JUSTICE NEWS

Assistant Attorney General for National Security John C. Demers Delivers Remarks Regarding Economic Espionage by the People's Republic of China

Washington, DC ~ Thursday, November 1, 2018

Remarks as prepared for delivery

The case unsealed today is representative of the Chinese government's trade secret theft that we see across the country and across industries. Whether by co-opting employees, by computer intrusions or by a combination of both, agents of the Chinese government are systematically stealing our nation's intellectual property for the benefit of their own companies and their own country's strategic priorities. To counter this activity, the Attorney General has launched a nationwide initiative, and I am honored to lead it.

To glimpse the scope of the problem, just look at the recent cases that we've charged. In the case we unsealed today, the defendants are alleged to have misappropriated the intellectual property of an American company and gone to a different company to use this privileged knowledge unlawfully, to clone a product to compete with the American product.

All after the Chinese Central Government and the State Council publicly identified the development of that stolen technology as a national priority and funded a company to mass produce the cloned products. Then to add insult to injury, the company that stole and is working to clone the legitimate American product turned around and sued the American company for violating its patents rights---which were built on the stolen technology.

In addition to the criminal charges, today, for the first time ever, we also bring a civil action to stop the export of the illegal goods and prevent the Chinese company from competing with the American product in America. And we commend the action by the Commerce Department to place the company on the Entity List, which means it won't be able to get the tools it needs to produce this product. As this case shows, we will continue to use all available legal tools to protect American workers and American companies from illegal activity.

Just two days ago, in *United States v. Zhang Zhang-Gui, et al.*, we charged ten defendants, including co-opted company insiders, working for or acting on behalf of the Jiangsu Ministry of State Security, also known as the "JSSD," an arm of the Chinese intelligence services. According to the charging documents from the Southern District of California, the defendants conspired to hack U.S. and European defense and aerospace contractors in order to steal information to develop a Chinese version of a commercial airplane turbofan engine.

Just over three weeks ago, in the Southern District of Ohio, we obtained the extradition of a JSSD intelligence officer who was also alleged to have attempted to co-opt an employee of a defense contractor in order to steal trade secrets related to commercial airplane engines.

In September, in the Northern District of Illinois, we charged an individual here in the United States who acted as a source for a JSSD intelligence officer, helping him, among other things, to assess engineers and scientists for recruitment.

In August, in the Northern District of New York, we charged an individual with stealing turbine technology and sending it to China.

And so it goes.

Taken together, these cases, and many others like them, paint a grim picture of a country bent on stealing its way up the ladder of economic development—and doing so at American expense. This behavior is illegal. It's wrong. It's a threat to our national security. And it must stop.

The National Security Division has a variety of tools available to deal with this problem. First, as we've talked about, we can bring prosecutions. These prosecutions have raised the stakes for intelligence officers and their alleged co-optees here in the United States. If you work at an American company and you help the Chinese steal its trade secrets, we will find you and prosecute you.

These charges, in all their specificity, also prevent China from hiding behind their long practiced, ritualized denials and feigned ignorance.

These charges also serve to educate the American public and alert U.S. business to what the Chinese government is doing on all fronts, including their efforts to target commercial technology pursuant to insiders, computer intrusions, and computer intrusions enabled by insiders.

And most important, through the criminal charges, a civil suit for an injunction, an entity listing and other economic tools, the U.S. government is making a coordinated, concerted effort to deprive the thief of the benefit of his crime.

In addition, when the Chinese use their financial clout to buy or make strategic investments to gain access to American technology and personal data, the National Security Division will work with our partners on the Committee on Foreign Investment in the United States to protect our sensitive technologies and data from national security risk.

And when Chinese activity turns to the malign influence of American politics in order to further its economic and political agenda, we will use the Foreign Agents Registration Act and related criminal and civil tools to ensure full transparency.

China wants the fruits of America's brainpower to harvest the seeds of its desired economic dominance. Preventing this from happening will take all of us, here at the Justice Department, across the U.S. government, and within the private sector. With the Attorney General's initiative, we will confront China's malign behaviors and encourage them to conduct themselves as the leading nation they aspire to be.

Speaker:
John C. Demers, Assistant Attorney General for National Security

Topic(s):
Cyber Crime
Intellectual Property
National Security

Component(s):
National Security Division (NSD)

Updated November 1, 2018