

US looking at action against China cyberattacks

LOLITA C. BALDOR - Associated Press - Associated Press

The Obama administration is considering more assertive action against Beijing to combat a persistent cyber-espionage campaign it believes Chinese hackers are waging against U.S. companies and government agencies.

As The New York Times and Wall Street Journal reported Thursday that their computer systems had been infiltrated by China-based hackers, cybersecurity experts said the U.S. government is eyeing more pointed diplomatic and trade measures.

Two former U.S. officials said the administration is preparing a new National Intelligence Estimate that, when complete, is expected to detail the cyberthreat, particularly from China, as a growing economic problem. Neither of the former officials was authorized to discuss the classified report and spoke only on condition of anonymity.

One of the former officials said the NIE, an assessment prepared by the National Intelligence Council, also will cite more directly a role by the Chinese government in such espionage. The former official said the NIE will underscore the administration's concerns about the threat and will put greater weight on plans for more aggressive action against the Chinese government.

Secretary of State Hillary Rodham Clinton, in an interview with reporters as she wound up her tenure, said the U.S. needs to send a strong message that it will respond to such incidents.

"We have to begin making it clear to the Chinese - they're not the only people hacking us or attempting to hack us - that the United States is going to have to take action to protect not only our government's, but our private sector, from this kind of illegal intrusions. There's a lot that we are working on that will be deployed in the event that we don't get some kind of international effort under way," she said.

"Obviously this can become a very unwelcome and even dangerous tit-for-tat that could be a crescendo of consequences, here at home and around the world, that no one wants to see happen," she said.

Although the administration hasn't yet decided what steps it may take, actions could include threats to cancel certain visas or put major purchases of Chinese goods through national security reviews.

"The U.S. government has started to look seriously at more assertive measures and begun to engage the Chinese on senior levels," said James Lewis, a cybersecurity expert at the Center for Strategic and International Studies. "They realize that this is a major problem in the bilateral relationship that threatens to destabilize U.S."

US looking at action against China cyberattacks

Published on Electronic Component News (<http://www.ecnmag.com>)

relations with China."

To date, extensive discussions between Chinese officials and top U.S. leaders — including President Barack Obama and Defense Secretary Leon Panetta — have had little impact on what government and cybersecurity experts say is escalating and technologically evolving espionage. The Chinese deny such espionage efforts.

Internet search leader Google focused attention on the China threat three years ago by alleging that it had traced a series of hacking attacks to that country. The company said the breaches, which became known as "Operation Aurora," appeared aimed at heisting some of its business secrets, as well as spying on Chinese human rights activists who relied on Google's Gmail service. As many as 20 other U.S. companies were also said to be targeted.

A four-month long cyberattack against The New York Times is the latest in a long string of breaches said to be by China-based hackers into corporate and government computer systems across the United States. The Times attacks, routed through computers at U.S. universities, targeted staff members' email accounts, the Times said, and were likely in retribution for the newspaper's investigation into the wealth amassed by the family of a top Chinese leader.

The Wall Street Journal on Thursday said that its computer systems, too, had been breached by China-based hackers in an effort to monitor the newspaper's coverage of China issues.

Media organizations with bureaus in China have believed for years that their computers, phones and conversations were likely monitored on a fairly regular basis by the Chinese. The Gmail account of an Associated Press staffer was broken into in China in 2010.

Richard Bejtlich, the chief security officer at Mandiant, the firm hired by the Times to investigate the cyberattack, said the breach is consistent with what he routinely sees China-based hacking groups do. But, he said it had a personal aspect to it that became apparent: The hackers got into 53 computers but largely looked at the emails of the reporters working on a particular story. The newspaper's investigation delved into how the relatives and family of Premier Wen Jiabao built a fortune worth over \$2 billion.

"We're starting to see more cases where there is a personal element," Bejtlich said, adding that it gives companies another factor to consider. "It may not just be the institution, but, is there some aspect of your company that would cause someone on the other side to take personal interest in you?"

Journalists are popular targets, particularly in efforts to determine what information reporters have and who may be talking to them.

The Chinese foreign and defense ministries called the Times' allegations baseless, and the Defense Ministry denied any involvement by the military.

US looking at action against China cyberattacks

Published on Electronic Component News (<http://www.ecnmag.com>)

"Chinese law forbids hacking and any other actions that damage Internet security," the Defense Ministry said. "The Chinese military has never supported any hacking activities. Cyberattacks are characterized by being cross-national and anonymous. To accuse the Chinese military of launching cyberattacks without firm evidence is not professional and also groundless."

In a report in November 2011, U.S. intelligence officials for the first time publicly accused China and Russia of systematically stealing American high-tech data for economic gain. And over the past several years, cybersecurity has been one of the key issues raised with allies as part of a broader U.S. effort to strengthen America's defenses and encourage an international policy on accepted practices in cyberspace.

U.S. cybersecurity worries are not about China alone. Administration officials and cybersecurity experts also routinely point to widespread cyberthreats from Iran and Russia, as well as hacker networks across Eastern Europe and South America

The U.S. itself has been named in one of the most prominent cyberattacks — Stuxnet — the computer worm that infiltrated an Iranian nuclear facility, shutting down thousands of centrifuges there in 2010. Reports suggest that Stuxnet was a secret U.S.-Israeli program aimed at destabilizing Iran's atomic energy program, which many Western countries believe is a cover for the development of nuclear weapons.

The White House declined comment on whether it will pursue aggressive action on China.

"The United States has substantial and growing concerns about the threats to U.S. economic and national security posed by cyber intrusions, including the theft of commercial information," said spokesman Caitlin Hayden. "We have repeatedly raised our concerns with senior Chinese officials, including in the military, and we will continue to do so."

Cybersecurity experts have been urging tougher action, suggesting that talking with China has had no effect.

"We need to find new approaches if we want to dissuade this type of activity," said Stewart Baker, former assistant secretary at the Homeland Security Department and now in private law practice with Steptoe and Johnson in Washington. He said the U.S. must do a better job of attributing the cyberattacks to particular groups or nations and "see if we can sanction the people who are actually benefiting from them."

The Obama administration has slowly been ratcheting up its rhetoric. In an unusually strong speech last October, Panetta warned that the U.S. would strike back against cyberattacks, even raising the specter of military action. And the White House has been urging Congress to authorize greater government action to protect infrastructure such as the nation's electric grid and power plants.

US looking at action against China cyberattacks

Published on Electronic Component News (<http://www.ecnmag.com>)

Alan Paller, director of research at SANS Institute, a computer-security organization, said that the level of cyberattacks, including against power companies and critical infrastructure, has shot up in the last seven or eight months. And the U.S. is getting more serious about blocking the attacks, including an initiative by the Defense Department to hire thousands of high-tech experts.

Just talking about it, he said, is having no effect.

Lewis, who has met and worked with Chinese officials on the issue, said their response has been consistent denial that China is involved in the hacking and counter-accusations that the U.S. is guilty of the same things.

"In the next year there will be an effort to figure out a way to engage the Chinese more energetically," he said. "The issue now is how do we get the Chinese to take this more seriously as a potentially major disruption to the relationship."

The answer, he said, is, "You have to back up words with actions, and that's the phase I think we're approaching."

—

Associated Press writers Bradley Klapper in Washington and Michael Lietdke in San Francisco contributed to this report.

Source URL (retrieved on 04/26/2015 - 3:02am):

http://www.ecnmag.com/news/2013/01/us-looking-action-against-china-cyberattacks?qt-most_popular=0