Catching a Chinese IP Thief: How the FBI Tracked and Caught Sinovel

APRIL 5, 2018 | JOSH MAYERS

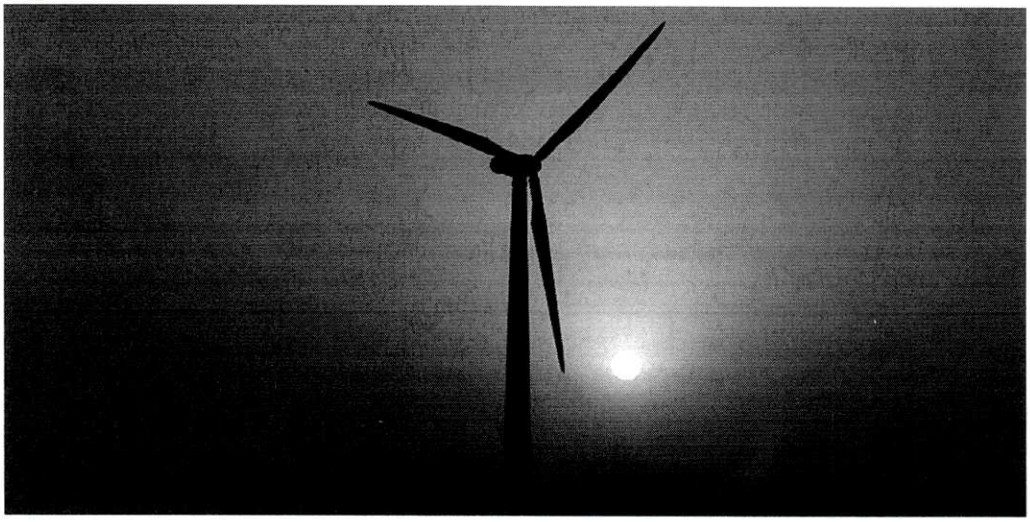

PHOTO: GETTY IMAGES

Resentment, an insatiable appetite for women and an even larger appetite for cash are all elements that led to an insider threat that spelled a devastating theft of U.S. technology by a Chinese company.

But this time, the culprit was caught – or at least, the company behind him was.

On Jan. 24, 2018, after deliberating for less than half a day, a federal jury in Madison, Wisc., found Chinese wind turbine manufacturer Sinovel Wind Group Co. Ltd. guilty on all counts of stealing the software technology of AMSC, a U.S. company.

Sinovel's actions were "nothing short of attempted corporate homicide," in the words of John Vaudreuil, then the U.S. Attorney for the Western District of Wisconsin.

For decades, Chinese firms have gotten away with stealing U.S. technology. What is different about the Sinovel case is that for the first time, a Chinese company has been charged and convicted of crimes in a U.S. federal criminal court.

This victory in court exposes a more difficult problem. Is the U.S. government willing to back the ruling with a meaningful deterrence strategy?

In 2015, President Barack Obama signed an executive order instituting harsh sanctions against countries or individuals found responsible for significant malicious cyber-enabled crimes, including the theft of intellectual property.

President Donald Trump renewed this executive order in 2017, declaring these types of crimes a significant extraordinary threat to the national security, financial stability and economic health of the United States. But no specific action has been taken by the White House to hold China or Sinovel accountable for these crimes, which caused Devens, Mass.-based AMSC to lose approximately $1.2 billion and more than 600 jobs.

The recent trade aluminum and steel sanctions slapped on China by the Trump administration may only be an opening salvo, and a raft of other tariffs have been declared on 1,300 Chinese products including robots and telecommunications equipment (though they won't be implemented until after a public comment period). But none of those actions

highlight the blatant theft of American technology as evidenced in the Sinovel case, nor do they deter China from stealing the product of American hard work and innovation.

AMSC is an energy technology company, founded by four MIT graduates in 1987, initially specializing in superconducting wire. In 2006, it acquired a small wind turbine control system and engineering company named Windtec, located in Klagenfurt, Austria. Their business grew rapidly, and the majority of its work was in developing and selling to customers the complex software of wind turbine control systems.

China-based Sinovel was its biggest customer.

Sinovel aimed to be the world's largest wind turbine manufacturer, and by 2010, the company was well on its way, ranking third. Partially state-owned, it benefitted from lucrative Chinese government contracts and the connections of Sinovel CEO Han Junliang.

These were boom times for the wind energy industry and China was especially motivated to reduce air pollution and the dependence on coal fired plants producing electricity.

But in 2010, Sinovel faced a large and expensive problem. The company needed to quickly retrofit thousands of turbines with new software, in order to meet new Chinese government standards to keep the turbines running and to avoid power outages and brownouts, which were common due to the large and unstable electrical power grid. But it would greatly reduce the company's profits to pay for the retrofit and continue to utilize the licensed software from AMSC, which had developed it.

So according to the government's case as argued in federal court, Han and his Sinovel R&D managers stole it. Han reportedly once told an AMSC executive that he thought software was "like cabbage" – essentially worthless, so why not just take it?

The investigation of Sinovel, an 18% Chinese state-owned enterprise (SOE), dates back to 2010 when AMSC engineers inspecting a Sinovel wind turbine in the Gobi Desert in Northwestern China suspected their proprietary control system software, which operates as the brains of a wind turbine, had been hacked by Sinovel. After AMSC confirmed that Sinovel had likely hacked its software, AMSC took several steps designed to protect itself. They added encryption to the wind turbine control system, and installed a timing limitation in an attempt to ensure Sinovel would continue to pay AMSC for its licensed software.

When AMSC acquired Windtec, it came with a young, smart cadre of engineers in Austria, including a bright and ambitious young Serbian named Dejan Karabasevic, or "DK" as he was called. He'd started at Windtec as an engineering student, and quickly rose to become a senior wind turbine engineer.

DK liked working in the field, sleeping and eating alongside Sinovel engineers in harsh conditions at remote wind farms in China. He was spotted early by Sinovel chief Han as someone who worked hard on behalf of Sinovel. DK was a young man who had a big ego, a penchant for partying and a growing hatred and resentment of his American parent company, AMSC. Han exploited all of that, properly surmising that DK's loyalties were for sale.

Companies can have fences, guards, firewalls, security training, and two-factor authentication to protect their intellectual property. But their employees have to collaborate and work together to be successful. Sinovel used one of the hardest methods to detect to steal ASMC's software: an insider determined to steal its secrets and cause it harm.

Han personally signed DK's $1.7-million-dollar contract in early 2011 – before DK had stopped working for AMSC – with the understanding that DK would steal AMSC's software that Han desperately needed to retrofit thousands of wind turbines.

DK procured the software, removed AMSC's encryption and hacked the

necessary program from an AMSC server in Wisconsin, working from the comfort of a luxurious Sinovel safe house in Beijing. He then sent the stolen AMSC software to Sinovel R&D managers via email.

The simple fact is that enormous economic damage was inflicted on AMSC by Sinovel, including the loss of hundreds of U.S. jobs and over a billion dollars in earnings to the American company AMSC.

This is just one version of a story that has been repeated over and over in the past 20 years, to the accumulating detriment of American workers, companies, and the larger economy. The thefts continue, even with the Sinovel conviction, and despite new tools in the U.S. government's arsenal, such as freezing the assets of companies like Sinovel and its officers, and preventing U.S. persons and entities from doing business with them.

The Sinovel case puts in stark relief the question: why is the U.S. government apparently doing nothing to correct this wrong, and hold Sinovel accountable and most importantly deter China and Chinese businesses from continuing to steal American technology, ideas and innovation?

Josh Mayers served as an FBI Special Agent for 27 years and was the sole agent handling the 7-year long Sinovel–AMSC investigation. Mayers worked most major investigative programs during his FBI career, including deployments to the Middle East and Africa. Mayers earned his B.S. in Criminal Justice from John Jay College of Criminal Justice in New York City, his J.D. from Kent College of Law in Chicago, and is earning a Masters Degree at Boston University, in Criminal Justice/Cybercrime & Cybersecurity.

The views expressed are those of the author and do not necessarily represent the views of the Federal Bureau of Investigation (FBI) or the U.S Government.