Reading Materials for Bookwarming

1. Christopher Wray, Responding Effectively to the Chinese Economic Espionage Threat. Feb. 6, 2020.

   ——Page 1-4

2. Andrew Chongseh Kim, Prosecuting Chinese "Spies": An Empirical Analysis of the Economic Espionage Act, Cardozo Law Review, Vol. 40 Issue 2, p749-822. (Dec. 2018).

   Online at: http://cardozolawreview.com/prosecuting-chinese-spies-an-empirical-analysis-of-the-economic-espionage-act/

3. How seed-rustling in Iowa fed American fears of China, The Economist. (Feb. 6th, 2020).

   Online at: https://www.economist.com/books-and-arts/2020/02/06/how-seed-rustling-in-iowa-fed-american-fears-of-china

4. Claude Peck, Review: The Scientist and the Spy, Star Tribune. (Feb. 7, 2020).

   Online at: https://www.startribune.com/review-the-scientist-and-the-spy-by-mara-hvistendahl/567654552/?refresh=true

5. Starred Review: The Scientist and the Spy, Publishers Weekly. (Oct. 29, 2019).

   Online at: https://www.publishersweekly.com/978-0-7352-1428-6

6. Frank Beyer, Starred Review: The Scientist and the Spy, Asian Review of Books. (Feb. 29, 2020).

   Online at: https://asianreviewofbooks.com/content/the-scientist-and-the-spy-a-true-story-of-china-the-fbi-and-industrial-espionage-by-mara-hvistendahl/

Christopher Wray
Director
Federal Bureau of Investigation

Department of Justice China Initiative Conference, Center for Strategic and International Studies
Washington, D.C.
February 6, 2020

Responding Effectively to the Chinese Economic Espionage Threat

Remarks prepared for delivery.

Thanks, Jim. I want to join John Demers in thanking CSIS for hosting this event, and for all you do to educate policymakers and the public. Having been FBI Director for over two years now, I can attest that our nation faces a wider than ever array of challenging threats. But one of them stands out as the greatest long-term threat to our nation's information and intellectual property, and to our economic vitality—and that's the counterintelligence and economic espionage threat from China.

You just heard a pretty sobering presentation from Bill about some of the costs, the impact of that threat. It's a threat to our economic security—and by extension, it's a threat to our national security.

To respond to the China threat more effectively, I believe we need to better understand several key aspects of it. So this morning I want to help further set the table for today's presentations.

A Diverse and Multi-Layered Threat

The first thing we need to understand about the threat from China is how diverse and multi-layered it is—in techniques, in actors, and in targets. China is using a wide range of methods and techniques—everything from cyber intrusions to corrupting trusted insiders. They've even engaged in 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 all working on their behalf.

It's also a diverse threat when it comes to the sectors and sizes of China's targets here in the U.S.—from Fortune 100 companies to Silicon Valley start-ups, and from government and academia to high tech and agriculture. Even as we speak, the FBI has about 1,000 investigations involving China's attempted theft of U.S.-based technology, in all 56 of our field offices, spanning almost 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 information, internal strategy documents, bulk PII—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. And those are all cases investigated by just one of our 56 field offices—Boston—and charged in a little over a month. You'll hear more about some of these cases later this morning.

But to summarize, the Chinese government is taking an all-tools and all-sectors approach—and that demands our own all-tools and all-sectors approach in response.

The Scope of China's Ambitions

The second thing we need to understand about this threat is the scope of China's ambitions, which are no secret. To be clear: This threat is not about the Chinese people as a whole, and certainly 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 and lawful competition, and not by giving their citizens the freedom of thought and speech and creativity 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: "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 American intellectual property 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 victimized—in effect, cheating twice over.

Part of what makes this threat so challenging is that the Chinese are using an expanding set of non-traditional methods—both lawful and unlawful—blending things like foreign investments and corporate acquisitions with 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 that's an understatement. They've made the long view an art form. They're calculating. They're persistent. They're patient.

Exploiting Our Openness

The third thing we need to remember about this threat is that China has a fundamentally different system than ours—and they're doing all they can to exploit our openness. Many of the distinctions that mean a lot here are blurred, if they exist at all, in China: distinctions between the Chinese government and the Chinese Communist Party, distinctions between civilian and military sectors or uses, and distinctions between the state and their business sector.

For one thing, many large Chinese businesses are state-owned enterprises—literally owned by the government, and thus the party. And even where not formally owned, they are legally and practically beholden to the government in a very tangible way. You don't have to take my word for it—you can take theirs. China has national security laws that compel Chinese companies to provide the 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 the companies stay in line with the party's principles and policies. It's hard to even imagine something like that happening in our system.

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 non-traditional collectors of our intellectual property. We know that through their "Thousand Talents Plan" and similar programs, they try to entice scientists at our universities to bring their knowledge to China—even if that means stealing proprietary information or violating export controls or conflict-of-interest policies to do so.

We know they support the establishment of institutes on our campuses that are more concerned with promoting Communist Party ideology than independent scholarship. We know 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 we know 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's crucial that we acknowledge these differences between our two systems—because the Chinese government is doing everything they can to turn those differences to their advantage. Obviously, they're exploiting our open academic environment for research and development. They're exploiting American companies' openness to foreign investment and partnerships. And they're acquiring U.S. firms to gain ownership of what those firms have created.

Meanwhile, they take advantage of their own system being closed. They often require our businesses to put their trade secrets and 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 Communist Party "cells" within their companies. This government control over our joint ventures has become so common that American companies don't always stop to think about it. But if these companies want to protect their information, they sure better think about it.

They should also think 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 it's safely off-limits.

Responding Effectively to the Threat

Understanding the Chinese counterintelligence threat better will help us respond to it more effectively. China is taking a multi-faceted approach, so we've got to have a multi-faceted response. Our folks at the FBI and at 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.

You'll hear more about that in the panels later this morning, but I'll briefly note that we're having real success, real impact. With the help of our many foreign partners, we've arrested targets all over the globe. Our investigations and 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. 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've got a host of tools we can use, from criminal charges and civil injunctions to things like economic sanctions, entity listings, and 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 working together. That's why we in the intelligence and law enforcement communities are working harder to give companies and universities the information they need to make informed decisions and 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 Domestic Security Alliance Council, where we share information with Fortune 1000 companies about China's continued efforts to steal intellectual property. We also have private sector coordinators in each of our 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 them connect to the right people in the FBI, on any concern. Our Office of Private Sector also engages with a variety of academic associations on the China threat, including the American Council on Education, the Association of American Universities, and the Association of Public and Land-Grant Universities.

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 toward 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. And 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 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 the long view in mind when engaging with China.

We're asking executives and boards of directors to carefully consider who they choose to do business with and who they make part of their supply chains. A decision to enter into a joint venture or contract with a particular vendor might look good to them in the near term. It might make a lot of money today; it might sound great on the next earnings call. But it might not look so great a few years down the road, when they find themselves bleeding intellectual property or hemorrhaging 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 them 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. We're going to keep working to build trusted relationships with them, so that they know—with confidence—that we're here to help.

Let me close by making one thing clear: Confronting this threat effectively does not mean we shouldn't do business with the Chinese. It does not mean we shouldn't host Chinese visitors. It does not mean we shouldn't welcome Chinese students or co-exist with China as a country on the world stage. What it does mean is that when China violates our criminal laws and international norms, we're not going to tolerate it, let alone 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.

Resources

- Confronting the China Threat (https://www.fbi.gov/news/stories/wray-addresses-china-threat-at-doj-conference-020620)