Cyber espionage for the Chinese government

QUANTICO, Va. -- ⋮ 5-7 minutes

Su Bin, a citizen of China and at the time a permanent resident of Canada, is shown at a U.S. border crossing in 2011. (FBI photo)

Cyber espionage for the Chinese government

In August 2014, a Los Angeles grand jury indicted a Chinese national named Su Bin (a.k.a. Stephen Su) for his involvement in a cyber-espionage scheme perpetrated by People's Liberation Army hackers. Bin resided in Canada and was a businessman and entrepreneur who specialized in aviation and aerospace products as the owner of a company named Lode-Tech. As far as the company's place in Air Force contracts, Lode-Tech was a small player, with only a handful of employees that specialized in aircraft cable harnesses.

Bin's influence, however, became farther reaching than perhaps sales suggested. He managed to make close business contacts within the global defense industry community, and used those contacts to gain insight into protected technology and eventually unfettered entry into company files. He even drew the attention of the business community through an article in the *Wall Street Journal* on his business model, products and contacts within the industry.

Between 2008 and 2014, Bin helped two People's Liberation Army hackers steal more than 630,000 files from Boeing related to the C-17 cargo aircraft. The group also targeted data related to the F-22 and F-35 fighter aircraft. Su Bin instructed the hackers on which individuals, companies, and technologies to target, and helped translate the data they obtained from English to Chinese. Bin and his co-conspirators also drafted and distributed reports directly to a department in the PLA's General Staff Headquarters. Such reports specifically identified what they obtained, how they obtained it and its value to their financial benefactors.

An Office of Special Investigations Special Agent consulted with the U.S. Department of Justice and the Federal Bureau of Investigation up until Su Bin's extradition and served as the sole point of contact providing evidence of theft and the valuation of the stolen material. By 2014, the U.S. DOJ had enough evidence to convince the Canadian government to arrest the suspect and consider an extradition request. Although this could have been a complicated process, Su Bin waived his rights to the extradition process and agreed to return to the U.S. to face the charges. OSI led the DoD investigation after the extradition.

OSI Office of Special Projects (PJ) agents played a crucial role in the case. The FBI is responsible for investigating allegations for DOJ prosecutions, but does not have easy access to Defense contractors, nor can they navigate across the various offices and contracts the way OSI PJ can. PJ agents were able to navigate between different contractors, program offices and senior U.S. government officials to gather relevant data to support the extradition, prosecution and sentencing. Agents worked directly with the C-17 program office, Lockheed Martin and other companies to compile the dollar loss to the DoD for information stolen by hackers.

Moreover, PJ agents provided consultation to the U.S. Attorney's Office along every step of the pre-trial process and provided all of the information needed to combat the numerous legal challenges from Bin's legal team. For the case to be closed, agents had to have a clear understanding of the extradition procedures, foreign relations and ensure that the U.S. Government gathered the most relevant information to bring forth in court. Bin and his associates had stolen quite a bit of data from defense contractors, but the prosecution had to select the right data to clearly state a value of the loss to the DoD due to the theft of the information. OSI's PJ agents clearly and successfully assisted the prosecutions efforts from 2014 to Su Bin's sentencing in July 2016.

The case was significant for several reasons. It provided President Barack Obama with a clear-cut and undeniable example of a Chinese national committing cyber-espionage directly on behalf of the Chinese military and government. This case was also an important step in attempting to hold the Chinese government accountable for intellectual property theft that clearly tied back to government officials. This impact cannot be understated as it greatly furthered the U.S. government's national strategy to confront the Chinese president on intellectual property theft and this case laid the groundwork for the U.S. to address these issues in the future.

The unique method of valuing the U.S. Government's losses was precedent setting. Bin's haul included many design plans and maintenance manuals of the Boeing C-17 Globemaster, one of the world's premier heavy lift aircraft. Even though much of the information stolen was not classified, sensitive or export controlled, in aggregate it allowed the Chinese to reverse engineer many aircraft components, thus saving much time and money in research, development and testing phases of technology production.

OSI's PJ agents were instrumental in defining and articulating the rationale used by U.S. attorneys to assign a monetary value lost.