Cyber war targets Middle East oil companies

October 22 2012, by Patrick Rahir

A flame from a Saudi Aramco oil installion is seen near the oil-rich area of Khouris, Saudi Arabia, in 2008. Middle Eastern oil and gas companies have been targeted in massive attacks on their computer networks in an increasingly open cyber war where a new virus was discovered just this past week.

Middle Eastern oil and gas companies have been targeted in massive attacks on their computer networks in an increasingly open cyber war where a new virus was discovered just this past week.

The United States and Israel, believed to behind the first cyber sabotage campaign that targeted Iran's nuclear programme, are now worried about

becoming targeted themselves.

"There have been increasing efforts to carry out cyberattacks on Israel's computer infrastructure," Prime Minister Benjamin Netanyahu said earlier this month, without giving details.

Netanyahu spoke just days after Washington issued a veiled warning to Iran over digital attacks and outlined a new digital warfare doctrine.

US Defense Secretary Leon Panetta also referred publicly for the first time about the "Shamoon" virus that hit Saudi Arabia's state oil company Aramco in August, disabling more than 300,000 computers.

The virus also hit Rasgas, a joint venture between US oil firm Exxon Mobil Corp and state-controlled Qatar Petroleum.

Panetta called the sophisticated virus "the most destructive attack that the private sector has seen to date."

It took Aramco, the world's biggest oil company, two weeks after the August 15 attack to restore its main internal network, but the group said that oil production had not been disrupted.

However the threat that digital attacks could cripple vital infrastructure is real, with Panetta warning of the possibility of a "cyber-Pearl Harbor" to justify a policy of moving aggressively against threats.

A disruption to Saudi Arabia's oil exports could cause oil prices to spike from their already elevated prices and tip the fragile global economy into recession.

In what was interpreted as a veiled threat against Iran, Panetta said the US military "has developed the capability to conduct effective

operations to counter (cyber) threats to our national interests."

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

US officials have "more than a suspicion" that Iran was to blame for the August attacks, said James Lewis, who has worked for the State Department and other government agencies on national security and cyber issues and who is now a senior fellow at the Center for Strategic and International Studies think tank.

He said the US authorities were used to cyber espionage from Russia and China, but were surprised by the swift rise in Iran's digital warfare capability.

"A lot of people didn't think it would develop this quickly," he said.

However it is unsurprising that Iran would seek a cyber warfare capability after having hundreds of centrifuges used to enrich uranium ruined by the Stuxnet virus in 2010.

Stuxnet marked a transformation for computer viruses, which had previously been used for spying or by organised crime, into a tool for sabotage.

It is widely suspected to have been the work of the United States and Israel, which believe Iran's nuclear programme aims to produce a bomb.

Tehran insists its nuclear programme is for peaceful uses only.

Iran has been victim of other digital attacks as well.

In April it was forced to unplug computers at its Kharg oil terminal from the Internet after they came under cyber attack, and in November last year an explosion at a missile terminal was attributed by US media to a computer virus.

—Only 'scratched the surface' of cyber warfare in Middle East—

Kaspersky Labs, which detected the "Flame" and "Gauss" viruses believed behind those attacks, announced Monday it had found a new cyber espionage weapon it dubbed "miniFlame".

It described the virus as "a high precision, surgical attack tool ... designed to steal data and control infected systems during targeted cyber espionage operations."

Kaspersky said "we have only just scratched the surface of the massive cyber espionage operations ongoing in the Middle East. Their full purpose remains obscure and the identity of the victims and the attackers remains unknown."

Christian Harbulot, the head of the Economic Warfare School in Paris, warned that "it is extremely difficult to undo the knot" in what is also a propaganda war.

He said Iran could be behind the "Shamoon" virus, but that "it could be an additional pretext to weaken Iran" which is already under international embargo over its nuclear programme.

For Nicolas Arpagian at France's National Institute of Advanced Security and Justice Studies, the latest attacks "show that arsenal of digital weapons is getting bigger, and that when you have such an arsenal the use of cyberweapons is bound to become more commonplace."

(c) 2012 AFP