**Washington Post (Nov. 15, 2018)**

# America's Overt Payback for China's Covert Espionage

By David Ignatius

**WASHINGTON -- While the bombastic U.S.-China "trade war" has been getting the headlines, U.S. intelligence and law-enforcement agencies have been waging a quieter battle to combat Chinese theft of trade secrets from American companies -- a practice so widespread that even China trade boosters regard it as egregious.**

**The Trump administration's much-ballyhooed campaign of tariffs will eventually produce some version of a truce -- economists say that any other result would amount to a mutual suicide pact. But the battle against Beijing's economic espionage is still accelerating, and it may prove more important over time in leveling the playing field between the two countries.**

**To combat Chinese spying and hacking, U.S. intelligence agencies are increasingly sharing with the *Justice Department revelatory information about Chinese operations. That has led to a string of recent indictments*, and in one case, the arrest abroad of an alleged Chinese spy and his extradition to America to face trial.**

**The indictments don't just charge violations of law, they expose details of Chinese spycraft. And there's a hidden threat: The Chinese must consider whether the U.S. has blown the covers, not just of the people and organizations named in the criminal charges, but others with whom they came in contact.**

**This *law-enforcement approach to counterespionage* requires public disclosure of sensitive information, something that intelligence agencies often resist. But it seems to be an emerging U.S. strategy. The Justice Department has pursued a similar open assault on Russian cyber-espionage, with three recent indictments naming a score of Russian operatives and disclosing their hacking techniques, malware tools and planned targets.**

**China, like Russia, is displaying an increasingly freewheeling and entrepreneurial approach to espionage. Several indictments unsealed since September reveal how the Ministry of State Security, the Chinese spy service, has operated through its regional bureaus -- in this case the Jiangsu provincial office of the MSS -- to obtain precious U.S. technology.**

**The indictments allege that from 2010 to 2015, the Jiangsu branch ran a team of nine hackers who tried to steal U.S. techniques for making jet engines. This is a subtle and highly valuable aspect of aerospace technology, one of the few that China hasn't yet mastered or stolen, and the Chinese evidently wanted to obtain by stealth what they couldn't produce on their own.**

**"The concerted effort to steal, rather than simply purchase, commercially available products should offend every company that invests talent, energy and shareholder money into the development of products," said Adam Braverman, the U.S. attorney in San Diego who helped prosecute the cases.**

**The San Diego indictment lists the hacker names used by the alleged conspirators, handles such as "Cobain," "sxpdlcl," and "mer4en7y." A separate indictment charged an MSS officer named Yanjun Xu, a deputy division director in the Jiangsu bureau, with trying to steal jet-engine secrets from GE Aviation; Xu was arrested last April in Belgium after he began trying to penetrate the company's operations, and he was extradited to the U.S. last**

**month. The U.S. in September arrested a U.S. Army reservist named Ji Chaoqun and charged that he had helped the Chinese gain information about aerospace industry targets.**

**This month, the Justice Department also unsealed a September indictment that accused a Chinese company and its Taiwanese partner, both funded by the Chinese government, of trying to steal eight trade secrets for a memory-chip technology known as "DRAM" from Micron Technology Inc., based in Silicon Valley. The indictment notes that the Chinese government had identified DRAM as "a national economic priority" that Beijing was determined to obtain.**

**The indictment, brought by the U.S. attorney in San Jose, uses blunt language to describe the alleged plot: "In order to develop DRAM technology and production capabilities without investing years of research and development and the expenditure of many millions of dollars," the defendants "conspired to circumvent Micron's restrictions on its proprietary technology."**

**What gives these indictments extra bite is that President Xi Jinping had promised back in 2015 that China wouldn't conduct economic cyberespionage anymore. That pledge followed an indictment the previous year that revealed an elaborate plot by Chinese military hackers to steal U.S. commercial secrets.**

**But in the espionage world, promises not to spy are dubious, at best. Over the last three years, the Justice Department has charged former CIA officer Jerry Chun Shing Lee and five other Americans for stealing secrets on behalf of Beijing.**

**As a rising power, China is also a rising threat in the intelligence sphere. The U.S. counterattack, in part, seems to be a public revelation of just how and why Beijing is stealing America's secrets -- overt payback for covert espionage.**