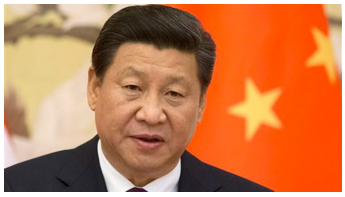
Chinese Spies Engaged in Massive Theft of U.S. Technology

By Bill Gertz (William D. "Bill" Gertz is an American editor, columnist and reporter for The Washington Free Beacon and The Washington Times.)
THE WASHINGTON TIMES
April 12, 2018


Chinese President Xi Jinping

China is engaged in large-scale theft of American research and technology from universities, using spies, students, and researchers as collectors, experts told Congress on Wednesday.

Compounding the technology theft, the administration of President Barack Obama weakened U.S. counterintelligence efforts against foreign spies by curbing national-level counterspy efforts, a former counterintelligence official disclosed during a House hearing.

Michelle Van Cleave, former national counterintelligence executive, said shortly after the creation of the office of the director of national intelligence in 2004, a national counterspy program against foreign spies was restricted during the administration of President George W. Bush.

"Unfortunately, the backsliding continued under President Obama," Van Cleave told two subcommittees of the House Science, Space, and Technology Committee.

Van Cleave said a directive issued by then-DNI James Clapper in 2013 and still in force reduced the national counterintelligence program authority by directing all counterspy programs to be run by individual departments or agencies.

"The national head of counterintelligence was rebranded director of a security and CI center, his duties further dissipated by the fixation on leaks and insider threats driven by the grievous harm done by Snowden, Manning, et al," Van Cleave said, referring to intelligence leakers Edward Snowden, an NSA contractor, and Army Sgt. Bradley Manning.

"Gone was any dedicated strategic [counterintelligence] program, while elite pockets of proactive capabilities died of neglect," she said.

"Read between the lines of existing CI guidance and you will not find a whiff of a national-level effort left, other than caretaker duties such as taking inventory and writing reports."

Several intelligence and security experts testified during the hearing that China poses the most significant threat of technology theft from an estimated $510 billion spent annually on U.S. research and development.

"China has a government-directed, multi-faceted secret program whose primary task is technology acquisition, as well as a highly refined strategy to develop and exploit access to advantageous information through the global telecommunications infrastructure," Van Cleave said.

Along with Russian intelligence agents, Chinese technology spies have developed specific lists of technology for theft. Beijing uses clandestine agents, front companies, and joint research ventures in the theft program.

"Indeed, the United States is a spy's paradise," Van Cleave said. "Our free and open society is tailor-made for clandestine operations."

Michael Wessel, chairman of the congressional U.S.-China Economic Security Review Commission, testified that the Chinese are focused on stealing American advanced technology related to artificial intelligence, robotics, and other cutting edge technology.

Beijing has national-level programs to obtain advanced technologies with both military and commercial applications. They include acquisition of know-how related to new energy vehicles, advanced information technology, biotechnology, new materials, aerospace, ocean engineering, railway systems, robotics, power equipment, and agricultural machinery.

"In the case of robotics and AI, two fields of study with the potential to fundamentally change the international economy as well as the future of war-fighting, China has released the Robotics Industry Development Plan and Next Generation Artificial Intelligence Development Plan with the goals of China assuming global leadership in the coming decades," Wessel said.

China also is infiltrating American universities by funding language and cultural centers called Confucius Institutes that are being used as cover for technology theft. About 100 of the institutes are operating on American campuses and use their funding as part of "soft power" efforts in the United States.

China is also using some of the 350,000 Chinese students in the United States for intelligence work. Chinese spies recruit students with appeals such as "can you help China?" Wessel said.

Recent spy cases have included an electrical engineering professor at the University of Tennessee, John Reese Roth, who in 2008 was convicted of illegally sending defense technology through Chinese students back to China.

In 2009, Ruopeng Lieu, a researcher at Duke University, passed sensitive technology data to China. The information helped Beijing create the Kuang-Chi Science Ltd, a multibillion metamaterials company engaged in wireless internet and mobile payment fields.

In 2015, Chinese professors were among six defendants charged with economic espionage by the Justice Department. An indictment charged stolen American trade secrets were used to assist Chinese universities and state-run companies in China.

Wessel said 20 percent of those working on advanced artificial intelligence at the Berkeley Artificial Intelligence Research Lab are Chinese nationals. Also, 30 of the 38 post-doctorial researchers at the University of Maryland's Bing Nano Research Group are from China, he said.

"While we should continue to work to contribute to the world's efforts to address the most vexing problems facing the world, we must take greater steps to protect the fruits of our work," Wessel said. "Efforts to infiltrate our universities and labs and exfiltrate their work must be a greater priority."

Van Cleave, the former counterintelligence official, said greater efforts are needed to stem the loss of technology to China.

"Counterintelligence—identifying, assessing, and neutralizing foreign intelligence threats—has been little more than an afterthought in U.S. national security strategy, a legacy of neglect that has cost us dearly in lives lost, resources squandered, and dangers unchecked," she said.

Counterspy efforts currently are divided among the FBI, CIA, and Pentagon. The division has created gaps allowing foreign spies to operate in the United States with impunity.

Congress passed the Counterintelligence Enhancement Act in 2002 to fix the problems, but intelligence bureaucracies resisted the reforms and as a result counterspying has been weakened, not improved, Van Cleave said.

"U.S. counterintelligence is finely tuned to work individual cases, but it is not postured globally to detect, deter, or disrupt the intelligence activities of China or any other foreign power, or to execute strategic counterintelligence operations," she said.

"We know surprisingly little about adversary intelligence services relative to the harm they can do."

Van Cleave urged going on the offense against foreign spies by penetrating and disrupting foreign intelligence organizations before they reach the United States.

The goal is to degrade foreign spy services and their ability to conduct operations against the United States.

"We can chase individual spies or technology thieves case by case, or we can target the services that send them here," Van Cleave said. "In short, we can go on offense but national leadership must be willing to direct and empower America's counterintelligence enterprise to carry out that vital mission."

Joel Melstad, a spokesman for the National Counterintelligence and Security Center, did not directly address Van Cleave's criticism. But he said: "Our workforce remains strongly focused on strategic counterintelligence capabilities."

Melstad said that other than the name change, counterintelligence authorities of the director of the National Counterintelligence and Security Center remain the same as those under the 2002 law.

"And while we must respond to demand signals from our government partners concerning important issues like insider threats and leaks, we have not lost sight of the larger strategic CI goal," Melstad said.

The hearing was a joint session of the committee's research and technology subcommittee and oversight subcommittee.

Oversight subcommittee chairman Ralph Abraham (R., La.), told the hearing China is the most aggressive at stealing U.S. technology but the problem involved other foreign nations as well and the activities must be stopped.

"Essentially, China steals our fundamental research and quickly capitalizes by commercializing the technology," he said.

Research and technology subcommittee chairman Rep. Barbara Comstock (R., Va.) said the theft of American technology is a serious problem.

"It is imperative that our academic institutions not close their eyes to the very real threat posed by foreign intelligence spies," she said. "They cannot be blinded by naiveté or ignorance when distinguishing between friend and foe."

This entry was posted in National Security and tagged China. Bookmark the permalink.