Christopher Wray

Hudson Institute Address on China

delivered 7 July 2020, Washington, D.C.

[AUTHENTICITY CERTIFIED: Text version below transcribed directly from audio]

Well, thank you, Walter. Good morning, everybody. I realize it's challenging, particularly under the current circumstances, to put on an event like this, 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 will 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 just an intelligence issue, or a government problem, or a nuisance largely just for big corporations who can take care of themselves -- you could not 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're 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 few moments, 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 underway across the country, almost half are all 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 it's 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.

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's in a generational fight to surpass our country in economic and technological leadership. Now, that's sobering enough. But it's waging that 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.

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 whole variety of other actors working on their behalf.

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 and stole more than $1 billion -- that's with a "b" -- 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 that Zhang stole.

These cases were among more than a thousand investigations the FBI has into China's actual and attempted theft of American technology -- and that's not even talking about the more than a thousand other 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 1300 percent.

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

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 just a few moments 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 any of 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? Well 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.

But compounding the threat, the data China stole is of obvious value as they attempt to identify people for secret intelligence gathering. On that front, China is using social media platforms -- the same ones Americans use everyday 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 so-called "consulting" services. Sounds benign enough 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 -- 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 ended that way.

It's a troublingly similar story in academia.

Through talent recruitment programs like the Thousand Talents Program I mentioned just a few moments 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're 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 of these guys 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 [National Institutes of Health] 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 dollar monthly stipend, more than 150,000 dollars in living expenses, and more than 1.5 million dollars to establish a laboratory back in China.

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 take one all-too-common illustration: Let's say China gets wind that some 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, of course, be contrary 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. But 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 goes ahead and takes that trip 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 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.

So, to continue with the illustration 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 that official trusts the 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 that 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 will note that the pandemic has unfortunately not stopped any of this. In fact, we've 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 even asked to introduce a resolution supporting China's response to the pandemic.

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

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 some kind of international anti-corruption campaign. It is 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 of China, across the world. We're talking about political rivals, dissidents, and critics seeking to expose China's extensive human rights violations.

Hundreds of these 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 example, 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 [re]turn 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 will 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.

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

Many of the distinctions that mean a lot here in the United States are blurry or almost nonexistent in China -- I'm talking about distinctions between the government and the Chinese Communist Party, between the civilian and military sectors, between the state and the "private" sector.[1]

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 kinds of 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.

Now, 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 also reportedly told employees that Huawei has "entered," -- to quote -- "a state of war." Now, 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 infrastructures 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.

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're not 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 policymakers, 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.

And I will briefly note that we're having real success. With the help of many of our 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.

Now, 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 that 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. And 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 are 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.

[1] Richly styled rhetorical figure that combines anaphora ("between the"), asyndeton (missing conjunction before the final prepositional phrase), and parallelism