US indicts Chinese nationals on trumped-up hacking charges

Jacob Crosse
22 July 2020

In an escalation of the bipartisan anti-China campaign, US Department of Justice officials in Spokane, Washington on Tuesday unsealed an indictment against two former engineering students, charging them with hacking in order to steal data on COVID-19 vaccine research.

In the 11-page indictment, Chinese citizens Li Xiaoyu, 34, and Dong Jiazhi, 33, are accused of working on behalf of the Chinese government to hack into the computer systems of US and international companies in order to steal trade secrets, personal information, and information on a potential COVID-19 vaccine.

The indictment states that the two not only worked on their own "for profit," but also at the direction of the Ministry of State Security (MSS), a civilian spy agency, on behalf of the Chinese government.

Each of the two is charged with one count of conspiracy to commit computer fraud, conspiracy to commit theft of trade secrets, conspiracy to commit wire fraud, unauthorized access of a computer and seven counts each of aggravated identity theft.

If convicted on all counts and given maximum sentences, the pair would spend up to 64 years in prison. However, it is extremely unlikely they will ever be extradited to the US.

Li Xiaoyu and Dong Jiazhi, the indictment alleges, are former classmates at the University of Electronic Science and Technology, "an electrical engineering college in Chengdu, China." Li and Dong are accused of using "their technical training to hack the computer networks of a wide variety of companies," beginning in September 2009.

The indictment does not allege that the defendants actually stole any information related to COVID-19 vaccine research. This, however, did not stop the *Washington Post*, CNBC, MSNBC and the *New York Times* from running headlines accusing the two of "stealing vaccine data for China" (the *Times*) or smearing China for "sponsoring criminal hackers targeting coronavirus vaccine research" (the *Post*).

The accusations come less than a week after the intelligence agencies of the US, Canada and the UK accused the Russian government of "plotting to steal" coronavirus research. The *Times* breathlessly promoted the baseless claims of the intelligence agencies on its front page, despite there being no actual evidence or named victims.

It also follows unsubstantiated allegations by FBI Director Christopher Wray and Attorney General William Barr that China has been hacking into US-based companies involved in coronavirus vaccine research.

As the *World Socialist Web Site* explained last week:

> There is a ferocious global struggle between competing corporations and nations to be the first to patent a vaccine for the coronavirus. At stake are billions of dollars for corporate CEOs, investors and bankers, and an immense geopolitical advantage for the country that wins the vaccine sweepstakes…
>
> Under no conditions is US imperialism prepared to allow either Russia or China to dominate the global market for a COVID-19 vaccine. It is seeking in advance to criminalize their efforts, very possibly as a prelude to banning the import of such a vaccine into the US and lesser powers dependent on it, such as the UK and Canada.

The indictment against Li and Dong does not name any companies but does give general locations and singles out industries that were allegedly hacked. The two are accused of compromising the security of various US engineering and technology firms as well as a “Virginia federal and defense contractor.”

The US also accuses the pair of breaking into a British artificial intelligence firm, a Swedish online gaming company, a Lithuanian gaming company, a South Korean shipbuilding and engineering firm, and an Australian solar company.

Li and Dong are alleged to have researched and identified targets through publicly available information. According to the indictment, they were able to gain access using “publicly known software vulnerabilities in popular products.”

In announcing the charges, FBI Deputy Director David Bowdich accused the Chinese government of stealing “intellectual property and research which bolster its economy, and then they use that illicit gain as a weapon to silence any country that would dare challenge their illegal actions.”

John Demers, head of the Justice Department’s National Security Division, ramped up the saber rattling, stating: “China has now taken its place, alongside Russia, Iran and North Korea, in that shameful club of nations that provide a safe haven for cybercriminals in exchange for those criminals being ‘on call’ to work for the benefit of the state, here to feed the Chinese Communist Party’s insatiable hunger for American and other non-Chinese companies’ hard-earned intellectual property, including COVID-19 research.”

The announcement of the charges comes one week after US Secretary of State Mike Pompeo branded nearly all Chinese claims in the South China Sea as “illegal.” Earlier this month, the US sent two aircraft carrier battle strike groups into the South China Sea for war games in the vicinity of Chinese military bases, escalating Washington’s war preparations against the nuclear-armed country.

It should also be noted that earlier this year reports surfaced that for at least five decades the Central Intelligence Agency and the National Security Agency, through a Swiss diplomatic encryption company they owned, have spied on the private communications of world leaders and government officials around the world.