US weighs tougher action over China cyberattacks

February 1 2013, by Lolita C. Baldor

(AP)—High-level talks with the Chinese government to address persistent cyberattacks against U.S. companies and government agencies haven't worked, so officials say the Obama administration is now considering a range of actions.

China-based hackers have long been an economic and national security concern, but as cybersecurity experts report an increase in attacks, U.S. leaders are looking at ways to better address the threat and analyze its impact.

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. One official said it also will cite more directly a role by the Chinese government in such espionage.

The official said the NIE, which reflects the views of the nation's various intelligence agencies, will underscore the administration's concerns about the threat, and will put greater weight on plans for more pointed diplomatic and trade measures against the Chinese government. The two former officials spoke on condition of anonymity because they were not authorized to discuss the classified report.

"We have to begin making it clear to the Chinese," Secretary of State Hillary Rodham Clinton said Thursday, "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."

She said the U.S. must help build an international alliance against the cyberthreat and added that there is a lot the U.S. is working on "in the event that we don't get some kind of international effort under way." She said no specifics have been finalized.

Underscoring that widespread threat, both The New York Times and The Wall Street Journal reported Thursday that their computer systems had been infiltrated by China-based hackers. In both cases they said the focus was on monitoring news coverage and the reporters digging into stories the Chinese government deemed important.

Although the Obama 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. 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.

The newly disclosed four-month long cyberattack against the Times is just 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. Companies ranging from defense and high-tech industry leaders to Internet search leader Google have complained for years of computer network attacks that cybersecurity firms traced back to China, including allegations that some were backed or endorsed by the Beijing government.

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, meanwhile, said its computer systems were 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?"

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

"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."

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.

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.

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.

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."

may not be published, broadcast, rewritten or redistributed.