Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

China Hacking Revelations Show Limits Of Political Pacts

By **Ben Kochman**

Law360 (January 10, 2019, 8:10 PM EST) -- A new indictment alleging a sweeping campaign by two Chinese government-backed hackers to loot sensitive business data from dozens of American companies is yet more evidence that political agreements between the two countries not to hack each other for economic gain have not gone far enough, attorneys say.

The court papers unsealed Dec. 20 in New York federal court charging Chinese nationals linked to the state ministry of security with hacking more than 45 U.S. technology companies and cloud storage service providers between 2006 and 2018 also add more fuel to the debate over whether indictments truly deter countries like China and Russia that routinely deny having anything to do with such attacks.

Ex-federal officials say that such public attributions will only be successful as part of a broader strategy that the Trump Administration has begun exploring but not yet finalized: describing what makes a cyberattack unacceptable and punishing nations that violate established norms.

"There are more effective means of raising the consequences of hacking American companies than indictments," said David Simon, a partner at Mayer Brown LLP who formerly served as a special counsel at the U.S. Department of Defense. "Depending upon the nature, duration and scope of the cyberattack, it may be appropriate to rely on a variety of tools of national power, including timely attribution, economic sanctions, bilateral and multilateral diplomacy and, as necessary, potentially military capabilities."

The hacks described in the U.S. Department of Justice indictment — which charges the alleged hackers with stealing hundreds of gigabytes of sensitive data from businesses involved in aviation, satellite and communications technologies, among other sectors — appear clearly to breach the terms of a detente reached by former President Barack Obama and Chinese leader Xi Jinping in 2015. Both countries agreed at the time not to target the other's private businesses through cyberattacks for economic gain.

Other evidence in the court papers charges the alleged intruders with activity more tied to traditional intelligence-gathering methods that China, according to U.S. authorities, has increasingly carried out in recent years, including in the notorious 2014 hack on the U.S. Office of Personnel Management and, as confirmed by Secretary of State Mike Pompeo in a television interview last month, in the massive hack into Marriott's reservation database.

December's indictment says that Zhu Hua and Zhang Shilong, members of the so-called Advanced

Persistent Threat 10 group, or APT10, made off with a trove of personal information, including the names, Social Security numbers, dates of birth and other data of more than 100,000 U.S. Navy personnel, and gained access to agencies including NASA and the U.S. Department of Energy.

Drawing a line between traditional spy-versus-spy information gathering and espionage that targets trade secrets or other sensitive data held by private companies is crucial, industry attorneys say, even as evidence mounts that China is not holding up its end of the 2015 bargain on that front. The indictments outlining China's cyberintrusions also come as both countries continue to work on a deal that will solve a bitter trade dispute that has led to both sides hitting roughly $360 billion worth of goods with punitive tariffs.

"We generally try not to involve government in manipulating economic actors," said Guillermo Christensen, a partner in Ice Miller LLP's data privacy and security and white collar defense groups who formerly spent over a decade as an intelligence officer with the CIA.

"We hold fast to the idea that stealing economic secrets, hacking into banks for example, is not what governments should be doing, " he added. "We expect criminals to be doing that."

Unsealing any indictment against rival nation-states carries with it potential benefits as well as its share of risks, former federal officials agreed. While it can be useful to publicly set the tone that certain cyberattacks are not acceptable, indictments also include information that other hackers can use to avoid detection in the future, said Christensen.

"I think that cumulatively it gives a lot of information to the hackers about the mistakes they are making," he said, noting that, while indictments might have a small deterrent effect on hackers afraid of not being able to travel to places where the U.S. has extradition agreements, "the reality is that the Chinese and Russians are not going to change their behavior because of the amount of evidence put in an indictment."

Indicting reputed agents of the Chinese government also carries the risk of prompting China to target U.S. servicemembers, said Jonathan Meyer, a partner at Sheppard Mullin Richter & Hampton LLP who served as deputy general counsel for the U.S. Department of Homeland Security during the Obama administration.

Noting that incentivizing China to stop or slow down its hacking activity without getting into a "tit-for-tat" battle is a "delicate situation," Meyer said that indictments can still be a valuable tool in establishing that the U.S. government is willing to follow up on its public criticism of China's hacking campaigns.

"The point is to send a message. It's important to have a consistency of message, and consistency of activity on this," he said. "It appears that we are seeing a more consistent drumbeat from the U.S. on this issue. If you are going to complain about someone breaking the law, you should take steps to enforce the law through the legal process."

December's indictments and the recent news about the Marriott hack, which according to the company dated back to 2014, come as the Trump administration has said it will form an international "cyber deterrence initiative," something cybersecurity experts in both the public and private sectors have long embraced.

The plan unveiled in September was light on details, but warned that "all instruments of national power

are available to prevent, respond to, and deter malicious cyberactivity against the United States," including but not limited to mounting offensive cyberattacks as well as levying sanctions and filing indictments.

But it's far from clear how U.S. officials might approve an offensive cyberattack. The administration has both eliminated the White House position of cybersecurity coordinator and said that it repealed an Obama-era directive, Presidential Policy Directive 20, that created a multiagency approval process for approving such an attack.

--Additional reporting by Stewart Bishop. Editing by Pamela Wilkinson and Alanna Weissman.