US thinks Iran behind cyberattack in Saudi: ex-official

October 13 2012, by Dan De Luce

This file photo shows visitors passing by the stand of Saudi Arabia's national oil company Aramco at the Abu Dhabi International Petroleum Exhibition, in 2008. The US believes Iran was behind a major cyberattack on Aramco and a Qatari gas firm, a former US official who has worked on cybersecurity issues said on Friday.

The United States believes Iran was behind a major cyberattack on Saudi Arabia's state oil company and a Qatari gas firm, a former US official who has worked on cybersecurity issues said.

In a major cybersecurity speech on Thursday, Defense Secretary Leon Panetta issued a veiled warning to Tehran that Washington is ready to take preemptive action to protect US computer networks, the former official said.

US government agencies have concluded that Iran orchestrated the "shamoon" virus that disabled tens of thousands of computers at Saudi Aramco and struck Qatari natural gas firm RasGas as well, said James Lewis, who has worked for the State Department and other government agencies on national security and cyber issues.

American officials had "more than a suspicion" that Iran was to blame for the August attacks, that also possibly included recent denial of service attacks on some US banks, said Lewis, a senior fellow at the Center for Strategic and International Studies think tank.

"There's generally a conviction that it was Iran," he told AFP.

Lewis said he was not privy to the intelligence reports that backed up the assertion, but said it was implausible the Iranian government would not be aware of a major cyber operation coming from sources inside the country.

"How could you do something that consumed a massive amount of bandwidth in Iran and not have the government notice, when it's monitoring the Internet for political purposes?" he asked.

US government officials had concluded that Iran likely launched the attack in retaliation for US-led sanctions over its nuclear program and a cyber sabotage campaign reportedly backed by Washington, he said.

A senior administration official, who spoke on condition of anonymity, told AFP the cyberattack on the Gulf oil giants was believed to be carried out by a "state actor" and acknowledged that Iran would be a prime suspect.

In his speech, Panetta referred to the "shamoon" virus for the first time publicly, saying it erased critical files on about 30,000 computers at

Saudi Aramco, the world's largest oil company.

He said the virus, which hit Qatar's Rasgas a few days later, was "probably the most destructive attack that the private sector has seen to date."

The Pentagon chief also spoke of "foreign actors" probing sensitive US networks and cited denial of service attacks on some large US financial companies in recent weeks.

While he reiterated US concerns about cyber threats linked to Russia and China, Panetta said Iran was building up its digital capabilities.

In the same speech to business executives in New York, Panetta said the United States had improved its ability to track the origin of digital attacks and suggested the military stood ready to take preemptive action in cyberspace to protect vital networks.

"He came as close to fingering Iran for some of the disruptions we've seen in the last month as you could do without actually saying it by name," said Lewis, who has advised the US government on cyber security.

"Hopefully, the Iranians picked it up as a warning."

Iran has advanced its digital warfare capacity faster than US officials had anticipated, Lewis said, though the attack on Saudi Aramco was relatively unsophisticated.

"We're used to China, we're used to Russia. But Iran is new, Iran is different. And a lot of people didn't think it would develop this quickly," he said.

US officials said information about the recent cyberattacks was declassified to allow Panetta to refer to the incidents in his speech.

The "shamoon" virus wiped out crucial files and replaced them with images of burning American flags.

Two weeks after the August 15th cyberattack on Saudi Aramco, the company announced it had restored its main internal network and that the assault had not disrupted oil production.

The firm targeted in Qatar, RasGas, is a joint venture between American oil firm Exxon Mobil Corp and state-controlled Qatar Petroleum.