China's Attempt to Influence U.S. Institutions: A Conversation with FBI Director Christopher Wray

TRANSCRIPT

- Walter Russell Mead, *Ravenel B. Curry III Distinguished Fellow in Strategy and Statesmanship, Hudson Institute*
- Christopher Wray, *Director of the Federal Bureau of Investigation*

Disclaimer: This transcript is based off of a recorded video conference and breaks in the stream may have resulted in mistranscriptions in the text.

A video of the event is available: https://www.hudson.org/events/1836-video-event-china-s-attempt-to-influence-u-s-institutions-a-conversation-with-fbi-director-christopher-wray72020

Walter Russell Mead:

Well, hello. And thank you for joining today's event at Hudson Institute, where we are all appropriately masked and physically distancing. We're here with FBI director, Christopher Wray. And it's my pleasure to be physically back at the office, and it's an honor to join the director in today's conversation. Christopher Wray currently serves as the eighth director of the FBI. Throughout his career, he has served in a number of roles within the federal government, including as the principal associate attorney general in the office of the deputy attorney general, where he oversaw investigations conducted by the DOJ's law enforcement agencies.

In 2003, President George W. Bush nominated Mr. Wray as the assistant attorney general for DOJ's criminal division, where he oversaw major investigations into domestic and international criminal activities. He also oversaw the DOJ's counter terrorism, counterintelligence, and export control sections. Mr. Wray was instrumental in the DOJ's post 9/11 efforts to combat terrorism, cyber crime, and international espionage. Today, Mr. Wray joins us to discuss China's ongoing efforts to interfere in the United States domestic affairs through espionage, disinformation campaigns, intellectual property theft, and monetary theft. It is my pleasure to welcome Director Wray to the Hudson Institute.

Christopher Wray:

Well, thank you, Walter.

Good morning. I realize it's challenging to put on an event like this under the current circumstances, so I'm grateful to the Hudson Institute for hosting us today.

The greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China. It's a threat to our economic security—and by extension, to our national security.

As National Security Advisor O'Brien said in his recent remarks, we cannot close our eyes and ears to what China is doing—and today, in light of the importance of this threat, I'll provide more detail on the Chinese threat than the FBI has ever presented in an open forum. This threat is so significant that the attorney general and secretary of state will also be addressing a lot of these issues in the next few weeks. But if you think these issues are merely a government problem, or just an intelligence issue, or a nuisance largely just for big corporations who can take care of themselves—you couldn't be more wrong.

It's the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history.

If you are an American adult, it is more likely than not that China has stolen your personal data.

In 2017, the Chinese military conspired to hack Equifax and made off with the sensitive personal information of 150 million Americans—we're talking nearly half of the American population and most American adults—and as I'll discuss in a moment, this was hardly a standalone incident.

Our data isn't the only thing at stake here—so are our health, our livelihoods, and our security.

We've now reached the point where the FBI is opening a new China-related counterintelligence case about every 10 hours. Of the nearly 5,000 active FBI counterintelligence cases currently under way across the country, almost half are related to China. And at this very moment, China is working to compromise American health care organizations, pharmaceutical companies, and academic institutions conducting essential COVID-19 research.

But before I go on, let me be clear: This is not about the Chinese people, and this is certainly not about Chinese Americans. Every year, the United States welcomes more than 100,000 Chinese students and researchers into this country. For generations, people have journeyed from China to the United States to secure the blessings of liberty for themselves and their families—and our society is better for their contributions. So, when I speak of the threat from China, I mean the government of China and the Chinese Communist Party.

The Chinese Regime and the Scope of Its Ambitions

To understand this threat and how we must act to respond to it, the American people should remember three things.

First: We need to be clear-eyed about the scope of the Chinese government's ambition. China—the Chinese Communist Party—believes it is in a generational fight to surpass our country in economic and technological leadership.

That is sobering enough. But it's waging this fight 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, China is engaged in a whole-of-state effort to become the world's only superpower by any means necessary.

A Diverse and Multi-Layered Approach

The second thing the American people need to understand is that China uses a diverse range of sophisticated techniques—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, ostensibly private companies, certain kinds of graduate students and researchers, and a variety of other actors working on their behalf.

Economic Espionage

To achieve its goals and surpass America, China recognizes it needs to make leaps in cutting-edge technologies. But the sad fact is that instead of engaging in the hard slog of innovation, China often steals American intellectual property and then uses it to compete against the very American companies it victimized, in effect cheating twice over. They're targeting research on everything from military equipment to wind turbines to rice and corn seeds

Through its talent recruitment programs, like the so-called Thousand Talents Program, the Chinese government tries to entice scientists to secretly bring our knowledge and innovation back to China—even if that means stealing proprietary information or violating our export controls and conflict-of-interest rules.

Take the case of scientist Hongjin Tan, for example, a Chinese national and American lawful permanent resident. He applied to China's Thousand Talents Program, stole more than $1 billion worth of trade secrets from his former employer, an Oklahoma-based petroleum company, and got caught. A few months ago, he was convicted and sent to prison.

Or there's the case of Shan Shi, a Texas-based scientist, also sentenced to prison earlier this year. Shi stole trade secrets regarding syntactic foam, an important naval technology used in submarines. Shi, too, had applied to China's Thousand Talents Program, and specifically pledged to "digest" and "absorb" the relevant technology in the United States. He did this on behalf of Chinese state-owned enterprises, which ultimately planned to put the American company out of business and take over the market.

In one of the more galling and egregious aspects of the scheme, the conspirators actually patented in China the very manufacturing process they'd stolen, and then offered their victim American company a joint venture using its own stolen technology. We're talking about an American company that spent years and millions of dollars developing that technology, and China couldn't replicate it—so, instead, it paid to have it stolen.

And just two weeks ago, Hao Zhang was convicted of economic espionage, theft of trade secrets, and conspiracy for stealing proprietary information about wireless devices from two U.S. companies. One of those companies had spent over 20 years developing the technology Zhang stole.

These cases were among more than a thousand investigations the FBI has into China's actual and attempted theft of American technology—which is to say nothing of over a thousand more ongoing counterintelligence investigations of other kinds related to China. We're conducting these kinds of investigations in all 56 of our field offices. And over the past decade, we've seen economic espionage cases with a link to China increase by approximately 1,300 percent.

The stakes could not be higher, and the potential economic harm to American businesses and the economy as a whole almost defies calculation.

Clandestine Efforts

As National Security Advisor O'Brien discussed in his June remarks, the Chinese government is also making liberal use of hacking to steal our corporate and personal data—and they're using both military and non-state hackers to do it. The Equifax intrusion I mentioned a moment ago, which led to the indictment of Chinese military personnel, was hardly the only time China stole the sensitive personal information of huge numbers of the American public.

For example, did you have health insurance through Anthem or one of its associated insurers? In 2015, China's hackers stole the personal data of 80 million of that company's current and former customers.

Or maybe you're a federal employee—or you used to be one, or you applied for a government job once, or a family member or roommate did. Well, in 2014, China's hackers stole more than 21 million records from OPM, the federal government's Office of Personnel Management.

Why are they doing this? First, China has made becoming an artificial intelligence world leader a priority, and these kinds of thefts feed right into China's development of artificial intelligence tools.

Compounding the threat, the data China stole is of obvious value as they attempt to identify people to target for secret intelligence gathering. On that front, China is also using social media platforms—the same ones Americans use to stay connected or find jobs—to identify people with access to our government's sensitive information and then target those people to try to steal it.

Just to pick one example, a Chinese intelligence officer posing as a headhunter on a popular social media platform recently offered an American citizen a sizeable sum of money in exchange for "consulting" services. That sounds benign until you realize those "consulting" services were related to sensitive information the American target had access to as a U.S. military intelligence specialist.

Now that particular tale has a happy ending: The American citizen did the right thing and reported the suspicious contact, and the FBI, working together with our armed forces, took it from there. I wish I could say that all such incidents worked out that way.

Threats to Academia

It's a troublingly similar story in academia.

Through talent recruitment programs like the Thousand Talents Program I mentioned a moment ago, China pays scientists at American universities to secretly bring our knowledge and innovation back to China—including valuable, federally funded research. To put it bluntly, this means American taxpayers are effectively footing the bill for China's own technological development. China then leverages its ill-gotten gains to undercut U.S. research institutions and companies, blunting our nation's advancement and costing American jobs. And we are seeing more and more of these cases.

In May alone, we arrested both Qing Wang, a former researcher with the Cleveland Clinic who worked on molecular medicine and the genetics of cardiovascular disease, and Simon Saw-Teong Ang, a University of Arkansas scientist doing research for NASA. Both were allegedly committing fraud by concealing their participation in Chinese talent recruitment programs while accepting millions of dollars in American federal grant funding.

That same month, former Emory University professor Xiao-Jiang Li pled guilty to filing a false tax return for failing to report the income he'd received through China's Thousand Talents Program. Our investigation found that while Li was researching Huntington's disease at Emory, he was also pocketing half a million unreported dollars from China.

In a similar vein, Charles Lieber, chair of Harvard's Department of Chemistry and Chemical Biology, was indicted just last month for making false statements to federal authorities about his Thousand Talents participation. The United States has alleged that Lieber concealed from both Harvard and the NIH his position as a strategic scientist at a Chinese university—and the fact that the Chinese government was paying him, through the Wuhan Institute of Technology, a $50,000 monthly stipend, more than $150,000 in living expenses, and more than $1.5 million to establish a laboratory back in China.

Malign Foreign Influence

There's more. Another tool China and the Chinese Communist Party use to manipulate Americans is what we call malign foreign influence.

Now, traditional foreign influence is a normal, legal diplomatic activity typically conducted through diplomatic channels. But malign foreign influence efforts are subversive, undeclared, criminal, or coercive attempts to sway our government's policies, distort our country's public discourse, and undermine confidence in our democratic processes and values.

China is engaged in a highly sophisticated malign foreign influence campaign, and its methods include bribery, blackmail, and covert deals. Chinese diplomats also use both open, naked economic pressure and seemingly independent middlemen to push China's preferences on American officials.

Just to take one all-too-common example, let's say China gets wind that an American official is planning to travel to Taiwan—think a governor, a state senator, a member of Congress. China does not want that to happen, because that travel might appear to legitimize Taiwanese independence from China—and legitimizing Taiwan would be contrary, of course, to China's "One China" policy.

So what does China do? Well, China has leverage over the American official's constituents—American companies, academics, and members of the media all have legitimate and understandable reasons to want access to Chinese partners and markets. And because of the authoritarian nature of the Chinese Communist Party, China has immense power over those same partners and markets. So, China will sometimes start by trying to influence the American official overtly and directly. China might openly warn that if the American official travels to Taiwan, China will take it out on a company from that

official's home state by withholding the company's license to manufacture in China. That could be economically ruinous for the company, would directly pressure the American official to alter his travel plans, and the official would know that China was trying to influence him.

That would be bad enough. But the Chinese Communist Party often doesn't stop there; it can't stop there if it wants to stay in power—so it uses its leverage even more perniciously. If China's more direct, overt influence campaign doesn't do the trick, they sometimes turn to indirect, covert, deceptive influence efforts.

To continue with the example of the American official with travel plans that the Chinese Communist Party doesn't like, China will work relentlessly to identify the people closest to that official—the people the official trusts most. China will then work to influence those people to act on China's behalf as middlemen to influence the official. The co-opted middlemen may then whisper in the official's ear and try to sway the official's travel plans or public positions on Chinese policy. These intermediaries of course aren't telling the American official that they're Chinese Communist Party pawns—and worse still, some of these intermediaries may not even realize they're being used as pawns, because they too have been deceived.

Ultimately, China doesn't hesitate to use smoke, mirrors, and misdirection to influence Americans.

Similarly, China often pushes academics and journalists to self-censor if they want to travel into China. And we've seen the Chinese Communist Party pressure American media and sporting giants to ignore or suppress criticism of China's ambitions regarding Hong Kong or Taiwan. This kind of thing is happening over and over, across the United States.

And I'll note that the pandemic has unfortunately not stopped any of this—in fact, we have heard from federal, state, and even local officials that Chinese diplomats are aggressively urging support for China's handling of the COVID-19 crisis. Yes, this is happening at both the federal and state levels. Not that long ago, we had a state senator who was recently asked to even introduce a resolution supporting China's response to the pandemic.

The punchline is this: All these seemingly inconsequential pressures add up to a policymaking environment in which Americans find themselves held over a barrel by the Chinese Communist Party.

Threats to the Rule of Law

All the while, China's government and Communist Party have brazenly violated well-settled norms and the rule of law.

Since 2014, Chinese General Secretary Xi Jinping has spearheaded a program known as "Fox Hunt." Now China describes Fox Hunt as an international anti-corruption campaign—it's not. Instead, Fox Hunt is a sweeping bid by General Secretary Xi to target Chinese nationals whom he sees as threats and who live outside China, across the world. We're talking about political rivals, dissidents, and critics seeking to expose China's extensive human rights violations.

Hundreds of the Fox Hunt victims that they target live right here in the United States, and many are American citizens or green card holders. The Chinese government wants to force them to return to China, and China's tactics to accomplish that are shocking. For instance, when it couldn't locate one Fox Hunt target, the Chinese government sent an emissary to visit the target's family here in the United States. The message they said to pass on? The target had two options: return to China promptly, or commit suicide. And what happens when Fox Hunt targets refuse to return to China? In the past, their

family members both here in the United States and in China have been threatened and coerced; and those back in China have even been arrested for leverage.

I'll take this opportunity to note that if you believe the Chinese government is targeting you—that you're a potential Fox Hunt victim—please reach out to your local FBI field office.

Exploiting Our Openness

Understanding how a nation could engage in these tactics brings me to the third thing the American people need to remember: China has a fundamentally different system than ours—and it's doing all it can to exploit our openness while taking advantage of its own, closed system.

Many of the distinctions that mean a lot in the United States are blurry or almost nonexistent in China—distinctions between the government and the Chinese Communist Party, between the civilian and military sectors, and between the state and "private" industry.

For one thing, an awful lot of large Chinese businesses are state-owned enterprises—literally owned by the government, and thus the Party. And even if they aren't, China's laws allow its government to compel any Chinese company to provide any information it requests—including American citizens' data.

On top of that, Chinese companies of any real size are legally required to have Communist Party "cells" inside them to keep them in line. Even more alarmingly, Communist Party cells have reportedly been established in some American companies operating in China as a cost of doing business there.

These features should give U.S. companies pause when they consider working with Chinese corporations like Huawei—and should give all Americans pause, too, when relying on such a company's devices and networks. As the world's largest telecommunications equipment manufacturer, Huawei has broad access to much that American companies do in China. It's also been charged in the United States with racketeering conspiracy and has, as alleged in the indictment, repeatedly stolen intellectual property from U.S. companies, obstructed justice, and lied to the U.S. government and its commercial partners, including banks.

The allegations are clear: Huawei is a serial intellectual property thief, with a pattern and practice of disregarding both the rule of law and the rights of its victims. I have to tell you, it certainly caught my attention to read a recent article describing the words of Huawei's founder, Ren Zhengfei, about the company's mindset. At a Huawei research and development center, he reportedly told employees that to ensure the company's survival, they need to—and I quote—"surge forward, killing as you go, to blaze us a trail of blood." He's also reportedly told employees that Huawei has entered, to quote, "a state of war." I certainly hope he couldn't have meant that literally, but it's hardly an encouraging tone, given the company's repeated criminal behavior.

In our modern world, there is perhaps no more ominous prospect than a hostile foreign government's ability to compromise our country's infrastructure and devices. If Chinese companies like Huawei are given unfettered access to our telecommunications infrastructure, they could collect any of your information that traverses their devices or networks. Worse still: they'd have no choice but to hand it over to the Chinese government if asked—the privacy and due process protections that are sacrosanct in the United States are simply non-existent in China.

Responding Effectively to the Threat

The Chinese government is engaged in a broad, diverse campaign of theft and malign influence, and it can execute that campaign with authoritarian efficiency. They're calculating. They're persistent. They're

patient. And they aren't subject to the righteous constraints of an open, democratic society or the rule of law.

China, as led by the Chinese Communist Party, is going to continue to try to misappropriate our ideas, influence our policy makers, manipulate our public opinion, and steal our data. They will use an all-tools and all-sectors approach—and that demands our own all-tools and all-sectors approach in response.

Our folks at the FBI are working their tails off every day to protect our nation's 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 to our intelligence capabilities.

I'll briefly note that we're having real success. With the help of our many foreign partners, we've arrested targets all over the globe. Our investigations and the resulting prosecutions have exposed the tradecraft and techniques the Chinese use, raising awareness of the threat and our industries' defenses. They also show our resolve, and our ability to attribute these crimes to those responsible. It's one thing to make assertions—but in our justice system, when a person, or a corporation, is investigated and then charged with a crime, we have to prove the truth of the allegation beyond a reasonable doubt. The truth matters—and so, these criminal indictments matter. And 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 our partners abroad. We can't do it on our own; we need a whole-of-society response. That's why we in the intelligence and law enforcement communities are working harder than ever to give companies, universities, and the American people themselves the information they need to make their own informed decisions and protect their most valuable assets.

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. It does not mean we shouldn't welcome Chinese students or coexist with China on the world stage. But it does mean that when China violates our criminal laws and international norms, we're not going to tolerate it, much less enable it. The FBI and our partners throughout the U.S. government will hold China accountable and protect our nation's innovation, ideas, and way of life—with the help and vigilance of the American people.

Thank you for having me here today.

Walter Russell Mead:

Thank you, Director. We will be taking questions from people who weren't able to be here today, so if you could email any questions you have to events@hudson.org. That's H-U-D-S-O-N.org. We'll be happy to take a look at them. A Hudson staff member will get it. The questions will be collated, and we'll see if we can get your question to the director. But before that, I have a few of my own that I'd like to ask. And the first one is one I think that may be on the minds of a lot of Americans who listened to your talk. And they hear that China is stealing personal data, and that their efforts may be intensifying. What would you suggest for Americans who are concerned about their own personal data security from China or other hostile foreign actors?

Christopher Wray:

Well, I think the American people need to be taking steps on their own to protect their data as well, so that includes things like changing your passwords frequently. That includes things like monitoring your credit history and you account transactions to see if somebody may have stolen your identity. We have

a whole bunch of information about that kind of thing on the FBI's website. And if people have more questions, they can reach out to their local FBI field office.

Walter Russell Mead:

Okay. Great. And how would they find their local FBI field office?

Christopher Wray:

It's pretty easy to find online.

Walter Russell Mead:

Okay. Terrific. You said that there has been a trend of increasing cooperation among different countries on this. Can you talk about that a little bit?

Christopher Wray:

Right. So one of the things that I actually have found most encouraging in the middle of everything I just finished talking about, is the degree of alignment and consensus that seems to be growing between the United States and our foreign partners on this threat, on the severity of the threat, the priority of the threat, the importance of working together to combat the threat. I find that when I sit down with my foreign partners, which I do all the time, that this threat, the Chinese threat, is one of the first things they want to talk about, even when it wouldn't be necessarily on my agenda. And I see the same thing, frankly, happening with the business community, with academia, both here in the US and elsewhere.

In fact, in many ways, in a time in this country where things often seem so divisive, sometimes it feels like people in this country can't even agree on what day of the week it is. On this threat, on the Chinese threat, on the seriousness of it, on the priority of it, on the need to come together to tackle the threat, I'm actually seeing a level of alignment and consensus, bipartisan, across the both public and private sector, with academia, and as you noted in your question, with foreign partners, in a way that I've never seen in my career. And I think that's good news.

Walter Russell Mead:

That is certainly different from a lot of the narrative that we hear. Do you get any sense that China is targeting the November elections? Do you have any special concerns about that?

Christopher Wray:

Well, I would say that of course China's malign foreign influence campaign targets our policies, our positions, 24/7, 365 days a year. So it's not an election specific threat. It's really more of an all year, all the time threat. But certainly, that has implications for elections. And they certainly have preferences that go along with that.

Walter Russell Mead:

And what are the issues that you see the most Chinese influence campaign, most of this malign foreign influence campaign around? You'd mentioned Taiwan. Are there others?

Christopher Wray:

Taiwan, Hong Kong, any calling out of Chinese oppression, of dissidence, human rights, the Uyghurs. China's response to the COVID pandemic, there's a long list of things. In some ways, China's government's own policies and positions and preferences are pretty well known. What's more

pernicious is their more indirect way to try to shape our policy makers on that threat in ways that sometimes our policy makers aren't even aware of.

Walter Russell Mead:

You mentioned some of those in the talk. Can you go beyond that to talk about ways that China seeks to exert this kind of influence?

Christopher Wray:

Well, as a general rule, if you have a question about whether the Chinese use this tactic or that tactic, think of it like a multiple choice question, where the last option is all of the above, and you're usually going to be right. But one of the threats that we're concerned about in particular is what I would call the more indirect, but equally significant, in some ways more significant influence through middlemen. So for example, if you're a governor, a state senator, a mayor, you probably are sophisticated enough to know that when the representative of the Chinese embassy comes in and starts telling you that you got it all wrong about Hong Kong or Taiwan, to at least be a little bit on your guard and take it with a grain of salt.

But what if the person who comes in and talks to you is somebody you've known for 10 or 15 years, maybe a prominent donor to your campaign, or some business that you've had a relationship with in the past, somebody you trust? And that person comes in and says, "Hey, Walter. I think you got it all wrong on this Hong Kong thing. You really should back off. I think you're overplaying your hand." Now if the person came in and said, "Hey, I just had this guy from the Chinese embassy ask me to tell you this," then, sure.

Walter Russell Mead:

Right.

Christopher Wray:

But that's probably not what's happening in most of these instances. And that's where you need to have all the information, so you as the government, mayor, senator, member of Congress, administration official, know what you're dealing with.

Walter Russell Mead:

When it comes to universities, China has a lot of possible points of leverage, from, as you've mentioned, allowing scholars to come visit China, which is necessary for some, to cooperation agreements, but also, I guess we could add student recruitment and so on. Do you see signs that China tries to orchestrate its various sort of instruments here to try to move universities to accept certain things?

Christopher Wray:

Well, certainly they look to try to influence academics. We see that quite frequently. We see them try to recruit academics through things like the thousand talents plan that I described before. We also have things, and I've spoken about this before, that are more sort of soft power, the Confucius Institutes that are in a lot of American colleges and universities, which are efforts to censor or kind of drive China friendly speech in a decidedly unorthodox way here in the US. Now the good news there is that more and more universities are closing those down. So in some ways, that's not as high a priority as a lot of the other things that I described in my speech.

Walter Russell Mead:

And these Confucius Institutes, how kind of do they work?

Christopher Wray:

Well, it's an effort to bring students together to ensure that the Chinese narrative makes its way into and dominates the conversation, if you will, on universities. I could be more specific, but that would take longer to describe.

Walter Russell Mead:

Well, let's get back to some of the business and technology security concerns. Are there particular areas where you see Chinese espionage is really at a very intense level? Do they seem to have priorities here?

Christopher Wray:

Well, as a general rule, China has these five year plans. And they have the made in China 2025 goal that they've articulated, strategy they've articulated. And in general, if you look at the industry sectors that are laid out in those plans, in that strategy, you will see a probably less than coincidental correlation with a lot of the intellectual property theft that I was describing. But it's certainly aviation, healthcare, in the middle of this COVID pandemic. It's not unusual for us to see right after some pharmaceutical company or research institution make some significant announcement about some promising research related to the pandemic, that we'll start seeing cyber activity tracing back to China, targeting with that institution is, sometimes almost the next day. So aviation, healthcare, robotics, but sometimes even agriculture.

I mean, I think that's one thing that a lot of people don't understand. When I mentioned that all 56 of the FBI's field offices have investigations of this sort, that's not because we're just trying to spread the work around. That's because the threat is all over the country. It's in rural areas and big cities. And it's in Fortune 100s all the way down to small startups.

Walter Russell Mead:

Do you have any estimates for how much damage is done to American business by this kind of espionage?

Christopher Wray:

I don't have an exact number. I think people are always trying to come up with a figure. I will tell you that every figure I've seen is breathtaking.

Walter Russell Mead:

So billions, and not just a few billions.

Christopher Wray:

Right. Take just the one case I mentioned in Oklahoma, where you had an individual, that's one guy, stealing $1 billion worth of trade secrets from one company. And then extrapolate that across the thousand or so investigations that I described that are all specifically in the area of Chinese attempted theft of US technology.

Walter Russell Mead:

Is there legislative authority that you don't have, that you would like?

Christopher Wray:

Well, you've probably never met an FBI director that wouldn't welcome more tools. I will say Congress has done a number of valuable things to help us, including for example, not that long ago, they amended CFIUS, which is the legislative scheme, for those who don't know, that deals with acquisitions, foreign acquisitions in the United States. And that's often a place where some of the more sensitive information can be compromised through foreign acquisition. So they've plugged some of the holes that existed in that scheme before, that statutory scheme, and made it more possible for the national security community to appropriately protect American information.

Walter Russell Mead:

Okay. I've got some questions coming in from the audience at this point. One is asking, "How prevalent is the Foxhunt problem within the US and Europe? And could you discuss any other similar tactics the CCP is conducting?"

Christopher Wray:

In terms of the prevalence of the Foxhunt efforts, I think we've seen hundreds just here in the United States, hundreds of you could call them targets, you could call them victims, frankly, hundreds of individuals that the Chinese government is trying to reach and coerce. It also is happening, as I said in my speech, in other countries too. In terms of the tactics, it's a variety of means of coercion. We've had situations where they show up and make comments about their family members back home in China in a way that is pretty unmistakably threatening. If you use your imagination, you're not going to be far off.

Walter Russell Mead:

And have we been working with other governments to try to counter this? Again, from the readers and watchers.

Christopher Wray:

Well, we certainly have worked with a lot of our good foreign partners to compare notes, best practices, and so forth to try to combat the Foxhunt threat. But there's another part of coordination that's important here. I mean, at one level, there is an established means. There are established processes for foreign law enforcement to cooperate with each other, legitimate foreign cooperation happens all the time all over the world. And there's a way you do that, and you coordinate with law enforcement in the country that the person is in. That's not what Foxhunt is. These people are essentially engaged in rogue law enforcement, unsanctioned, uncoordinated with US law enforcement here in the United States. And that really exposes what this is really about, which is suppressing dissent, and trying to pressure dissidents and critics.

Walter Russell Mead:

What can the world's countries do to make this response to Chinese questionable conduct more urgent and more of an actual deterrent to China?

Christopher Wray:

I think the more we can communicate collectively, nations around the world, that we welcome competition. We welcome academic exchange. We welcome travel. But rampant IP theft is not okay. Cyber intrusions into people's personal data, not okay. Economic espionage, not okay. So it's about the behavior. And the more we can communicate that part of participating in a global economy is playing by the rules that other nations play by, adhering to the rule of law and international norms that civilized countries respect, the more hopefully the Chinese government will adjust its behavior and understand that there's a right way to compete and there's a wrong way to compete. But if they keep violating our criminal laws and undermining our national security, they're going to keep encountering the FBI.

Walter Russell Mead:

Another one of the viewers would like to know whether there's some kind of global institutional framework that's needed to fight this IP theft or tech security theft.

Christopher Wray:

Well, certainly, there are ... I think that's being addressed through a variety of means with some improvement. But clearly, a long way to go. Nations working together in a bilateral way, but also multilateral. There are international standard setting bodies, for example, of all shapes and sizes that both we, and to some extent the Chinese, as well as other nations participate in, and nations coming together in those kinds of forums to make clear again that there are rules. And no country I know thinks stealing somebody else's property is okay.

Walter Russell Mead:

Another question. In the recent case of a Chinese national convicted of trespassing on Naval Air Station Key West, the person was found to be working for China's Ministry of Public Security, not the Ministry of State Security of the PLA intelligence. Is the FBI seeing China use the Ministry of Public Security for intelligence operations against the United States?

Christopher Wray:

Well, I mean, I would say that the Foxhunt effort, for example, is more through the MPS than it is the MSS or the PLA. But as a general rule, an awful lot of the kinds of things I was describing in my remarks are more geared towards the MSS and the PLA.

Walter Russell Mead:

I have another viewer who would like to know more about China's interest in agriculture and IP theft there. Can you tell us a little bit more about what some of their targets are and how it works?

Christopher Wray:

So we certainly, the United States, is I think rightly recognized as the world leader in agriculture and in advanced agricultural techniques. And that includes things like genetically modified seeds and different things like that. There's an enormous amount of very sophisticated research and development that happens in the world of agriculture. And we've had cases in the Midwest, we've had cases in places like Kansas, Iowa, Nebraska, where you've had people trying to steal, Chinese actors trying to steal to bring back to China to essentially reverse engineer some of those seeds. It could be rice, corn. We had a case, I can't remember which state it was, not that long ago, where they caught various non state actors working on behalf of the Chinese government, basically digging up seeds into the cover of night to steal

them. We had another one where they were caught at the airport with the seeds in their luggage to try to bring them back.

Walter Russell Mead:

So when you look at the bulk of the cases the FBI has thus far brought against researchers, are most of the violations procedural and false pledges, financial malfeasance? What portion sort of specifically looks at transmission of significant research inside IP? How does that whole universe break down? One of our viewers would like to know.

Christopher Wray:

Well, we will use whatever charges we think are the most readily provable. And in some instances, we will choose to charge a case a certain way to protect sources and methods, for example, because we're trying to take the long view. But certainly, there are a variety of intellectual property theft type charges. But a lot of the charges I described are about concealment at some level. Right? It's not just the underlying theft. It's the concealment of the theft, and that's where things about that include false statement, false tax returns, things like that become important because they're concealing their relationship with the Chinese government from, whether it's American university, an American employer, whoever it happens to be.

At the end of the day, I have high confidence in American companies, American universities, and the American people, if given the right information, to make informed, sensible, patriotic decisions. But when some of these non state actors conceal their relationship with the Chinese government, those employers, the companies, the universities, the people, can't make those informed decisions.

Walter Russell Mead:

You've been talking about a sort of whole of society approach to the problem and the importance of non governmental actors in the US. We have a question here. Does the FBI, DOJ, have resources for private sector entities? Or what would you counsel some of these entities to do?

Christopher Wray:

Well, in all of our FBI field offices, we have established individuals who are entrusted with developing relationships with businesses and universities in their area, private sector coordinators. And that's a new feature over the last 10 or 15 years in the FBI. And it reflects, I think, the degree of partnership that currently is needed and happens between the FBI and the private sector, whether it's again a business or a university. So the resources that we provide, not funding, but it's information. It's know how. It's information about how they can take steps to protect their information technology, their ideas, their innovation. And we have materials we provide. We answer questions and things like that. And I've been to all 56 of the FBI's field offices. And in every single one, I think part of what I've done is met with private sector partners in those states. And you can see the relationship, the partnership that exists today.

Again, I want to be clear. These are institutions. I'm talking private companies, universities that in many ways are making strictly their own ... We're not telling them what to do. They are voluntarily deciding to terminate a relationship to increase their cyber security, whatever it happens to be, to protect themselves, which I think is part of the strength of our system.

Walter Russell Mead:

It's clear that the FBI, DOJ, and other federal entities are stepping up their pressure on this. Are you seeing signs of China changing tactics, or even pulling back a little? Is any of this having an impact on China?

Christopher Wray:

I think it is having an impact. Whether the impact will be the positive impact that we want to have in the long run remains to be seen. Certainly, we've seen China in some ways be less overt about some of their tactics. Open question is to whether that's progress. Are they just hiding it better? Or are they actually pulling back? But I think they are starting to get the message, without getting into some of reasons we know that, that we're not going to tolerate violations of our laws. And that other countries that we work with have similar views.

Walter Russell Mead:

We are coming to a close here. But I wonder if, you spoke a lot in your speech about the need to keep open channels China, not for attacks on the Chinese government, not to bleed over into attacks on Chinese Americans or other things. Anything you would like to add to this? And how can we, what can we do to keep students and other Chinese welcome here, even as all of this is going on?

Christopher Wray:

I mean, the way I look at it, they're targeting our system, our ideas, our innovation. In a way, have you heard the old saying about imitation is the purest form of flattery? They envy the success of our system. And they should envy the success of our system. We're very proud of the freedom and the free market environment that we have here. And so I think it's important to make clear that we're not afraid of competition. We're not afraid of competition over business or ideas. But it's about the behavior. And the behavior is what has to change. It's about the rule of law at the end of the day.

Walter Russell Mead:

All right. Well, thank you very much for joining us today. It's been a terrific session. I've certainly learned a lot. And this emerging US really consensus over how to deal with some aspects of Chinese behavior is I think one of the most striking things that we see, even in a very divided and polarized moment in American life. So Mr. Director, thank you so much for joining us. Hope to see you here again one of these days.

Christopher Wray:

Thanks, Walter. Thanks for having me.