http://online.wsj.com/article/SB10000872396390444657804578052931555576700.html

Iran Blamed for Cyberattacks

U.S. Officials Say Iranian Hackers Behind Electronic Assaults on U.S. Banks, Foreign Energy Firms

By SIOBHAN GORMAN And JULIAN E. BARNES

10/12/2012

WASHINGTON—Iranian hackers with government ties have mounted cyberattacks against American targets in recent months, escalating a low-grade cyberwar, U.S. officials say.

The Iranian effort culminated in a series of recent attacks against U.S. banks as well as electronic assaults this year on energy companies in the Persian Gulf. The attacks bore "signatures" that allowed U.S. investigators to trace them to the Iranian government, the officials said.

The hackers appear to be a network of fewer than 100 Iranian computer-security specialists at universities and network security companies in Iran, investigators said.

Iranian officials didn't return a call seeking comment.

- **Iran Promises Flexibility in Talks**

U.S. officials said detailed evidence linking the attacks to Tehran is classified. But Iranian hackers don't have the resources to mount major attacks without the support and technical expertise of the government, the officials said.

"These are not ordinary Iranians," one senior U.S. official said.

Defense Secretary Leon Panetta alluded to the Iranian cyberattacks in a policy announcement this week on U.S. efforts to counter the threat. He didn't directly finger Iran in these attacks, but said they mark "a significant escalation." Mr. Panetta, in an address in New York, outlined procedures being put into place to block such attacks, identify attackers and retaliate, if necessary.

A Litany of High-Tech Assaults

Incidents have escalated in recent months.

- January 2012: Potent but smaller-scale denial-of-service attacks against U.S. banks.
- July 2012: Cyberattack at Saudi Arabian Oil Co. unleashes a virus called 'Shamoon,' destroying data on 30,000 computers.
- August 2012: Cyberattack at Rasgas, a Qatari natural gas company, disabled websites and email system.
- September 2012: A group called "Qassam Cyber Fighters" announced plans for cyberattacks on U.S. banks. Powerful denial of service strikes hit Bank of America Corp, J.P. Morgan Chase & Co., U.S. Bancorp, PNC Financial Services Corp. and Wells Fargo & Co.
- October 2012: The Qassam Cyber Fighters issued announcements, followed by cyber strikes, involving other U.S. banks, slowing or interrupting consumer websites

WFC -2.64%"They have been going after everyone—financial services, Wall Street," said a senior defense official. "Is there a cyberwar going on? It depends on how you define 'war.'"

The attacks against U.S. banks were so-called denial of service attacks, in which computers are programmed to bombard a particular website and knock it off line. But investigators fear that they represent a first step to more destructive electronic assaults, which already had been mounted on a Saudi oil company.

The attacks began early this year in what some officials surmised was retaliation for harsh sanctions on Iran's oil and financial sectors, imposed as part of an effort by the U.S. and its allies to halt Tehran's nuclear program. Tehran denies Western charges that it is seeking to use the nuclear program to develop atomic weapons.

The Iranian effort may also be payback for a high-tech campaign against Iran that involved the U.S., including the cybersabotage project known as Stuxnet. That project targeted Iran's Natanz nuclear plant with cyberattacks that caused a large proportion of its centrifuges to spin out of control beginning in 2008.

U.S. officials have long considered Iran as a second-tier cyberpower, behind China, Russia, France, Israel and the United States. They now are debating the extent to which Iran has the capability to damage the financial system and other U.S. infrastructure.

Iran has stepped up its cyber capabilities in recent years, spending at least $1 billion on them since the beginning of this year, said Ilan Berman, a Middle East expert at the American Foreign Policy Council. The Pentagon spends about $3 billion a year on cyberdefenses.

Iran's strategy has shifted from fortifying its cyberdefenses to developing offensive cyberweapons, said Mr. Berman.

Defense officials see the cyberattacks as part of a larger effort by Iran. U.S. investigators allege Iran was behind an attack in July on Israeli tourists in Bulgaria, the killing of a Saudi diplomat in May in Pakistan, and the attempted assassination last year of the Saudi ambassador in Washington. Iran has denied involvement in all the incidents.

U.S. banks were the first targets of attacks that were comparatively small in scale, according to former U.S. officials.

The attacks expanded to oil and gas companies in the Persian Gulf and Middle East over the summer, then returned to U.S. banks with far more potent attacks in recent weeks.

Three more banks were hit this week, and each of those actions was preceded by an Internet warning of an imminent attack.

"In the last year, there's been a cyberwar going on in the Middle East, and it's spilled over now" into America, a former U.S. official said.

The attacks began shortly after approval last December of a U.S. defense bill that stepped up punitive sanctions. Iranian hackers initially mounted potent, but smaller-scale denial of service attacks on a group of U.S. banks in January, investigators say. The attackers were testing the banks' responses to each assault and adjusting their tactics to penetrate banks' defenses.

The Tel Aviv Stock Exchange and the website of Israeli airline El Al also came under attack that month, each suffering website outages. Although an unknown hacker who claimed to be a Saudi took credit, investigators are examining a possible Iranian role. The stock exchange and airline acknowledged the attack at the time and said they quickly recovered from it.

The Iranian hackers re-emerged in July with an attack on the Saudi Arabian Oil Co., known as Saudi Aramco, investigators believe. That attack, wielding a virus called "Shamoon," destroyed data on 30,000 computers. A group calling itself "Cutting Sword of Justice" claimed responsibility for the attack, which U.S. investigators believe was tied to Iran.

Aramco acknowledged then that its computers had been taken down by an electronic attack and said it expected more attacks in the future. It said that it quickly recovered.

The Aramco attacks set off alarms within the U.S. government as a shift in tactics from stealing information to destroying it.

In August, the target was Rasgas, a Qatari natural gas company that is a leading global provider of liquefied natural gas. The attack, which U.S. officials believe was carried out by the same Iranian network, shut down its website and internal email servers. Rasgas also acknowledged the attack and said it had no impact on operations.

In September, the group redoubled its attacks on the U.S. financial sector. It announced its plans in advance under the moniker "Qassam Cyber Fighters," a previously unknown group.

On Sept. 18, the group announced it would target Bank of America Corp. It followed with several more attacks, including J.P. Morgan Chase & Co., U.S. Bancorp, PNC Financial Services Corp., and Wells Fargo & Co.

This past week, the pre-announced attacks continued with Capital One Financial Corp., COF -1.15%SunTrust Banks Inc., STI -3.38%and Regions Financial Corp. RF -4.46%Following the announcements, the attacks bombarded computers that run bank websites, slowing website performance of some and taking others offline temporarily.

Bank of America declined to comment and J.P. Morgan wouldn't confirm an attack but acknowledged some customers had difficulty accessing its website. PNC's president wrote an open letter to customers about the attacks, which lasted about 31 hours. Wells Fargo and U.S. Bancorp also acknowledged they had been hit.

With this week's attacks, a Capital One spokeswoman said that some customers were intermittently unable to log on to their accounts on Oct. 9 due to a large volume of traffic. A SunTrust spokesman said the company experienced increased traffic Oct. 10 that led to service outages. A Regions spokesman said the company experienced intermittent Internet service disruption on Oct. 11.