Center for Strategic and International Studies

TRANSCRIPT

China Initiative Conference

"Opening Remarks"

EVENT DATE
Thursday, February 6, 2020

TIME
8:30 a.m. EDT

LOCATION
2nd Floor, CSIS Headquarters, Washington, D.C.

FEATURING
Speaker
Christopher Wray
Director of the Federal Bureau of Investigation (FBI)

CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Transcript By
Superior Transcriptions LLC
www.superiortranscriptions.com

Christopher Wray: Well, thanks, John. And I want to add my thanks to those of others to CSIS for hosting this event and for all you to do educate policymakers and the public.

You've 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 nation's 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, ostensibly 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 for 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 PII; really just about anything that can 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 offices, one of our 56 field offices, the Boston field office, in about a month. So, it 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 depends 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 Americans 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, 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 victimize; 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 hire hacking contractors who do the government's bidding 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 are calculating, they are persistent, they are patient.

The third thing we need to remember about this threat is that China has a fundamentally different system than ours, and they are doing all they can to exploit the openness of ours. Many of the distinctions that we hold dear and that are so ingrained 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, and 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 government's 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 party's 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 academic 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 nontraditional 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 than independent scholarship. We also know that they pressure Chinese students to self-censor 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 are exploiting American companies' openness for foreign investment and partnership, and they are 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 their 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 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 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 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 tradecraft 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 things like economic sanctions, entity listings, visa revocations. We're also working with CFIUS – the Committee on Foreign Investment in the United States – in its review of foreign investments in American companies that produce critical technologies or collect sensitive personal data of U.S. citizens.

But 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 and 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 Grand Universities. Just last October at FBI Headquarters we hosted an academia summit where more than 100 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 benefits 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, 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, 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 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 nation's innovation and ideas.

Thanks for having me here today. (Applause.)

(END)