The Washington Post

National Security

In a first, Chinese hackers are arrested at the behest of the U.S. government

By Ellen Nakashima and Adam Goldman October 9

The Chinese government has quietly arrested a handful of hackers at the urging of the U.S. government — an unprecedented step to defuse tensions with Washington at a time when the Obama administration has threatened economic sanctions.

The action came a week or two before President Xi Jinping's state visit to Washington late last month. The hackers had been identified by U.S. officials as having stolen commercial secrets from U.S. firms to be sold or passed along to Chinese state-run companies.

The arrests come amid signs of a potential change in the power balance between the U.S. and Chinese governments on commercial cyberespionage, one of the most fraught issues between the two countries. For years, U.S. firms and officials have said Beijing hasn't done enough to crack down on digital larceny. Experts estimate that Chinese industrial hacking costs U.S. firms tens of billions of dollars annually.

In recent weeks, U.S. intelligence and law enforcement agencies drew up a list of the hackers the United States wanted arrested.

"We need to know that you're serious," was the way one individual familiar with the matter described the message. "So we gave them a list, and we said, 'Look, here's these guys. Round them up.'"

Now, administration officials are watching to see if China will follow through with prosecutions. A public trial is important not only because that would be consistent with established principles of criminal justice, but because it could discourage other would-be hackers and show that the arrests were not an empty gesture.

Administration officials say they are not sure whether the arrests mark a deeper shift in China's stance — or whether they were a short-term move to avoid getting hit by sanctions.

"You'd want to see it sustained over time," said one U.S. official, who, like several others, spoke on the condition of anonymity because of the matter's sensitivity. "And in a situation when there wasn't a major state visit coming up. That will be the proof that the cooperation really is improving."

When Xi arrived in Washington, he pledged his country would not engage in commercial cyberespionage as part of a new broader agreement between the two countries aimed at lessening tensions in cyberspace.

The deal includes a Chinese commitment to provide “timely responses” to requests for assistance from the United States regarding cyberintrusions and cyberattacks. “As we move forward,” the official said, “we will be watching to ensure China’s words are matched by actions.”

China’s Public Security Bureau, which would be the agency with jurisdiction over the arrests, did not respond to a request for comment.

White House and intelligence officials declined to comment on or confirm the arrests, but a senior administration official provided a statement: “As the president has said, we have repeatedly raised our concerns regarding cybersecurity with the Chinese, and we will continue to use all of our engagements to address our concerns directly with the Chinese.”

Catherine Lotrionte, who teaches international law and cyberpolicy at Georgetown University and is a former CIA lawyer, said she had been skeptical that the pact was more than words. But China’s arrests, she said, “makes the U.S. government look much smarter coming into this agreement” with Xi. “You want to see the Chinese do something,” she said. “This would be one of those things that I want to see. It is a good-faith move by the Chinese.”

She too, however, cautioned that there must be follow-through. “You want to watch over the next couple of months for action, for the cessation of attacks,” she said.

It is not clear if the hackers arrested were with the Chinese military, but they were accused of carrying out state-sponsored economic espionage, individuals familiar with the matter said. Commercial espionage is defined as hacking systems to steal intellectual property for the benefit of a country’s own industries. The hacks of U.S. government personnel information, which officials say were carried out by Chinese individuals, fall in a separate category since they do not deal with companies or industry.

The Chinese government arrested several individuals but did not publicize it.

One complication, said a second individual familiar with the case, is that Chinese prosecution would entail the United States sharing evidence linking the cyberintrusions to the individuals. And to do so could compromise sensitive information on how the U.S. government tracked the suspects.

But some U.S. officials said that enough evidence can be shared while still protecting sources and classified techniques. Moreover, they say, federal prosecutors have obtained convictions of criminal hackers in U.S. courts with evidence that ends up in the public domain.

“Cybercases are more sensitive than the average prosecution,” said Lotrionte, who also worked at the Justice Department. “But it’s doable. You just have to be careful about the information that you negotiate to hand over.”

The U.S.-China cyber-agreement announced on Sept. 25 provided that both countries would cooperate "with requests to investigate cybercrimes" and "collect electronic evidence" and to mitigate malicious cyber-activities coming from their territory.

"Particularly now that we have reached this agreement with the Chinese, we should hold them at their word and see what they're willing to do," the U.S. official said. "We have maintained all along that what we want to see is actions."

At a Senate Armed Services Committee hearing last week, Director of National Intelligence James R. Clapper Jr. said that if China does not stick to its pledge and continues to filch U.S. commercial secrets for its own industries' benefit, economic sanctions remain on the table.

The administration was very close to imposing sanctions before the state visit, officials said.

"We are preparing a number of measures that will indicate to the Chinese that this is not just a matter of us being mildly upset but is something that will put significant strains on the bilateral relationship if not resolved," President Obama said in remarks to the Business Roundtable shortly before Xi's visit.

Then, a week before Xi's arrival, the Chinese president sent his special envoy Meng Jianzhu, a member of the political bureau of the Communist Party Central Committee, to Washington to negotiate a deal. The outlines of the agreement were hammered out during the talks, which went through the night, with Secretary of State John F. Kerry, Homeland Security Secretary Jeh Johnson and national security adviser Susan E. Rice.

Sanctions are still very much a possibility, administration officials say.

"No one particular step is going to solve all of our problems" with China over cyberespionage, the U.S. official said. "But seeing evidence that they were taking action based on information that we've passed would be a useful and important step forward."

The arrests were apparently separate from a mass sweep launched by the Chinese government in July in which authorities as of early September had arrested about 15,000 people for alleged cybercrimes, which included hacking, sending spam text messages and online scams. Those arrests were part of a six-month campaign called "Operation Clean Internet," according to a statement from the Ministry of Public Security.

Simon Denyer and Emily Rauhala in Beijing contributed to this report.

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties.

Adam Goldman reports on terrorism and national security for The Washington Post.

Your Three. Videos curated for you.

From clubfoot to clim 6:01

Learn to make traditi 1:19

Sleep advice you wor 1:44

Is f

A f

Kic