globe, to win contracts from operators, and blunt Huawei's drive to domination?

It is always-- it is all very well to tell our friends and allies that they shouldn't install Huawei's, but whose infrastructure are they going to install? If we and our allies and other countries that do not want to put their economic fate in China's hands are not going to install Huawei's infrastructure, we have to have a market-ready alternative today.

What is a customer looking for, after all? What is the operator looking for in moving from 4G to 5G? It is a one-time decision. It is a big decision. You cannot afford to make a mistake. You need to know you are buying a reliable system, that will perform. Because you do not have the luxury of tearing it out down the road. And, you need a system that will allow you to seamlessly migrate your installed 4G base to 5G.

And you need to know that your supplier has staying power. That they are not here today and gone tomorrow. They will be there for the long haul. Those of the products that are necessary to win contracts today. And there are only two companies that can compete with Huawei right now: Nokia and Ericsson. They have the reliable products; they can guarantee performance. They have proven successful in managing customer migration from 4G to 5G.

The main concern about these suppliers is that they have neither Huawei's scale nor the backing of a powerful country with a large embedded market, like China. Now, there have been some proposals that these concerns could be met by the United States aligning itself with Nokia and or Ericsson, through American ownership of a controlling stake, either directly or through a consortium of private American and allied companies.

Putting our large market and financial muscle behind one or both of these firms, would make it a far more formidable competitor and eliminate concerns over its staying power, or their staying power. We and our closest allies certainly need to be actively considering this approach. Now, recently there has been some talk about trying to develop an OpenRAN approach.

Which aims to force open the RAN, into its components and have those components be developed by the U.S. or Western innovators. The problem is that this is pie-in-the-sky. This approach is completely untested and would take many years to get off the ground and it would not be ready for prime time for a decade, if ever. What we need today, as I said, was a product that can win contracts right now, a proven infrastructure, one that will blunt Huawei's advance.

As a dictatorship, China can marshal an all of nation approach, the government, its companies, its academia, acting together as one. We are not able to compel this. When we have faced similar challenges in the past, such as World War II and Russia's Cold War technological challenge, as a free people we rallied together.

We were able to form a close partnership among government, the private sector, and academia. And through that cooperation, we prevailed in the challenges we have met. Unfortunately, the cooperative bonds and sense of purpose we were able to muster in the past are harder to call on today. And in the 1950s, we had the Sputnik moment to help galvanize the nation and bring unity to our response, and we have not seen a similar catalyst today.

If we are going to maintain our technological leadership, our economic strength, and ultimately our national security in the face of this blitzkrieg, we need the public and private sectors to work together and come shoulder-to-shoulder. To our private-sector friends, I would say that appeasing the PRC may come with short-term benefits, but I urge you to question the long-standing assumption that promises of market access are worth the steep costs. The PRC's ultimate goal is to replace you with a Chinese company.

University and think tank colleagues, I'd ask that you not allow the theft of technology under the guise of academic freedom. Do not allow the PRC to dictate your research or pressure you into ignoring diverse voices on controversial topics. Consider whether any sacrifice of academic integrity or freedom is worth the trade-off.

And to our allies, I applaud your efforts to stand up to China's economic leverage, but we must do more and act collectively. Let's not forget that our collective economic influence and power is far stronger. Throughout history, free societies have faced regimented adversaries. At critical junctures, they have achieved the unity and purpose necessary to prevail, not because they have been compelled to do so but because they freely choose to do so. We must make that choice today. Thank you very much.

(APPLAUSE)

DEMER: Alright. Thanks to the Attorney General. Our next panel is a panel of individuals from industry and I will allow our moderator, of course, to introduce them. Our moderator is Aruna Viswanatha, of the Wall Street Journal. Having dealt with her over the last few years on these issues I can say that she is as knowledgeable on these issues as many, many people in this room and maybe all of them.

So, I would like to thank Aruna for agreeing to moderate this panel and for all of her excellent work on the issues that we have been talking about today. And to welcome all of the panelists including my predecessor, John Carlin, up on stage today. Thank you.

VISWANATHA: Thank you. So just to do brief introductions for everyone on this panel, first, we have Bill Zarit, who is a Senior Counselor at the Cohen Group (SP) and he is Vice-Chair of the American Chamber of Commerce in China. He also previously worked at the U.S. Embassy in Beijing where he was Minister of Commercial Affairs.

Next to him is Jeremie Waterman, of the China Center of the U.S. Chamber of Commerce and he is responsible for policy initiatives in China, Hong Kong, Taiwan, and Mongolia, as well as, helping to steer the chamber's policy work across the Asia-Pacific region.

Next to him is John Neuffer, who runs the Semiconductor Industry Association, who as we just heard, is probably one of the industry's most affected by the national security implications of the U.S. China relationship. And he sources the industry's main advocate in maintaining U.S. leadership in semiconductor design, manufacturing, and research.

And next to him is John Carlin, who as John Demers just said, ran the National Security Division in the Obama Administration and was Chief of Staff to Robert Mueller(SP), when he was FBI director and now advises companies on cyber and other issues and is also the author of Don--Dawn of the Code War.

So maybe to jump right in, we will get to 5G in a moment, but maybe if we step back a little bit Bill Evanina, had earlier put up a slide where he listed a number of industries that China has designated in its 2025 plan as priorities, as technologies that they really want to develop, and he said all CEOs need to be thinking about this.

So, to put it in some context, I mean obviously, CEOs are also thinking about other things, the Phase I deal, opened up some China market access, potentially for American companies. There are other China risks to worry about including the coronavirus impacts on supply chains. Maybe just started off Jeremie or Bill. Do you want to talk about how does the--what that slide showed in terms of Chinese 2025 initiatives, how does that play into what CEOs think about, in terms of approaching business in China?

ZARIT: Well, this is no news--this is no new news to the folks that have been doing business with China for a long time. So, we actually should thank our Chinese friends for publishing the Made in China 2025 list of the 10 major industry sectors. Because it really was-- and this was done in 2015, it really was a start of a wake-up call. Now, I had worked in the Embassy, in Beijing. So, intellectual property theft, cyber theft, is also nothing new to companies active in China.

We have been dealing with that for a long time. I think one interesting aspect that was brought up earlier is about retribution and I just wanted to make a comment on that. We saw that when I was in the Embassy, we would talk to our friends at the American Chamber of Commerce in China, which is one good way of addressing issues without actually having the company's stick its individual neck out.

So, the effort is; okay, we have companies that are having problems and the chamber tells us about this and we want to go to the Chinese officially and through our bilateral dialogues that we used to have, Joint Commission on Commerce and Trade being one of them, we would bring it up.

Okay, well, the Chinese and they are justified, I think, to ask well, do you have any examples? And we would go back to AMCHAM(SP) and nobody, not one company would volunteer. And, this has been the problem for years,

this continues to be the problem the Chinese, of course, the retribution is in all kinds of different modes, but it is real.

So again, working through these associations, and I know John is heading up one of the major associations involved here, is probably the best way to get around that--that retribution problem. So, another issue that we have been facing is profit versus patriotism. And--you--our--our multilateral companies, many are led by non-Americans, number one.

So, this really has not been a very effective way to try to bring companies out to tell--to make public what is going on. So, I think that the new approach and we heard it already--loss to companies from the loss of their IP, and so forth and so on. Is really--is really the best approach. And I-- there's a lot more to talk about but I'm going to stop right there.

WATERMAN: Maybe I can just add two additional brief points, I think, to Bill's excellent opening. I guess the first point that I would highlight is that and it is a bit trite, but I think very important and apt, at this moment in time. The relationship is highly multifaceted and multidimensional. And what do I mean by that?

When we are talking about a very serious pressing set of issues today and I think that there's actually very strong alignment between the business community and the U.S. law enforcement Department of Justice and the national security community on those challenges. And if you look at a lot of the prosecutions that the Department of Justice has engaged in those are often in close collaboration, partnership with the U.S. companies, affected U.S. companies.

Because at the end of the day, that's where the Chinese are going. They are taking the IP, they are taking of American companies. One very, very important piece, that though coexists with a substantial-- an enormous commercial relationship and a Phase 1 trade deal, that was just negotiated in December. Where the U.S. government is working very hard to level the playing field with China and to create more opportunities for American business in China because it is a critical market.

And it impacts directly the vitality of the U.S. economy, the ability of our companies to compete with China around the world and in China, is an economic security issue, a national security issue. In many respects because it goes to the vitality of our economy. And of course, that also coexists with the coronavirus. Where you have significant challenges, of course, you know, I think we certainly in the business community are doing what we can to support the Chinese people as they go through a very, very trying time, a very difficult period.

But all of these things coexist together, and it makes it very, very complex to navigate. But certainly, I think that the business community stands squarely with the U.S. government in protecting national security. We can talk more about that. The other point, that I would make really to echo what Bill had said, is that the American business community has been talking about these issues for a long time.

Quite frankly, to be frank, a lot longer than many in the U.S. government have been talking about them before. We issued at the chamber our first report on China's indigenous innovation policies in 2010. We followed up with that--with that report with a report on China's investment regime in 2012, we underwrote a narrative on China Inc. on state capitalism in China authored by Jim McGregor also in 2012.

We issued a report on China's use of its anti-monopoly law as an industrial policy in 2014. And of course, we issued a report on Made in China 2025, in early 2017. So, I think that AMCHAM and SIA and others have done similar things. So, I think to the point that Bill is making, we stand with the U.S. government on these issues, they are of deep concern.

But we also have to ensure that American companies are able to continue to compete in a critical market and also vis-a-vis Chinese companies and third-country markets around the world.

VISWANATHA: So, Bill, you had mentioned that companies are reluctant to kind of stick their neck out. I think that the Justice Department had tried to get executives from individual companies to appear on this panel and had a lot of, no thank you's. And could not really get anyone--

NEUFFER: Do you mean that we were not the first choice?

(LAUGHTER)

Oh, I'm disappointed.

VISWANATHA: John Carlin, you have seen this from both sides now. Why do you think people are reluctant to come forward? Do you think that they have valid concerns? Do you think that anything is changing there?

NEUFFER: Thanks for that easy question, Aruna. Also, I just wanted to say, Jeremie, I know you don't like wearing a jacket and tie but breaking your arm is a little extreme, isn't it?

(LAUGHTER)

So, the practical and political reality is that retribution is a variable in this game. And everybody knows it. And that is the biggest problem, as Bill suggests. So, just stepping back a little bit, semiconductors, the backbone of semiconductors, is the IP. Our companies are obsessed with keeping that IP, safe and secure.

Our companies spend billions of dollars a year to the tune of $30 to $40 billion dollars a year, developing this IP. We go out to the university campuses and we hire the best and brightest to develop this IP. So, the most advanced chips now have roughly 20 to 30 billion transistors on them and they are that size.

That's 20 to 30 billion, on-off switches. And that is all built on our very, very powerful and valuable IP. So, IP is everything for our industry. It is the backbone of the industry and we take it very seriously and we are very, very much applauded to the Department of Justice's effort to launch the China Initiative, this has been an ongoing problem for us. We actually had, Mr. Demers, come and speak to our board, last year. Thank you for that.

But back to the original question, as long as the threat of retaliation hangs, looms large, it is a very difficult thing to do for companies.

VISWANATHA: John Carlin, do you have thoughts on, you've seen it from both sides now, what is your take on this reluctance to come forward now?

CARLIN: Look, in some respects, there has already been a seat change when you think about where we were 5 to 10 years ago. So it was only in 2014, that we brought the first case of its kind, the indictment of five members of the People's Liberation Army, Unit 61398 for their acts of economic espionage and laid out, in great detail, exactly what they were doing and it showed, hey, this is not the type of conduct of state versus state, this is things like targeting the solar company for its pricing information, using the theft of that information to price dump, and then to add insult to injury, when that company sues for unfair trade practices, stealing their whole litigation strategy and watching them go bankrupt.

Or another case, stealing the color white. So when you're saying that they are taking everything, this is not a national state secret, it sounds like it's a theft of titanium dioxide, it might have some military application, but actually what they were stealing was the color white, that is used in Oreo cookies. So, it is just for economic benefit.

Prior to that case, I spent years prosecuting on the criminal side of computer hacking an intellectual property cases. And, most of the victim companies precisely because of this fear retaliation, number one, and number two, a sense that there would be some short-term pain, in terms of the loss of intellectual property or trade secrets, but long term it was work that pain because of the benefits of the market.

And I think you saw a change in the way companies were thinking about that and a realization that if it's a determined strategy of a nation-state this large, utilizing the second-largest military in the world, to steal IP and

trade secrets, that no company could compete against that. And, long term, the economic prospects were bleak. And this has been a rare area-- there are a few differences of opinion between the Trump and Obama Administrations. I have heard, on some issues.

But this has been a rare area of continuity and I think it shows, in some respects, that across party lines, that this is a threat to Americans, regardless of your political affiliations. And, you see that in terms of company reaction. Why aren't more, why isn't, you know, a CEO up on stage with us today?

I think there is a gap in our current thinking, and the Attorney General touched on it. So, you heard from the FBI director and the FBI, this one of our top law enforcement threats. And you have seen excellent work done by agents and analysts, to bring cases. You have also seen actions in terms of toughening so more stick on SIFIUS (PH).

You have seen actions toughening in terms of the FCC is looking at license approvals. We lack the carrot. So, I think for a lot of these CEOs, they do not see, they see the risks, but they don't see an alternative successful business strategy if they are unable to sell into the Chinese market.

And similarly, for allies who share some of the security concerns about being dependent on 5G, they don't see a viable alternative and they don't want to lose out on the advantages of the industrial Internet.

Which I think calls for serious consideration, which I believe the Attorney General was touching on of what industrial policy, in this space, can we identify what we need? What are the gaps for this industry? Is there additional funding that should be provided to lead innovation in this area? Should we be thinking 6G?

You know we lost 5G, we heard that today, the bulk of the world is not using, there is no American alternative and the bulk of the world is not using the Western alternative. So, in order to be safe, does that mean virtualization across networks for when you are trying to communicate with allies abroad?

Does it mean some new technology of the future? Some type of moonshot that puts us into a more secure setting. I think we need to think about--we need to continue with the stick but also think about where--what the carrots are.

VISWANATHA: We just heard the Attorney General talk about proposals to potentially throw the weight of the U.S. government behind the competitor an alternative to Huawei, John Neuffer if you could talk to us a little bit about how realistic do you think these proposals are? How viable are they?

NEUFFER: Yeah so, we just make the semiconductors that go into this stuff. But underscoring what John just said, we didn't lose a Huawei competitor because of defensive measures, we lost the Huawei competitor because we did not have the right kind of affirmative agenda, to keep one and to build one.

And I think that it is important that we think about our strategy, it's having the sticks, to have the defensive measures in place, but the bigger emphasis always needs to be on the affirmative agenda. And the semiconductor sector, that means a focus on cultivating talent, we are not cultivating enough indigenous talent that goes--that becomes electrical engineers that want to work for semiconductor companies.

We have an immigration system, so we fill the gap with foreign talent. And, we have a new innovation system where we bring in the foreign talent and a lot of time and money spent on educating the foreign talent and then we chase them away, to work for competitors. That does not seem to make any sense.

And the other--perhaps even a bigger piece to this is, we need to double down on our investment and research in the semiconductor area. It is a fundamental technology in our government investments have been falling-- well investments in fundamental research and semiconductor area have been rising and other key economies like China but others so, I think that it's very important that we have a much bigger focus on our affirmative agenda while maintaining the defensive agenda to protect our interests.

VISWANATHA: Jeremie, do you have thoughts on, at a high level, these are proposals to potentially bring the U.S. government into the private sector in ways that may be historically, we don't necessarily think about in the tech--in this specific space? What do you make of what the Attorney General was talking about?

WATERMAN: So, so, what I would say first, as a representative of the U.S. Chamber of Commerce, are strong preferences for market-based competition. Of course, we don't have in so many areas, as has been outlined today, we don't have market-based competition.

Of course, we don't have in so many areas, as--as has been outlined today, we don't have market-based competition. And so, that raises a whole series of questions. Very much agree with John in terms of the affirmative agenda. I guess to go one step further and--and I think 5G, in particular, is driving a-- discussion as we heard from the attorney general a bit earlier, about--about how we invest in ourselves, not just how we protect ourselves, the defensive piece, but how do we invest in ourselves and how do we work with allies.

There's a carrot and stick approach there as well with allies. What are our priorities with our allies in terms of trade? Right. Where does China fall in that set of priorities in terms of our trade agreements and so forth? There's a--there's a--we're at the beginning, I think, of that discussion. And we're also at the beginning of a discussion where--where if in certain areas and of course, the business community's strong preference is for export controls and investment measures, which, by the way, we supported we supported FIRMA (SP), we supported EKRA strongly. But if--when those measures are deployed and--and when market opportunities are denied for our companies, number one, we need to make sure that those opportunities don't just go somewhere else, we're not just squeezing a balloon.

And then the question, you know, and John can speak more to this than I can when you look at corporate budgets, R&D budgets continuing to remain competitive, if--if--if your market, if your scale is going to shrink, there has to be a discussion there among the executive branch, among appropriators and industry together about how we--about the issues and how we address those challenges. And I think--in my own observation would be that we're just at that we're just scratching the surface of that kind of a discussion in terms of what we really need to do. And that's hard work because it is--it really it's--I think it's--it's much easier and certainly more in vogue to champion a defensive measure, an export control or a restriction than it is to actually integrate all aspects of--of our policy in a very coherent way. So we're--we're doing the least--we're helping ourselves the most, investing ourselves the most, and then also doing the least damage to ourselves in any protective measures that we may be taking.

NEUFFER: I just jump in something that Jeremy said about R&D investments. So semiconductor industry is special in a number of ways. One that it's amazingly foundational, but another that we invest about 20 percent of our sales back into R&D. We, along with the pharmaceutical industry are the most R&D intensive industries in the world.

There's two things that have really been this secret ingredient to our success. One is our amazing innovation, ability to innovate, and the other one is our scale where we--we control about 50 percent of the global market in semiconductors. That all allows us to have huge resources. It brings in huge profits that allows us to dump amazing amounts of money into R&D and that allows us to pedal faster than anybody else in the world, in the semiconductor--in this semiconductor arena.

So this is a complicated issue. We have to have access to the big markets around the world. China happens to be our biggest market. So when you're thinking about limiting China's bad behavior, which needs--needs to be done by the U.S. government, that's the job of the U.S. government, all hat that--also has to be contemplation about what it's doing to a super important industry for the United States in terms of its national security and its economic security.

ZARIT: Yeah, if I could--I could quickly jump in agreeing with what has been said. I'm very encouraged that we are looking very seriously at the China threat. And while we're doing that, I--I--as--as John intimated, we really need to be careful. We need to have a balance so that we don't cut off our nose to spite our face. Now, I would say the analogy that we're seeing is within--in trade, where this administration has, in my opinion, done a very good thing in calling out China on its market access issues, IP issues, unlevel playing field issues. I would say again, my opinion and it is actually the opinion of AmCham China that tariffs--the way--the wholesale use of tariffs was not exactly the best way.

And according to our membership, our companies were hurt as much by our tariffs as by the Chinese tariffs, and companies are still reeling from this. And the analogy is, as we go forward with this China initiative in law

enforcement that we do, as John said, take into consideration that there could be negative effects on our economic health and this could actually be counterproductive. So, again, I'm really encouraged this is happening and I do encourage that as we go forward, we do it in a balanced way.

CARLIN: Just jump in thereon. I think it's important to distinguish the China initiative and the actions of law enforcement and the Justice Department from the general trade debate and to be clear in--in our messaging continually that a--the Justice Department is pursuing cases and its theory is based on facts. And so, seeing particular conduct that we have all agreed because President Xi stood with President Obama and said it, so both countries agree, along with all of the major industrial powers that one should not be using your state apparatus to target private companies for the economic gain of their competitors. It's a principle we've agreed on.

Then the Justice Department and you saw the unleashing of the U.S. attorneys, which was part of that initiative that started in 2014 and the panel earlier today looks to see are people abiding by the pledge that they have made. And when they have not, when they are corruptly paying individuals inside companies to steal intellectual property, when they're using access in order to through cyber means to steal secrets or disrupt operations, then they should know that law enforcement is going to follow.

And so that needs to, I think, occur. And the results of those cases should not be bargained away or put into diplomatic channels and confused with trade issues. I do think there's been some confusion in the way that these issues are spoken about, where it seems as if a tariff type to echo Bill's point, a tariff type dispute is then linked and you're going to go find a case to show them that we can do that. That--that may be the way certain other countries operate with their use of the law for--their--their law enforcement but one of the battles we're fighting is one of values that says our law enforcement acts independently based on facts and law.

WATERMAN: I just--I don't think business thinks any of that should be bargained away. I think business is very--certainly with the U.S. Chamber, I think we're--we're--we're very supportive of holding China to account where there is behavior that needs to be addressed. I think the only point that I would make in terms of the, again, the multifaceted if we're going to talk about the China challenge, Bill talked about is China threat. You know, one very well-known case that I won't name, I think I mean, to--to highlight that--these things overlap. And so I think that that's a challenge also for the U.S. government in terms of how it's developing a strategy to deal with some of these issues.

You can have--you can have individual cases that involve trade secret theft, involve use of the Chinese judicial system to provide injunctive relief for Chinese competitors and simultaneously, the anti-monopoly authority in China bringing actions to exert pressure on a foreign company. Right? And so you have China using all of these tools, right? China doesn't--China doesn't draw those bright lines as we do between trade policy and antitrust policy or patent policy. In fact, so many of the agencies within China that are, you know, you now have actually under the state administration of market regulation, you have the antitrust authority, the standards authority and the IP authority all under one roof.

So I think that--that has to be worked through on--on the U.S.--on the US government side and thought through a bit more.

VISWANATHA: To jump to Some questions from the audience, here's one maybe I can direct all of you. Can you give a specific example or of a company that has done a good--that you think has done a good job with internal controls to protect against Chinese theft either in the U.S. or in China?

ZARIT: I have a lot of examples, but I'm not going to name them specifically, but going back to the early--

CARLIN: Just to echo Bill's thinking on that, if someone in this space is now advising companies, it would be a bad idea, I think, to tout that you had done it right you'd be asking for that--

ZARIT: But--but you've--you've done it, they exit.

VISWANATHA: Maybe if you can talk about what that looks like.

ZARIT: Well, you know, going back to the time in the embassy, we would have companies come in. We have a regional security officer and he has an organization that meets on a regular basis and this is one of the issues that they talk about. So they're educating companies on this. When a specific company which happened more than once would discover an issue, this company would come in and talk to us on a confidential basis and we would then work with that company.

I am not a cyber expert, but folks that are would work with that company to help improve their cyber protection. And there were a number of companies that were very successful in this.

CARLIN: A few concrete suggestions. One would be that--and I--I think this is a new space. So not--I'm continually surprised when giving advice on--on this side to C-suites and boards, how even for some of our largest companies this is not an issue that they've thought about or invested in. So couple of thoughts on how to improve that. One would be do exercises, call them tabletops or games where you use and this is what's the advantage of the cases the Justice Department is bringing because they lay out in such detail the facts of how economic espionage has occurred. So apply those against your company, have the C-suite executives play out the investments that they've made to protect against it and also how they'd respond if they detect it and those can be quite eye-opening.

Number two, there's often a divide within companies between the physical security and cybersecurity sides of the house. You're seeing the defense industrial base move faster I think in that area of having one integrated insider threat program that looks across the range of--range of threats. And unfortunately, what you as you hear about the tradecraft, that's what the adversary is using all these different tools in order to be able to obtain it, so you need to think similarly inside the company.

And the third is when designing, this is security by design when thinking about new products and before rolling them out to think through not just whether they work, but whether they work if a bad guy, whether it's a crook or a terrorist or in this state, a nation-state, wouldn't want it to work.

NEUFFER: Let me just jump in. the--for sure, semiconductor industry companies have had problems with trade secrets walking out the door, but the companies in my membership did not fall off a turnip truck yesterday. Our industry is very, very, very IP heavy. So as I said earlier, there is an obsession with protecting that IP in the semiconductor industry, probably much more than most companies, I'd say.

WATERMAN: And I guess the only point I'd add is that it's--it's not something that you ever--you never sort of--with regard to protecting your core IP, you never cross the finish line. You never--you never--you never score a touchdown and spike the ball.

It's an ongoing exercise as your competitors evolve, as--as the regulatory environment evolves, I mean, there's--there's a cyber--as your investor-- as your footprint changes. I would also add that, you know, there's some really interesting trade secret provisions, I think exciting trade secret provisions in the Phase 1 agreement that not only cover trade secret theft prior to--excuse me--after the agreement goes into effect, but cases of ongoing impact that occurred prior to the agreement going into effect.

I think there is a big question out there about how those provisions in conjunction with the dispute settlement of Phase 1 will be used and how cases that have occurred within China and that are subject to Chinese law will be advanced in the context of--of the Phase 1 agreement and the dispute settlement mechanism.

There's clearly an opportunity there because the Chinese have made some very clear commitments, explicit commitments and, you know, I think certainly, the U.S. government is as well-positioned to hold China accountable with regard to cases that have occurred.

VISWANATHA: We did hear directory talk about Tao across the field, FBI field offices, they're trying to do more private sector outreach and try to do more briefings and just get to know more companies within their districts. What impact is that having? Can you speak to any specific things that you've seen as a result of that outreach?

CARLIN: So, you know, it's--I'm seeing it with clients now where particularly the overall message that we're gonna treat you as a victim and be cognizant of your business needs if you come into us and provide information, paying--paying dividends. It's important the companies are looking for when they're victimized certainty, as much certainty as they can about and control of the process. What happens if I--I want to tell? I want to do the right thing but what happens with the information? Am I going to--is it going to be used against me in some regulatory proceeding? Is there going to be some public splash where am outed in a way that causes my employees jeopardy? Or to Jeremy's point, you know, antitrust trumped-up antitrust action against me overseas.

So I think it's--yeah, it's working and it's--it's important to continually, as part of that effort, emphasize and work on the ways in which you can keep the victim in control of the victim by their own decision decides to come to you to provide information that will help more companies come in.

ZARIT: John, do you think that's actually reassuring to the companies? Because it seems that if there is some case, there's a legal case, I don't think the company would be able to actually stop it from going forward. Would they?

CARLIN: So--so the decision to bring a case, res--a criminal case resides uniquely within the province of the attorney general and the Department of Justice. But John Demers will be speaking later, my successor, assistant attorney general, I know I said repeatedly, and I'm sure we'll say again later today. But that--that if a company comes forward voluntarily in a case of economic espionage, they won't make a flat guarantee.

So if it ended up involving loss of--potential loss of life like a terrorist case, or if it's a company who were the victims are primarily other companies that rely on that company's technology but--but by and large, that if you come in voluntarily in the case of economic espionage, they will not even though it's their decision, but they will not bring a criminal case. I know it's something I said similarly when I was in the spot. But that's the message to your point, Bill. That's important to keep--keep repeating if we want companies to come in voluntarily.

VISWANATHA: And here's another question from the audience. How can U.S. companies, especially startups, find investment funding that does not come from China?

ZARIT: Have a good idea.

VISWANATHA: Anyone come in on that?

ZARIT: There's a lot of--there's a lot of V.C. money sloshing around. I think that the companies just need to be really careful and do due diligence on where that money is coming from. But if it's a good idea, there is a lot of money available.

WATERMAN: I think Rhodium posted a report, released a report that actually indicated that the amount of BC funding from China has been--for example and that in--in--in the DIU ex report actually overstated and so I would--that's their report, that's not--but--but I think to the point that there's--obviously the U.S. has a tremendous BC industry. And I think to Bill's point, to your point, if the idea is a good one, I think you can get it funded.

I think part of the issue with Chinese venture capital funding is that they've just made it highly available. And, you know, it's been easier to--to come by and that's attractive. Obviously, there's also the market there in terms of being able to commercialize technology to scale, right, which is something that we also have to talk about in terms of how we address that issue here in terms of the points that John made earlier.

VISWANATHA: And one more from the audience. What are large U.S. tech companies doing to address insider threats and IP exfiltration? I guess to bring in, I think the example that Adam Hickey had mentioned earlier today where there was an employee that was approached to put a thumb drive into his companies ser--servers and otherwise something bad might happen to family back home, and they addressed it in a way where they secured the computer, he stuck in the thumb drive, nothing happened. He went back and said, oh, I don't know what happened, it didn't work out. Have you seen similar episodes? Do you--do you have thoughts on this broader issue of what our large U.S. tech--tech company is doing to address this?

NEUFFER: I think, again, if--if you reveal all the work that's being done, you're kind of defeating the purpose. But there is a--a lot of effort--protocols within companies to compartmentalize information, that's for sure. Data on company equipment is--is--is monitored and everyone knows that. So there's a--a lot of work internally in the companies to--to keep the information inside.

ZARIT: And in--all companies--so many companies are not necessarily high tech but including high tech have been dealing with this issue for a long time in China and actually not just in China, but other countries. So they--they have been working on different strategies on how this - to stay ahead of the espionage, how to--to screen employees.

And--and many companies knowing that their IP is going to be taken, I also have a strategy on, you know, how to stay ahead of the folks that are stealing their IP. So it really runs the gamut and the successful companies have been working with their marketing and legal folks to have a strategy because the companies want to stay in China, they want to either manufacture, but increasingly they want to be able to sell there, and again, increasingly, more and more companies are manufacturing in China for China.

So it's a matter of doing the diligence security work and also a strategy on how to--because they're stealing IP is going to happen, I hate to admit it, staying ahead in the market, bringing in new products and so forth.

VISWANATHA: And I think we have a hard stop at 11:20. So I'll just open it up for any final thoughts you might have to offer. John Carlin, you want to start?

CARLIN: Sure. I think this is an important initiative and part of the importance is--is fostering the type of dialog that we're having today by not keeping secret as we did for a long time and as--as it can be tempting to do when you are a victim and in government. It was the default in terms of the way we were keeping information classified. So to make sure - although, the solution may be difficult and multifaceted as we've touched on, that we are honest and transparent about the problem.

And so that we continue to make public to figure out why the theft of intellectual property and trade secrets is occurring, to make it public, to impose consequences through the rule of law, and then to use the public information that is out there to help inform how companies defend themselves, but also where--what our policy should be in this area.

NEUFFER: Just--just a couple of points. Again, one, apply the Justice Department for launching this initiative little over a year ago. As I said before, IP is the backbone of our industry and the U.S. government stepping in to help us preserve that IP and keep it safe is very, very important for us. The last thing I'll say is that I'd love to see more resources going into these efforts, going to these field offices which are staffed but maybe not staffed as fully as they should be to provide the best services possible. Thank you.

WATERMAN: I too would applaud the department. We at the chamber have had a great engagement, ongoing dialog with the Department of Justice on the full range of national security issues, principally through our national security division. And that's been very, I think, beneficial for industry and hopefully for the department.

The only closing thought, again, it's a point I made earlier, which is I think we're at the very beginning of a conversation about--about what the--what the challenges in law--in certain--perhaps not all, but many made in China 2025 areas. Perhaps not the policy itself, but the areas that China's focused on and what that means in terms of both protecting ourselves but also investing in ourselves and then related to that, how we work with our allies.

And I think there's a lot more work that needs to be done in all of those areas. The conversations, I think this is--this is a great program today and--and hopefully we'll--we'll continue to advance those discussions so that the plan is that we're approaching these issues from a more holistic perspective and in a way that advantages us the most and minimizes damage as I mentioned, to--in particular to U.S. industry in the U.S. economy.

ZARIT: And I have three real quick thoughts. I agree wholeheartedly with Jereme about allies slash like-minded countries. Unlike our approach in the trade area, which I don't think we really worked with our allies as much and I

think we can get a lot more power if we do work with our allies, both on the trade side in the China challenge and also on this legal side.

The second point is and--and it was brought up and--and we really need to encourage policy that gives incentive to companies to do the right thing in terms of protecting IP, but also policies that will promote education and R&D in this country because the Chinese are doing what they--whatever they can do to be competitive. And much of it is--is should be done if they want to be as competitive as possible and we need to stay competitive with the help of policies that encourage that.

And one last point we--I'm saying balanced in our approach, I'm thinking mostly that the--the--the CCP, the government's activity is one thing, it's not an ethnic thing and we have to be very, very clear that we don't punish the Chinese people and in--in this whole process, we don't punish--punish the Chinese people, but actually focus on the real culprits.

VISWANATHA: Thank you.

(APPLAUSE)

LEWIS: Okay. Our final panel, ladies and gentlemen is on the academic experience, which you heard quite a bit about as one of the principal avenues for technology transfer. It's going to be moderated by my colleague, Jude Blanchette, who is the Freeman chair here at CSIS, the Freeman Chair in China studies. So I'll turn it over to Jude to introduce the panel. Maybe I won't.

BLANCHETTE: Well, thank you very much. We're going to get right into this because although Aruna mentioned, she had a hard stop. We actually have a much harder stop. We got to be off the--off the panel here off the dais by 12:08, so we'll get right into it. My name is Jude Blanchette, I'm the Freeman chair in China studies here at CSIS. It's a real privilege to be here and to be sharing the stage with my former colleagues here for a really important discussion on the issue of how does the United States and its academic and scientific institutions respond to many of the challenges that were discussed earlier in today's program.

Just to put it at its bluntest, I think the topic under discussion for this panel will be how does the United States maintain their--ensure that it maintains its position as a global leader in academic and scientific excellence, while at the same time protecting national security, but crucially, also protecting the rights and privileges of U.S. citizens and non-citizens alike. I think it's those three elements, rather than just the normal two of national security and academic openness and excellence that are important here.

But as we're going to discuss today, getting this balance right is extraordinarily complicated and it's one that I as an outsider looking at this, it seems that nearly all sides are dissatisfied with. Obviously, I think what we heard earlier today was that we're--we're not doing enough, that the problem is big, it's been framed as existential. On the other side, though, there are those who are very worried that some of the actions taken by the U.S. government, law enforcement officials are-- overreaching, overzealous, and there's concerns of a proto witch hunt that's in the making here.

So as if to confirm this, I just want to read a quote from December 9th, 2019 report by the advisory panel, Jason, which concluded - this was on fundamental research security and they concluded; the scale and scope of the problem remain poorly defined. Academic leadership, faculty, and frontline government agencies lack a common understanding of foreign influence and U.S. fundamental research, the possible risks derived from it and the possible detrimental effects of restrictions on it that might be enacted in response.

So hopefully, we've got a really fantastic group of individuals up on the stage here to help us wade through these really difficult issues. From my left on the way down, We have Dr. Doug Girod, who's the chancellor of Kansas University, Dr. Greg Fenves, who is the president of the University of Texas at Austin. Dr. Mary Sue Coleman, who's the president of the Association of American Universities, which I think 65 member universities. And then at the far end is Mike Lauer, who is the deputy director for Extra Mayo Research at the National Institutes of Health, which has been at the center of this as well.

So we're going to spend a lot of time or at least 40 some odd minutes talking about some of the negatives here. So I actually wanted to start out with a positive, which is I wonder if I could just go down the line and ask the four of you to talk about the value of continued collaboration with China right now. I think we're looking so much at the risks, we often forget how important this has been. So just for you as an individual--individual or institutional level, how does continued and ongoing research in partnership with China benefit your institutions and the United States? (INAUDIBLE) down the line.

GIROD: Thank you very much for the opportunity to participate today, and for all of you taking interest in this as we certainly have great interest in this. And to that point, really, what makes our international research universities successful is, in fact, our collaborative nature and our open nature. And--and that's interacting with countries across the world and most certainly that includes China.

And our success, and quite frankly, the success of the United States, both economically, technologically and from the innovation perspective, has relied heavily on this environment and has driven our economy really since World War 2. And so, to your point, to not continue to embrace this approach of how our research universities work really, I think threatens our economy into the future. So--so I think it's absolutely critical that we continue to embrace this.

FENVES: Well, thank you, Jude. I'll pick up on Doug's comment. Since 1950, the United States has had the greatest talent program in the history of the world. It began with the National Science Foundation Act of 1950 and for the past 70 years, if you look at the economic advances in the United States, if you look at our national security, the health advances, so much of that has been tied to fundamental research that takes place at our--our universities in the United States. And around the world, we have been the leader in collaboration about open science, creating knowledge and educating future talent that will come up with the innovations and international collaboration has been essential for that.

And we as a nation should be concerned about the rise of China in academic research. If you look at their scientific papers, if you look at the amount of funding that is going into Chinese universities, they are an academic competitor with the United States and part of that is how do we--part of the question is how do we best collaborate with a very powerful academic competitor now?

COLEMAN: So it's ironic that in a few days, we're gonna be celebrating the 75th anniversary of the (INAUDIBLE) Bush Declaration after World War II to really heighten that in science, the endless frontier, that's what this is about. We have developed since World War II, the most powerful, the best universities in the world. We have attracted foreign talent. We have collaborated with our international partners, and we have created this enormous powerhouse that is based on competition for the best projects, competition for the best people and openness for fundamental research. We share, we share, we share and I think we are at our peril will lose this advantage that we've had.

But we also and I appreciate so much the working relationship that we're developing now with the Department of Justice and the FBI to let us know more about the threats. But they are because we cannot convince our faculty if they don't really have the information. So kudos to the federal government for bringing these groups together to help us really know what the threat is, develop the armor to protect ourselves from the threat, but not kill what has made us so powerful for the last 75 years.

LAUER: Thanks, Jude. From the point of view, the NIH collaboration, including international collaboration, is first and foremost to successful science. The current events with the Coronavirus and this brings back memories of what happened with SARS and then what we routinely deal with--with influenza points out that it is incredibly important for us to have strong collaborative relationships with China and with--with other nations around the world in order for our scientific enterprise to be successful.

NIH has collaborated with Chinese granting agencies. We've had longstanding collaborative program with the National Natural Science Foundation of China. But I think another important positive message here is that - and has pointed out in the Jason report is that our values of honesty, integrity, transparency, reciprocity, and merit-based competition, fair merit-based competition is something that maybe started with then, over Bush and has become an

international standard. And I think an important part of this discussion is that in our collaborations with other countries, including with China, these--these values should be first and foremost to the success of the enterprise.

BLANCHETTE: Great. Thanks, Mike. This concludes the positive portion of today's program. So now, I wanted to--to drill down a little bit on some of the more specific issues that we're wrestling with here and I want to start with the--the threat challenge side of this, which is before we move into the issue of how do we make sure where we're staying and open and free society. I think it's important to recognize that we are dealing with some sophisticated challenges that are really, I think, stressing the institutions of our free society and the four of you are at the core of this.

So given that there's sort of a mismatch between the institutions represented here, I'm going to ask something at a more general level to give you an opportunity to break this out in your own specific institution, which is there's a lot of issues that have arisen, at least in media coverage and at the national level stemming from cooperation with China. Obviously, Confucius Institutes are one of these in recent weeks, including some indictments that came down last week, the so-called--the talent programs of which the thousand talent is the most famous or infamous of these.

But I wanted to ask you, at your own institutional level, what are the--what are the pressing challenges that you see maybe these overlap with the ones we're talking about at a national level. But I'm more interested in what are the ones that we're really not talking about that you see as really pressing? And these could both be in terms of an incoming threat or in terms of implementing some of these responses that--that you're coming up with to deal with these. And happy to go down the line again, starting with you, Doug.

GIROD: Thank you. I think from our perspective, some of the challenges are that our systems are built to be open and collaborative and our policies are built to be open and collaborative and where we have regulation, it's really to be compliant with the environment in which we work. Our systems are not built for these issues and so really working with--with our federal colleagues to understand where those threats are and then how we can mitigate those in a way that does not impair what we're trying to do, but actually enables our faculty and students to continue to do what they do so well, but do so in a safe and secure fashion.

And some of that's on our end, it's--it's understanding how we have to modify our policies and some of it is information because quite frankly, we don't have access to this information. So if we're trying--if you want to go to the conflict of interest issue, if somebody discloses a conflict of interest, we have no way to assess that. And so we are going to need some help through this process as well.

BLANCHETTE: Doug, can I just--just a push on that one a bit. Can you talk about what--what are some of those specific challenges that are--that your systems are not built for?

GIROD: Well, I'll touch briefly on conflict of interest. So--so it's certainly how we enforce those. And what it means to violate a conflict of interest is--is really, I think, evolving at our institutions right now, and part of what we've seen happen is driving some of that. But--but again, it's also building a system in place that allows us to adequately understand where the risks are, what companies are a challenge, what--what are restricted entities, what are talent programs. And we don't have access to that information, that's certainly one.

Another one we're challenged with is--is our visitor program. So when we have people coming on our campus, do we even know who they are? Do we know where they're coming from? Do they know why they're there? And it's not to say we want that, we want to welcome them but--but it's becoming clear that we need to know who they are and not just for this reason. We just had an episode of a potential coronavirus person in our community and to not know who we have on our campus, when you have that that arise, it really creates a major challenge for us.

We also, to be honest, don't always know where our people are and includes our students and our faculty as they are going out and--and engaging in this collaboration, which is wonderful and that's what we encourage it to do, but we probably need a little better tracking system for that.

BLANCHETTE: Thank you.

FENVES: So our--our goal is to have our research enterprise open, collaborative, thriving as it has done throughout history, but also with integrity. So it's fundamentally a question of the integrity of the academic research that takes place at--at my university and our--other universities. And as we've been thinking about it at the University of Texas; there are four elements of that. The first is just communication with our faculty, aware--faculty awareness about what the environment is, what potential threats are, what their responsibilities are, what is integrity and how do we--how do we define integrity and monitor it.

That goes to the second point. As Doug had alluded to, we have a number of requirements that have evolved over the years from federal regulation, legal requirements on reporting information. And they've all--they all go to different offices depending on who asked for the information originally and which office maintained it. So we're in the process of merging the streams of reporting that faculty have to do and it's sometimes an onerous process. So maybe we can even simplify it but things like financial interests, things like outside commitments and potential conflicts of interest, those all have to be reported. But they go to different places right now, we're going to merge those.

Travel authorization, at least at (INAUDIBLE), every travel has to be authorized. It goes to a travel office, but not the Office of Research Integrity so we're going to merge that. Annual reports of faculty fill out and they don't like to do it but they have to fill them out. And so how does that information correlate with other reports that are provided?

And finally, we're going to start doing something that's at least new for us is that many faculty - I shouldn't say many - faculty do have research labs in other countries. Many in many cases, this is very advantageous. They can double their productivity, but it has to be disclosed, we have to know about it. And for the first time, we're gonna have all grants run through our grant management system, even if the grant doesn't even come to the university so that we can monitor all activities and--and help advise faculty where there is potential conflict or where there are areas of concern.

Finally, other grants that are coming to the university gifts, other agreements, we have been and will continue to do more due diligence about the origin of those gifts, the purpose of the gifts and the provenance of those types of agreements. And finally, this has been something that's relatively new for us over the past couple of years, very strong collaboration with our local FBI office and local law enforcement. We have a very I think, a very good relationship. That kind of general information helps convey to the faculty what--what the risks are. But we also need specific information, even though if some of it may be confidential or--or classified, and I would encourage all universities to--to work with their local FBI office and develop that that type of ongoing relationship.

And finally, working with the federal agencies, NIH and the other science agencies, we have very close relationship. What are their concerns? What are they looking for? We hope the agencies work together so that we have a fairly unified and uniform way of dealing with these issues but--but they are the funders and they represent the taxpayers of the United States and we want to be responsible to the federal--federal S&T (SP) agencies.

COLEMAN: So before I came to AAU, I was president of the University of Michigan and before that president of the University of Iowa. So I can sympathize with my colleagues about all the issues that they face. Universities are inherently very decentralized places, and that has been a strength for us because it's encouraged innovation, it's encouraged faculty to do out-of-the-box things and try some things that may fail and so that's been helpful.

But now we're in an environment where we must have more coordination, more centralization. I mean, I understand precisely the problem when all these--info--this information goes to different places within the university and we're not used to the command and control environment, we're just not. And I don't think we need to go to a command and control environment, but we have got to get more sensible about how we coordinate everything, how we know what is going on within the--within our own institutions.

And we're talking about this a lot now at AAU and we work very closely with APLU and ACE to make sure that we are distributing this information. I will tell you what's been the most helpful thing to convince the faculty are some of these cases that are being prosecuted. When they see a department chair at Harvard being called to account and who may go to jail, believe me, that has done more to help us than anything abstract that we could possibly have

done. And so, I applaud bringing those things to the public so that we can then go to our universities and say, look at what is going to happen if you don't pay attention to what we are asking you now to do. So that's been helpful.

LAUER: So I'll extend on Mary Sue. I think one of the important challenges is to recognize and communicate that the behaviors that we're seeing and that we're seeing at NIH constitute egregious ethical breaches. These are not subtle. So as an example, we've actually had several cases of this, of people, scientists who have obtained funds through their Chinese employment, undisclosed Chinese employment, they've obtained grants from Chinese grading agencies that are absolutely identical or very similar to the grants that are funded by NIH.

We actually had a case where a translator said to us, you know, I don't really need to continue translating the grant because you have the translation, it's the grant that you funded. Now, that is not collaboration, that's cheating, that's double-dipping, that's absolutely wrong. And the university leader had no trouble with that and when we said we need to get a refund because this was duplicative funding, they totally understood it.

But there's another way of thinking about that as well, which is that someone else didn't get a grant-funded. We only find about 20 percent of the grants that we get. So somebody got a grant through duplicitous means, and meanwhile, somebody else who may have--this may have been the grant that could have cured cancer, didn't get funded because of this cheating. Now, another example that we've seen where unfortunately we've seen a fair number of these cases deals with peer review.

So when scientists send in their applications for peer review, they assume that the process will remain confidential, that the only people who will see their nascent and innovative ideas are peer reviewers and NIH staff who has a business to know. Well, we know it's been reported in the press. There have been cases in which reviewers who have connections to--to institutions in China have e-mailed their applications to China. And these are confidential applications that have been e-mailed away. This is not collaboration. this is cheating, this is absolutely wrong and nobody really would have too much difficulty understanding that. So I think this is an important message that we need to send.

BLANCHETTE: I wonder if I could just drill down a little bit more on this decentralization issue, which in many ways is--it is a structural problem that we face. You'd referenced there's a case indictment that came last week from a small university in the greater Cambridge, Massachusetts area. And I, you know, one of the striking things reading through the indictment a couple of days ago was that this individual, as a professor, a department chair at this university, had signed an agreement with a foreign university using the name of this university. It looked like an official agreement as far as the Chinese partner was concerned without consulting the university and that this had gone on for a long time, I think probably until I forget the exact date in the indictment.

If someone is--is dedicated to circumventing or exploiting the decentralization, how do we--how does a university ever get around that problem? I mean, this--this particular detail I found quite glaring. So, you know, I have a hard time understanding, was that an outlier or is there a more structural ability to exploit the decentralization and what, if anything, can--can be done about that? I mean, obviously, relying on the--the FBI to be the sort of think tank that's out there doing the research for universities is untenable. I suspect you won't be hiring a threat cell that is just dedicated to this. What can we do?

COLEMAN: So I won't--I don't want to assume that there are a lot of bad actors out there deliberately trying to cheat. They're always going to be some bad actors. You know, we understand that but I--I do happen to think that's in the minority. I think until the recent time - and Greg, I'd be interested and Doug in your thought about this, too - until this recent last couple of years when this conversation has really been elevated and we've got more evidence to talk to our faculty about so that they're now convinced, they see these cases now. That's why the case prosecutions are so valuable. But I think more likely has been and I confronted this when I was back at a conference at Michigan about a year ago. It's just innocence and--and you know, and we were talking on a panel about how you need to disclose every single dollar that you are getting for your research, regardless of the source. You need to disclose it.

And I had a very innocent young person who probably young faculty member in the audience said, well, I knew I had to disclose my U.S. sources, but I didn't think I had to disclose international. And I said, no, no, no, no. When it says disclose every dollar, we mean every dollar from every single source that it possibly comes. So these efforts at education, this rising of this information, I think has been very instructive to people who are just innocent. And I have to believe that there's some innocent people out there and they're not all guilty. And so I don't want us to create some sort of a terrible approach where we assume that everybody's guilty.

FENVES: Jude, on your specific question of how--how do we detect this? The--our university is very protective of our name. So it's a--it's--we have a--a lot of ways, especially with social media, it's very easy to find when the university's name is being used somewhere. So we--we actually monitor that and when it comes up, we try to track down unauthorized use the names. So it could be in China, it could be in Kansas. You know, we--we want to make sure that the university is--name is used and only an author--authorized way.

GIROD: You know, flag flying on top of my building at our last football game was not authorized. You know, I think increasingly it's a matter of building some of the infrastructure that Greg was just talking about, of how we--we help inform and--inform what is needed, why it's needed, help inform decisions that faculty are making because they are challenged also to understand what's a really exciting collaboration and what's maybe a challenging collaboration.

So we've actually formed an office of global operations and Security that we've had for--for at least four years now and really came out of conversations, frankly, with our original FBI people as a--we've been having these conversations about some potential challenges and as we think about how do we address some of those. So this office is really trying to focus on helping our faculty and our students be--be highly successful and do what they want to do, but do so in a safe and secure fashion.

So it's everything from accessing some of these collaboration, assessing the international contracts, every contract, every affiliation that we do now goes through this office for assessment. We're doing more so on the travel side for safety as much as security and then for--informing our people when they are traveling internationally, what the risks are associated with that and what they can do to mitigate those risk in terms of what devices they take and those sorts of things. And so this has really helped it--IT'S also my intermediaries as I've stepped into this world. This--this group helps me interact with our federal agencies, our partners who've been great, both the regional FBI, but also the U.S. attorney's office. And there's a couple representatives here today so thank you for being here. They've been great partners but this office has really helped us translate that out of their world into our world.

BLANCHETTE: Mike, I wonder if I could ask you a question as a--as a grant-giving body an age has also been thinking through some of these issues and trying to do its own investigations to determine the behavior of grantees. I saw a memo that--that your boss, Francis Collins, had written in August 2013.

NIH is aware that some foreign entities have mounted systematic programs to influence NIH researchers and peer reviewers and to take advantage of the long tradition of trust, fairness, and excellence. NIH supported research activities. You said there are three areas or three buckets that NIH would be working towards; improving accuracy of reporting of all sources of research, support, financial interests, relevant affiliations, mitigation of rest IP security, and exploring steps to protect intact--research and integrity. I was wondering if I could get a sense from you on--on what actions have been taken and where these--these three buckets where they stand today.

LAUER: So these concerns that we had and that we articulated back in 2018. I think the only modification I would make is that, if anything, it's worse than what we thought back then. As--as the Jason report said, we--we don't fully understand the scope of the problem, but it does appear to continue to grow. We have taken actions on both a--on a macro level and on a micro-level. In that memo, we indicated that if there were scientists of concern that we would be reaching out to individual universities to engage in dialog with them and we have done that.

We have contacted over 80 universities so far, about approximately 180 scientists and we're continuing to do that. And I have to say, this is consistent with a comment that was made earlier this morning that we're observing that universities are being remarkably responsive and working with us to discover what's been going on on their

campuses and sometimes what they discover is rather shocking to them that their faculty have engaged in--in very disturbing behavior.

So that's on the micro-level and we have seen all of those. We've seen diversions of intellectual property, we have seen duplicative funding, undisclosed conflicts of interest, peer review violations, everything that we said that we talked about in that letter, we have seen. And then we've also worked on a macro level. And here, I want to particularly compliment OSTP, the Office of Science Technology Policy, Kelvin Drogin Meyer (SP) has led an effort.

We have a committee of the National Science and Technology Council on Science and Security. I'm one of the co-chairs of that committee. And what this committee has done is it's brought to--to together, the major funding agencies, including NIH, NSF, DOD, DOE, and many others. And we're working together on a on an outreach package, a communications package, messaging, harmonizing our--our approaches and the way we--we think about these concerns. So on both the macro level and micro level, there's been a huge amount of work that--that's been going.

BLANCHETTE: I want to be cognizant of time and I realize there's--there's just so much to get through here. But we've got ten, eleven minutes left. I wanted to flip the equation, so to speak, and talk about the responsibility that the four institutions have, but also the national responsibility we have to maintain an atmosphere of open collaboration safety for whether those are Chinese researchers, students or--or ethnic Chinese American citizens.

This has been--I reached out to some colleagues and friends before this to get a sense of what questions I should ask and thought--that the ratio was pretty heavily tipped towards. Are we overreaching? Is this a witch hunt? Some of the cases that have been in the news do appear troubling in terms of some of the investigations that have been ongoing. I've heard this personally from--from Chinese friends, but also Chinese American friends. I'd like to ask for going down the line, again and again, I think broadly we're all going to agree it's a problem. But so I'd like to drill down beyond that of simply a Kumbaya statement to more what are you doing at an institutional level to maintain a not only an open environment but a welcoming environment?

GIROD: Thank you, Jude. I think this is absolutely a very real issue and I think as time has gone on and the conversations have continued, it's gotten to be a little bit easier to--to help people understand that this is not an ethnic issue, this is not a race issue. This is a challenge of a particular handful of--of--of governments, quite frankly, I mean, we certainly saw that currently predominately we're dealing with China but we are dealing with other countries with this issue as well.

And so helping them understand that what we're dealing with is an organized effort of governments, not of people and--and that we--we still welcome and--and encourage not only collaboration, but we welcome them to our campuses and we want them to be on our campuses. And that's a constant tension as--as we're dealing with this. And so repeating that message as frequently as possible is certainly one strategy we've tried to use.

BLANCHETTE: Are there any specific measures or policies or anything besides just reinforcing a message of openness, is there anything specific that--that the university is doing?

GIROD: In terms of maintaining openness.

BLANCHETTE: Yeah. Or--or I guess to add onto that in terms of how you work with law enforcement officials to--to ensure that if students or faculty be investigating, that their rights are being protected.

GIROD: Absolutely. I mean, our general counsel's office is very engaged in that as well and we take that very seriously. And--and I think Maria Sue comments are appropriate as a couple of these cases have come to fruition. It's helped us all understand a little bit more what they are looking like and how to do it in a way that preserves individual freedom and academic freedom. And--and but it's--it's a shift of culture for us and--and so trying to think about to your point, trying to think how we preserve what's so wonderful about our system and so successful and yet address what is clearly a very serious need.

FENVES: Well, I think the Keys are, first of all, recognizing we're looking for mirror, we're looking for the best talent and the best ideas. We're supporting that institutionally without any--any--any bias whatsoever, we're protecting academic freedom, we're communicating these values clearly both university-wide and within to down to individual faculty that have concerns. A lot of it--a lot of it is communication.

And again, I want to also echo what Mary Sue said. Some of the cases that have come--come--come out publicly are so egregious that actually helps in the communication effort. We're not talking about missing a deadline on filing a report or an oversight that is--is realized and then fixed. These cases are so egregious. I haven't heard anyone on our faculty saying, well, that's a concern that--that those are--those are being prosecuted. Nobody--nobody supports those and supports an open, collaborative research environment.

COLEMAN: Well, from the standpoint of an association, since we're a collection of 65 universities, you know, we have this topic on our agenda every time our presidents and chancellors meet. I mean, we're talking about it, talking about what we're doing. We're gathering information about--about how our institutions dealing with the issue of conflict of commitment and conflict of interest.

I mean, because these have nothing to do--these aren't countries specific. I mean, these have to do with your integrity as a researcher. And I think that's what you're getting to as well, Mike, is they keep emphasizing that these, you know, we're asking people to live up to the standards that we think are important for any good scientist or for that matter, you know, any--any scholar to live up to.

And I think it's our continuing focus on that point that has been--it's been very important for us and for them--for--what we can do as an association, that's the most beneficial is when we gather our presidents and chancellors together twice a year, we talk about the issue, we talk about what we're doing, we talk about best practices that are--that various campuses have and we're sharing an awful lot of information. And that sharing not among ourselves as well as with agencies of the federal government, has been one of the most beneficial things that I've seen evolving in the last couple of years.

LAUER: John, I will echo that we have been quite amazed at so at how our institutions and groups of institutions have come together to--to improve their--their systems and controls while also maintaining an atmosphere of collaboration and openness. I do think an important message for scientists is that we're not looking for late forms or forms that haven't been filled out incorrectly. What we're dealing with are egregious ethical breaches. But how does one avoid those? And one way of thinking about this is never be afraid to ask for help.

If somebody is asking you to sign a piece of paper, a contract, but particularly if it's in a--in a system that you're not used to in a foreign country, don't sign it. Say, I need to go to my VPR and or my office of general counsel and I need to have them look at it. And we've sometimes said we've looked at some of the contracts, we've looked at now dozens of contracts that scientists have signed without the knowledge or approval of university officials. And I'll sometimes ask, had you seen this, had this faculty members shown this to you before, before he signed it, what would you have said? And it would be something like absolutely no way.

Now, we did see one institution that way back, long before this became a public matter caught one their faculty in one of these situations. It actually said, look, if you want to set up a legitimate collaboration, we're happy to work with you. And well, what we'll do is at our institutional level, we will work with our counterparts in China and we will set something up and we'll set up a joint program. And that's exactly what happened. And that's a happy ending story. And in that case, the systems actually worked very well. We've actually shared the system that they put in place with OSTP as an example of the best practice.

BLANCHETTE: Again, cognizant of time. We're just going to spend the last four or five minutes here. I'm just going to ask folks to go down the line. But if there is one concrete specific suggestion that you'd have for--for the U.S. government, but DOJ, FBI on how we can make this system better, what would it be? I'll give you 15 seconds to think of that as I was going to do, is we don't have time to answer these questions, but respectful of the people who have put forward the questions. And so folks have an idea of--of what people are interested in.

I'm just going to summarize some of the questions that--that came in. One was on Confucius Institutes, which the NDAA has made an easier thing for some universities getting research funding. But the second is and I'm going to reword this one slightly, is how do we partner with a China and the Communist Party now that its political trajectory seems to be heading in a more authoritarian direction? This one is about how to--protecting the rights of Chinese citizens on--on campuses here who may have opinions that are divergent from the Chinese government, whether that's on the situation in Shenyang, on Hong Kong or in the situation of Tibetans.

And one is asking, again, just emphasizing the concern for ethnic Chinese faculty on campuses and--and investigations by the FBI. What is being done to protect--to protect their rights? So those are just some of the questions we got. I hope that bought you a little bit of time. So in--in a spirit of constructive criticism or advice, what can the U.S. government be doing better?

GIROD: Well, I guess mine would be a plead for consistency and an organized effort that we can come up with one set of guidelines, rules, regs, and reporting and not 10 because that will not be manageable.

FENVES: I will repeat that one. I think that's absolutely essential for the future of the research enterprise in the United States and at our universities. The second you specifically asked about law enforcement and FBI, as I said, we have a very good relationship as we can have more specific information that helps us to identify specific problems that that would be beneficial.

And I think somebody Doug mentioned, we do have issue of how do we do proper due diligence on visitors, visiting scholars. We want them, that's an important part of international collaboration and international exchange. But I think there is more that--that needs to be done. And every university can't figure it out on its own because we don't have--have the resources or the expertise to do it. So some coordination on--on how to properly do due diligence on--on visitors.

And the third is we've had a lot of discussion about IP. At fundamental research, the real IP is in people's heads, it's the talent themselves. And of course, we attract the best students from around the world, including China. We spend a lot of money training them, they get a lot of expertise, they add a lot to the research enterprise, and the semiconductor industry in the telecommunication industry would like to hire them, I think. And so if we can do a better job on immigration for these very talented students who are contributing to the U.S. research enterprise, I think that would be long term beneficial.

COLEMAN: So I'm going to resoundingly second everything my colleagues have said. But something that I think we haven't talked at all about today that I think would be extraordinarily useful is to have the U.S. government and federal agencies start investing in Chinese language study. We don't have nearly enough students in this country. We did it. We did crash courses in Russian back in the Cold War. We've done nothing about China. The Chinese language is extraordinarily important. And we need to have more investment in getting our own people fluent in this language because now we can't even read all the stuff that's coming out.

LAUER: So since I work for the government, I won't give advice to myself. But--but I will take your question to give one very practical piece of advice to academic leadership, which is please have a very low threshold to tell us about potential problems. And you can call me directly, you can e-mail me directly. Many academic leaders have, and I think this has turned into a useful partnership. So please don't hesitate to contact me anytime.

BLANCHETTE: And with that and two minutes early. We will conclude. Again, thank you, everyone. There's obviously a lot we couldn't discuss today, but I appreciate the discussion.

Load-Date: February 16, 2020