U.S.: Hackers in Iran responsible for cyberattacks

By Lolita C. Baldor - Associated Press Friday, October 12, 2012

WASHINGTON (AP) — U.S. authorities believe that Iranian-based hackers were responsible for cyberattacks that devastated Persian Gulf oil and gas companies, a former U.S. government official said. Just hours later, Defense Secretary Leon Panetta said the cyberthreat from Iran has grown, and he declared that the Pentagon is prepared to take action if American is threatened by a computer-based assault.

The former official, who is familiar with the investigation, said U.S. authorities believe the cyberattacks were likely supported by the Tehran government and came in retaliation for the latest round of American sanctions against Iran.

Before Panetta's remarks on Thursday, U.S. officials had said nothing publicly about the Gulf attacks or the investigation. But Panetta described them in a speech to business leaders in New York City, saying they were probably the most destructive cyber assault the private sector has seen to date.

Panetta did not directly link Iran to the Gulf attacks, but he said Tehran has "undertaken a concerted effort to use cyberspace to its advantage." And, he said the Pentagon has poured billions into beefing up its ability to identify the origin of a cyberattacks, block them and respond when needed.

"Potential aggressors should be aware that the United States has the capacity to locate them and hold them accountable for actions that harm America or its interests," said Panetta in a speech to the Business Executives for National Security.

A current U.S. official acknowledged Thursday that the Obama administration knows who launched the cyberattacks against the Gulf companies and that it was a state actor.

U.S. agencies have been assisting in the Gulf investigation and concluded that the level of resources needed to conduct the attack showed there was some degree of involvement by a nation state, said the former official. The officials spoke on condition of anonymity because the investigation is classified as secret.

While Panetta chose his words carefully, one cybersecurity expert said the Pentagon chief's message to Iran in the speech was evident.

"It's not something where people are throwing down the gauntlet, but I think Panetta comes pretty close to sending a clear warning (to Iran): We know who it was, maybe you want to think twice before you do it again," said cybersecurity expert James Lewis, who is with the Center for Strategic and International Studies. "I think the Iranians will put two and two together and realize he's sending them a message."

He said Panetta's remarks were an important step by the U.S. because the Iranian cyberthreat "is a new dimension in 30 years of intermittent conflict with Iran for which we are ill-prepared. It's really important to put them on notice."

The cyberattacks hit the Saudi Arabian state oil company Aramco and Qatari natural gas producer RasGas using a virus, known as Shamoon, which can spread through networked computers and ultimately wipes out files by overwriting them.

Senior defense officials said the information was declassified so that Panetta could make the public remarks. The officials added that the Pentagon is particularly concerned about the growing Iranian cyber capabilities, as well as the often discussed threats from China and Russia. The two officials spoke on condition of anonymity because they were not authorized to discuss the cyberthreats publicly.

In his speech, Panetta said the Shamoon virus replaced crucial system files at Aramco with the image of a burning U.S. flag, and also overwrote all data on the machine, rendering more than 30,000

computers useless and forcing them to be replaced. He said the Qatar attack was similar.

Panetta offered no new details on the Pentagon's growing cyber capabilities or the military rules of engagement the department is developing to guide its use of computer-based attacks when the U.S. is threatened.

He said the department is investing more than $3 billion a year in cybersecurity to beef up its ability to defend against and counter cyberthreats, including investment in U.S. Cyber Command. And the Pentagon is honing its policies so that any actions comply with the law of armed conflict.

"Our mission is to defend the nation. We defend. We deter. And if called upon, we take decisive action to protect our citizens," he said.

He added, however, that the Defense Department will not monitor American citizen's personal computers, or provide for the day-to-day security of private or commercial networks.

Panetta used the Persian Gulf attacks in his remarks as a warning to business community that it must embrace stalled legislation that would encourage companies to meet certain cybersecurity standards. And he is endorsing a planned move by President Barack Obama to use his executive powers to put some of those programs, including voluntary standards, in place until Congress acts.

"These attacks mark a significant escalation of the cyber threat," Panetta said. "And they have renewed concerns about still more destructive scenarios that could unfold."

U.S. authorities have repeatedly warned that foreign Internet hackers are probing U.S. critical infrastructure networks, including those that control utility plants, transportation systems and financial networks.

"We know of specific instances where intruders have successfully gained access to these control systems," Panetta told the business group. "We also know that they are seeking to create advanced tools to attack these systems and cause panic and destruction, and even the loss of life."

Business leaders, including the U.S. Chamber of Commerce, opposed the legislations, arguing it would expand the federal government's regulatory authority over companies already struggling in the tough economy. The bill also encourages more information sharing between the government and private companies.

Panetta pressed the group to support the stronger cybersecurity measures, warning that failure to do so could have catastrophic consequences.

"Before September 11, 2001 the warning signs were there. We weren't organized. We weren't ready. And we suffered terribly for that lack of attention," said Panetta. "We cannot let that happen again. This is a pre-9/11 moment."