Is China spying on American ports?

Port operations only 1 prong of China's espionage in the US

John Paul Hampstead

Wednesday, March 13, 2024

(ZPMC cranes at the Port of Long Beach. Photo: Jim Allen / FreightWaves)

On Feb. 29, the chairman of the House Committee on Homeland Security, Rep. Mark Green, R-Tenn., sent a strongly worded letter to an obscure Chinese equipment manufacturer: Shanghai Zhenhua Heavy Industries Co. (known as "ZPMC"). ZPMC is the world's top producer of ship-to-shore gantry cranes used at container terminals the world over — nearly 80% of the cranes at U.S. ports are ZPMC cranes, and the company has a higher share in Europe.

The subject of Green's letter wasn't a trade dispute of the kind that has erupted between China and the U.S. in the past five years, but something

rather more serious: accusations ZPMC secretly installed communications devices in cranes bound for the U.S. that would enable spying and even remote control (or sabotage) of the cranes.

Green wrote that "cellular modems" were found in the cranes which were completely extraneous to the functioning of the cranes and were not covered in the purchase agreements between U.S. port authorities and ZPMC. Green noted that ZPMC's proximity to elements of the Chinese security and intelligence apparatus — the company's base is adjacent to the Jiangnan Shipyard at Shanghai where China builds warships — could allow the Chinese military to exert undue influence on the manufacture of the cranes. The letter pointed out that because Liu Chengyun is both ZPMC's chairman and president and also serves as the chairman of the company's internal Communist Party committee, there is nothing in ZPMC's corporate governance that would mitigate the Chinese Communist Party's influence at the company.

The letter was not just a one-off missive responding to a headline in the 24-hour news cycle. It was the result of a congressional investigation by the Committee on Homeland Security and the Select Committee on the Strategic Competition between the United States and the Chinese Communist Party (CCP) that began in June 2023. But suspicions about the CCP leveraging maritime infrastructure to spy on the United States have been brewing for years, as the letter makes clear. It was back in 2021 when FBI agents discovered "intelligence gathering equipment" aboard a ship delivering gantry cranes to the Port of Baltimore.

On March 10, ZPMC responded to the letter with a public statement that said while it took the committee's concerns seriously, "The cranes provided by ZPMC do not pose a cybersecurity risk to any ports."

And for its part, the Association of American Port Authorities (AAPA) said in a statement that "there have been no known security breaches as the result of any cranes at U.S. ports, despite alarmist media reports. Further, modern cranes are very fast and sophisticated but even they can't track the origin, destination, or nature of the cargo."

The AAPA did emphasize one fact important to the broader context of the ZPMC cranes and their proliferation. China, the AAPA said, subsidizes the cost of ZPMC's cranes such that they cost about half of what competing cranes sell for, and port authorities have almost no choice but to buy them. The AAPA recommended that the U.S. revitalize its own capacity to manufacture ship-to-shore cranes, writing that "without reshoring our domestic manufacturing capacity, legislative proposals to hastily remove cranes from U.S. ports without immediate replacements would harm U.S. supply chains, jack up prices for everyone, and exacerbate inflation even further."

ZPMC is a wholly owned subsidiary of China Communications Construction Co. (CCCC), a majority state-owned enterprise and one of the main contractors of China's ambitious Belt and Road Initiative. The Belt and Road Initiative is a long-term plan to expand China's sphere of influence through the construction of infrastructure projects around the world, often financed by initially cheap debt that comes with some serious strings attached. A typical project might involve China building a rail, highway or port project in a developing country as well as providing the financing, then seizing ownership of the property if the country defaults on its loan payments. In Tanzania, China demanded a 99-year lease on a port project it built; in Eurasia, China is pressuring Tajikistan to cede more than 400 square miles of territory in exchange for a $1.2 billion debt owed to China — so-called "debt trap diplomacy."

In the case of ZPMC's ship-to-shore cranes, the Chinese government has found other means of inducing partners to install seemingly cheap infrastructure over which China plans to exert an unusual amount of control. The subsidized prices of the cranes can be said to work in the same way as the China-financed infrastructure projects in developing countries — a way to artificially accelerate the penetration of Chinese infrastructure and control.

The CCP has been even more explicit regarding digital surveillance and the worldwide growth of a telecommunications infrastructure controlled and operated by China. The Digital Silk Road, which can be considered a subset of the Belt and Road Initiative, saw China construct 34 terrestrial cables and "dozens of underwater cables" in 12 countries from 2017 to 2022. The development that can be sold to countries as the foundation of a digital infrastructure and the stimulus of a high-tech economy can also be wielded as a weapon in cyberwarfare or simply passively monitored as part of a growing global surveillance network.

Whether ZPMC's cranes in the United States have been or can be used by the Chinese government to spy on and potentially sabotage the United States, the CCP is certainly spying on American ports via multiple vectors, including turning members of the U.S. military. In January, U.S. Navy Petty Officer Wenheng Zhao was sentenced to 27 months in prison for selling military secrets to agents of the Chinese government. And on March 7, a U.S. Army intelligence analyst and soldier, Korbein Schultz, was arrested and charged with conspiracy to obtain and disclose national defense information, exporting technical data related to defense articles without a license, conspiracy to export defense articles without a license, and bribery of a public official. Specifically, the foreign entities paying off Schultz requested information about the U.S. military's plans to defend Taiwan in the event of a Chinese attack.