Christopher Wray

Address to London Business Leaders on National Security Threats Posed by the People's Republic of China

delivered 6 July 2022, MI5 HQ, London, England

Thank you, Ken. It's an honor to be here this week, talking about common threats our nations face, and the superb cooperation between our two agencies.

The FBI has no closer partner than MI5. We work together on almost every mission our agencies confront -- from countering terrorism to cybertheft and transnational repression to espionage.

Now, you'll notice that there's a common thread running through all the challenges we tackle together, which is that they're all hard.

Our world is certainly filled with enduring, difficult challenges. Not least, Russia's invasion of Ukraine and their ruthless killing of civilians and destruction of homes and infrastructure.

As laser-focused as both our agencies are on the Russia threat, though, I want to talk today about another complex, enduring, and pervasive danger to the kinds of innovative businesses we have here in the audience.

We consistently see that it's the Chinese government that poses the biggest long-term threat to our economic and national security, and by "our," I mean both of our nations, along with our allies in Europe and elsewhere.

And I want to be clear that it's the Chinese government and the Chinese Communist Party that pose the threat we're focused on countering. Not the Chinese people, and certainly not Chinese immigrants in our countries -- who are themselves frequently victims of the Chinese government's lawless aggression.

Now, we understand the appeal of doing business in and with China. Before returning to public service, I spent 12 years in the private sector, advising and representing some of the world's leading companies. And at the FBI, we're engaged with businesses of all sizes and stripes every day, so we understand the perspective of firms looking to the China market, as they try to find and keep a competitive edge.

But the point I want to leave you with today is that the Chinese government poses an even more serious threat to Western businesses than even many sophisticated businesspeople realize. So, I want to encourage you to take the long view as you gauge that threat and as you plan to meet it.

I'll start with what this danger looks like. The Chinese government is set on stealing your technology -- whatever it is that makes your industry tick -- and using it to undercut your business and dominate your market. And they're set on using every tool at their disposal to do it.

For one, they use intelligence officers to target valuable private sector information -- multiplying their efforts by working extensively through scores of "co-optees," people who aren't technically Chinese government officials but assist in intelligence operations, spotting and assessing sources to recruit, providing cover and communications, and helping steal secrets in other ways.

We've seen the regional bureaus of China's MSS -- their Ministry of State Security -- key in specifically on the innovation of certain Western companies it wants to ransack. And I'm talking about companies everywhere from big cities to small towns -- from Fortune 100s to start-ups, folks that focus on everything from aviation, to AI, to pharma. We've even caught people affiliated with Chinese companies out in the U.S. heartland, sneaking into fields to dig up proprietary, genetically modified seeds, which would have cost them nearly a decade and billions in research to develop themselves.

And those efforts pale in comparison to their lavishly resourced hacking program that's bigger than that of every other major country combined.

The Chinese Government sees cyber as the pathway to cheat and steal on a massive scale.

Last spring, for instance, Microsoft disclosed some previously unknown vulnerabilities targeting Microsoft Exchange Server software. Chinese hackers had leveraged these vulnerabilities to install more than 10,000 webshells, or backdoors, on U.S. networks, giving them persistent access to data on those systems. That's just one example of the Chinese government finding and exploiting vulnerabilities, albeit a big one.

But over the last few years, we've seen Chinese state-sponsored hackers relentlessly looking for ways to compromise unpatched network devices and infrastructure. And Chinese

hackers are consistently evolving and adapting their tactics to bypass defenses. They even monitor network defender accounts and then modify their campaign as needed to remain undetected. They merge their customized hacking toolset with publicly available tools native to the network environment -- to obscure their activity by blending into the "noise" and normal activity of a network.

The point being, they're not just big. They're also effective.

But in addition to traditional and cyber-enabled thievery, there are even more insidious tactics they'll use to essentially walk through your front door -- and then rob you. The Chinese government likes to do this by making investments and creating partnerships that position their proxies to steal valuable technology.

To start with, a whole lot of Chinese companies are owned by the Chinese government -- effectively the Chinese Communist Party. And often that ownership is indirect and not advertised. And those that aren't owned outright are effectively beholden to the government all the same, as Chinese companies of any size are required to host a Communist Party cell to keep them in line.

So, when you deal with a Chinese company, know you're also dealing with the Chinese government -- that is, the MSS and the PLA [People's Liberation Army] -- too, almost like silent partners.

But the problem is bigger than that China often disguises its hand in order to obtain influence and access where companies don't suspect it.

Outside of China, their government uses elaborate shell games to disguise its efforts from foreign companies and from government investment-screening programs like CFIUS, America's Committee on Foreign Investment in the U.S.

For example, they're taking advantage of unusual corporate forms like SPACs, or Special Purpose Acquisition Companies, and buying corporate shares with overweight voting rights that let their owners exert control over a company out of proportion with the actual size of their stake in it.

The Chinese government has also shut off much of the data that used to enable effective due diligence, making it much harder for a non-Chinese company to discern if the company it's dealing with is, say, a subsidiary of a Chinese state-owned enterprise.

We're working with MI5 and other partners to identify these types of hidden investments. In the U.S., we've identified and pulled into our CFIUS screening hundreds of concerning transactions that participants failed to notify us about. Within China, you've got all those same problems -- and then some.

You probably all know that the Chinese government requires U.S. and U.K. companies to partner with Chinese businesses, partners that often turn into competitors. But they're also legislating and regulating their way into your IP and your data.

Since 2015, they have passed a series of laws that eat away at the rights and security of companies operating in China. For example, a 2017 law requires that if the Chinese government designates a company as "critical infrastructure," that company must store its data in China -- where, of course, their government has easier access to it.

Another 2017 law would allow them to force Chinese employees in China to assist in Chinese intelligence operations. And a series of laws passed in 2021 centralizes control of data collected in China and gives their government access to and control of that data.

Other new laws give the Chinese government the ability to punish companies operating in China that assist in implementing international sanctions, putting those businesses between a rock and hard place. And one requires companies with China-based equities to report cyber vulnerabilities in their systems, giving Chinese authorities the opportunity to exploit those vulnerabilities before they're publicly known.

If their government could be trusted with that kind of information, that'd be one thing, but we've seen the Chinese government take advantage of its laws and regulations to steal intellectual property and data.

In 2020, for example, we learned that a number of U.S. companies operating in China were being targeted through Chinese government- mandated tax software. To comply with Chinese law, these businesses had to use certain government-sanctioned software. The U.S. companies then discovered that malware was delivered into their networks through this same software. So, by complying with Chinese laws for conducting business in China, they

ended up unwittingly installing backdoors into their systems that enabled hackers' access into what should have been private networks.

This is all just a small sampling, and I could go on.

What makes the Chinese government's strategy so insidious is the way it exploits multiple avenues at once: They identify key technologies needed to dominate markets, like the ones they highlight in their "Made in China 2025" plan. Then, they throw every tool in their arsenal at stealing those technologies -- causing deep, job-destroying damage across a wide range of industries, like when they tried to steal cutting edge jet engine technology, recruiting an insider at GE's joint venture partner to enable access by hackers back in China.

Or in another example, combining human spying with hacking in a joint effort to try to steal COVID research from one of our universities.

So it's long been clear that the danger China poses to businesses is complex and challenging.

Where we see some companies stumble is in thinking that by attending to one, or a couple, of these dangers, they've got the whole Chinese government danger covered -- when really, China just pivots to the remaining door left unattended.

But the danger China poses to companies isn't just complex. It's also getting worse.

That's in part because, as you all know, there's been a lot of discussion about the potential that China may try to forcibly takeover Taiwan. Were that to happen, it would represent one of the most horrific business disruptions the world has ever seen. More on that in a minute.

But it's also because the Chinese government is using intimidation and repression to shape the world to be more accommodating to China's campaign of theft. Examples of the intimidation the Chinese government wields to bend people, companies, and governments to its will could keep us here all day.

But to take just one example, this spring, the Chinese government went so far as directly interfering in a Congressional election in New York, because they did not want the candidate -- a Tiananmen Square protester and critic of the Chinese government -- to be elected.

A former Chinese intelligence officer hired a private investigator to dig up derogatory information and derail the candidate's campaign. When they couldn't find anything, they decided to manufacture a controversy using a sex worker. And when that didn't work out, they even suggested using violence, such as arranging for the candidate to be struck by a vehicle and making it look like an accident.

The Chinese government's crackdown on dissidents crosses borders all over the world, including here in the U.K. In the U.S., they've gone after Chinese-national college students for participating in pro-democracy rallies at U.S. universities or even just for expressing themselves in class.

The FBI battles the Chinese government's transnational repression because it's an evil in its own right and an assault on the freedoms of an open society.

The FBI and MI5 are united in this fight -- from our leadership teams down to our case agents and officers. But this audience should bear in mind that China's repression is also a means to an end -- and we counter it for that reason, too.

Repression is part of how the Chinese government tries to shape the world in its favor, making the world more pliable and susceptible to its nefarious campaign to steal our data and innovation. That connection -- between the Chinese government's ugly repression and its strategic economic goals -- is too little recognized. So, I want to take a few minutes to focus on it.

The Chinese government is trying to shape the world by interfering in our politics (and those of our allies, I should add), like the Congressional example I just mentioned. In other instances, using GPS trackers and other technical surveillance against activists inside the U.S. speaking out against the Chinese government. Even covertly and deceptively running a purported pro-democracy organization to collect information on Americans opposed to them.

But they try to shape the world by going after companies, too -- sometimes just for being associated with people Beijing wants to silence.

Like when, after one U.S.-based employee of a major hotel chain "liked" a social media post by a Tibetan separatist group, the Chinese government made that U.S. hotel chain shut down all of its Chinese websites and applications for a solid week.

Or when an executive with one NBA basketball team appeared to tweet in support of Hong Kong democracy protests, the Chinese government banned all NBA broadcasts in China for an entire year.

Part of that effort is strong-arming companies to do Beijing's bidding and actually help it undermine our political and judicial processes.

Like last November, when the Chinese Embassy warned U.S. companies that, if they want to keep doing business in China, they need to fight bills in our Congress that China doesn't like. That's not something listed in the brochure when you sign up to work with China. And you won't find those types of requirements -- or a warning that you're about to lose your I.P. -- in any contract you might sign.

But if you're considering partnering with a Chinese-owned company, you should ask their Ministry of Commerce: Can they assure you that your employees won't be dragooned into working for their Ministry of State Security and against you? That you won't have to load their tax software or any other state-sanctioned software onto your systems? That your company won't be punished because of one of your employees' tweets?

Their ministry's not going to give you a satisfactory answer -- at least not one that's not belied by the text of the laws on their books or by the way they've actually been treating foreign companies operating there.

All of that is to say -- China poses a far more complex and pervasive threat to businesses than even most sophisticated company leaders realize.

But as I said earlier, I'm not here to tell you to avoid doing business in or with China altogether. Of course, sophisticated Western businesses have long found ways to succeed in tough environments. It's risk versus reward, with a premium on accurately assessing that risk.

But I do have just a few suggestions for those who do plow ahead, because we're not in the business of just articulating problems. We're doing something about them, together -- with MI5, with the private sector itself, with other government partners.

First, I would encourage everyone to work with the two agencies up here. We can arm you with intelligence that bears on just what it is you're facing.

For example, when it comes to the cyber threat, everything from details about how Chinese government hackers are operating to what they're targeting. And when incidents do occur, we can work together -- our agencies and you -- to degrade the threat.

Our folks will race out to give you technical details that will help you lessen the effects of an attack. Together, we can also run joint, sequenced operations that disrupt Chinese government cyber attacks, like we did in that Microsoft Exchange example I noted earlier, working with the private sector, including Microsoft itself, and our government partners to slam shut those backdoors the Chinese government had installed on corporate networks across the U.S.

And we can also help you to ascertain whether the cyber problem you've encountered is actually part of a larger intelligence operation, whether the hackers you do see may be working with insiders, or in concert with other corporate threats, that you don't see.

Finally, I'd ask you to take the long view.

I'm thinking of the view that high-performing boards of directors bring to a company. Looking past the nearest earnings report, to maximizing the value of the company over the course of years, long after today's management team may have moved on. Consider that it may be a lot cheaper to preserve your intellectual property now than to lose your competitive advantage and have to build a new one down the road.

I'd encourage you to keep in mind the complexity of that threat to your innovation I just talked about -- how hard it is to recognize and close every avenue. Maintaining a technological edge may do more to increase a company's value than would partnering with a Chinese company to sell into that huge Chinese market, only to find the Chinese government, and your "partner," stealing and copying your innovation, setting up a Chinese competitor, backed by its government, that is soon undercutting you -- not just in China, but everywhere.

Now, when it comes to the threat against Taiwan I mentioned a minute ago, I'm confident in saying that China is drawing all sorts of lessons from what's happening with Russia and its invasion of Ukraine -- and you should, too.

We've seen China looking for ways to insulate their economy against potential sanctions, trying to cushion themselves from harm if they do anything to draw the ire of the international community. In our world, we call that kind of behavior a clue.

But it's not just Russia that's hurt by what's happened to their economy today as a result of sanctions and disruptions. There were a lot of Western companies that had their fingers still in that door when it slammed shut.

Even a few weeks ago, a Yale study reported in the Wall Street Journal assessed that Western businesses had already lost $59 billion in Russia because of the conflict. The losses grow every day.

And if China does invade Taiwan, we could see the same thing again, at a much larger scale. Just as in Russia, Western investments built over years could become hostages, capital stranded, supply chains and relationships disrupted. Companies are caught between sanctions and Chinese law forbidding compliance with them.

That's not just geopolitics. It's business forecasting.

As I've heard one business leader put it recently, companies need to be wrestling with the strategic risks China poses to their growth in the long-term -- and thinking about what actions they can and should be taking now, to prevent catastrophe later.

I know this all sounds alarming. But while the threat is immense, that doesn't mean harm is inevitable, because while the private sector can't stand alone against the danger -- you're not alone. The FBI and MI5 share a relentless focus on a common mission: protect our countries and keep our people safe.

I spend a lot of my time talking with other leaders focused on national security, both at home in the U.S. and abroad. I know Ken does too. And I'll say the frequency with which this threat dominates the discussion is striking, because our counterparts say they're fighting to protect their students from intimidation, too: that Chinese officials are targeting their policies and candidates with malign influence, too; that hackers in China are carrying their companies' innovation off; that Chinese companies or proxies are using quasi-legal investments to undermine their economies, too.

But the lesson the Chinese government has been unable to learn is that by targeting countries around the world that value the rule of law, they band us even closer together. Beijing may think our adherence to the rule of law is a weakness -- but they're wrong. As rule-of-law agencies in rule-of-law nations with rule-of-law partners, we see how our democratic and legal processes arm us.

We're confronting this threat and winning important battles, not just while adhering to our values -- but by adhering to our values and by continuing to foster close partnerships with all of you. In the process, we're showing why the Chinese government needs to change course -- for all our sakes. All of us in America, in the U.K., and across the free world, are in this together -- and together, we're an awfully formidable team.
