FAIRBANK CENTER FOR CHINESE STUDIES
HARVARD UNIVERSITY

CGIS SOUTH BUILDING
1730 CAMBRIDGE STREET
CAMBRIDGE, MA 02138
617 495 4046
fairbank.fas.harvard.edu

Critical Issues Confronting China:
Beyond Espionage: IP Theft, Talent Programs, and Cyber Conflict with China

James Mulvenon, SOSi Intelligence Solutions Group

April 22, 2020

Following his 2013 book, "Chinese Industrial Espionage", James Mulvenon, Director of Intelligence Integration for SOS International's Intelligence Solutions Group, is about to publish a sequel to his first full account of the complete range of China's efforts to illicitly acquire foreign technology. For the CICC audience, he explained the continuity and change in Chinese espionage activities over the recent decades. He preferred talking about his observations and conclusions gleaned from specific cases instead of citing those large numbers that some people use to claim the damages caused by Chinese espionage because those numbers can be self-serving.

Having examined numerous cases, he felt that U.S. attorneys tend to be too conservative in bringing such cases to court, despite a dramatic increase in the number of investigations involving intellectual property (IP) theft in recent years. Mulvenon cited a study by the Committee of 100, a non-partisan organization of prominent Chinese-Americans in all fields, of all the cases investigated by the Department of Justice since 2004. It reveals that only 147 cases out of over 1,000 investigations were prosecuted in court, and only in 114 cases where the defendants were convicted. This very low conviction rate is also an indication of our independent judiciary at work. This study also finds that national origin is more pertinent in these cases than ethnicity. The Chinese government has begun in recent years to recruit non-ethnic Chinese in the U.S. to work for them as well.

Mulvenon re-assessed China's apparent economic success from 1978 to 2004, and said that it could not obfuscate the fact that its modernization process thus far was very shallow, as manifested in its lack of indigenous innovation and brand names. The Chinese government then began to promote technological innovations as a strategic goal. It offered direct funding or state subsidies, through bank credit or tax breaks, for companies to acquire advanced technologies around the world. It also encouraged intelligence "collection by other means," which is a euphemism for IP theft. Consequently these activities mushroomed, breaking cyber security laws, and distorting the investment and competition playing field.

Recently the Chinese government has focused more on non-traditional ways of collecting intelligence, including China's various talent programs aimed at attracting talents around the world. "Thousand Talents Program" is the most prestigious one. Under such programs, thousands of researchers with scientific expertise around the world received funding from the Chinese

government. These experts are invited to meetings and tours in China frequently on the government's expense, then return to their home base. Mulvenon viewed the role of these programs as filling in the gap between the fundamental scientific blueprint and the actual physical production of advanced products. Most Chinese engineers, albeit China produces many more engineering graduates than the U.S. each year, don't understand the know-how at the core of some advanced technologies.

Some cases recently investigated by the FBI involve inappropriate behavior, such as lack of adequate disclosure, as well as violating academic rules and standards. For example, some American scientists having received funds from NIH and/or NSF also received funding from the Chinese government for the same research without proper disclosure. Some of them hold professional positions in Chinese universities without correct filing with the U.S. government. The FBI investigated more than 60 such cases and took actions on 16 of them.

Turning to cyber espionage, Mulvenon stated that it has been China's preferred mode of espionage because of the enormous amount of information online as result of the tendency of oversharing and because of all the vulnerabilities associated with human assets. Now with increasing travel restrictions during the Covid-19 pandemic, he expected cyber espionage to be more actively used. He distinguished Chinese cyber strategy from the Russians'. While the Russians tend to be involved in the domestic politics of a foreign country, pitting one party against another, the Chinese tend to use venues of social media to refute criticism of China and cast China in a positive image to foreign audience.

Looking forward, Mulvenon anticipated a very different world after the pandemic. With China's regress of strengthening central planning and state-owned enterprises, state-sponsored research and development, further tilting the playing field in recent years, more and more American business expatriates – presumably the last pillar of pro-China engagement - have left China. The U.S. trade war with China, according to Mulvenon, only accelerated this trend. He expected further diversification of American businesses' global supply chain outside of China, strengthening the enforcement of the Foreign Agent Registration Act in the U.S., more strict export control of technologies with potential dual-use, more scrutiny of Chinese investment in the U.S., as well as student visas to Chinese citizens. He also anticipated Hong Kong to eventually lose its special trade status with the U.S. due to its role in facilitating illicit technology transfer to China.