THE SABOTAGE ATTACK ON THE SYRIAN COALITION

The NYT reports — adding to an earlier WaPo story — that hackers have attempted to sabotage a bunch of US energy companies.

> A new wave of cyberattacks is striking American corporations, prompting warnings from federal officials, including a vague one issued last week by the Department of Homeland Security. This time, officials say, the attackers' aim is not espionage but sabotage, and the source seems to be somewhere in the Middle East.

It ties these attacks to earlier attacks, claimed to have been launched by Iran, against ARAMCO and Qatar's RasGas.

> Two senior officials who have been briefed on the new intrusions say they were aimed largely at the administrative systems of about 10 major American energy firms, which they would not name. That is similar to what happened to Saudi Aramco, where a computer virus wiped data from office computers, but never succeeded in making the leap to the industrial control systems that run oil production.
>
> [snip]
>
> At Saudi Aramco, the virus replaced company data on thousands of computers with an image of a burning American flag. The attack prompted the defense secretary at the time, Leon E. Panetta, to warn of an impending "cyber 9/11" if the United States did not respond more efficiently to attacks. American officials have since concluded the

> attack and a subsequent one at RasGas, the Qatari energy company, were the work of Iranian hackers. Israeli officials, who follow Iran closely, said in interviews this month that they thought the attacks were the work of Iran's new "cybercorps," organized after the cyberattacks that affected their nuclear facilities.
>
> Saudi Aramco said that while the attackers had attempted to penetrate its oil production systems, they had failed because the company maintained a separation between employees' administrative computers and the computers used to control and monitor production. RasGas said the attack on its computers had failed for the same reason.

And while the adoption of earlier sabotage approach used with ARAMCO and RasGas infrastructure to US energy producers does not mean all members of the coalition to topple Bashar al-Assad have been attacked by an entity insinuated to be Iran (unless the European parters' energy companies have been attacked and we just don't know about it). But this attack does seem to be an assault on the coalition trying to undercut Iran by taking down its client regime in Syria.

Which has me wondering whether this is an Iranian attack — revenge, if you will, for StuxNet, serves the US right. Or if it's an attack launched by a coalition, possibly including Russia.

I also wonder whether the point of the sabotage isn't on the information side of the equation, rather than the operational one.

In other news, remember how former NSA head and all-around cyberwar profiteer Mike McConnell declared digital 9/11 warning based on the ARAMCO attack and some crude DNS attacks on

banks here in the US? Guess who has become a player in Saudi (and Gulf generally) cybersecurity?

> During this event, Booz Allen Hamilton leadership shared their insights on global cyber security practices and the importance of a cross-border cooperative approach to protecting critical infrastructure in the Gulf.
>
> Commenting at the event, McConnell said, "The GCC states have become global hubs in finance. However, this growth introduces increased cyber security risks by threat actors who target this region for monetary or political gain. GCC states have already experienced significant cybercrime in the recent past, it is now more important than ever to ensure that these are not repeated."
>
> He also added, "Financial institutions are a prime target for cyber criminals, and as a result, they need to focus on staying ahead of cyber threats by developing the right human capital, developing appropriate training programmes and retaining the right skills and technology to properly access and protect corporate data."
>
> **Booz Allen Hamilton was recently registered by the Kingdom of Saudi Arabia Ministry of Commerce and Industry to pursue business opportunities in the Kingdom in support of domestic economic diversification**. The firm will provide services to government and commercial clients on critical issues related to the Kingdom's development, most notably in the areas of cyber security, information technology, financial services and other selected infrastructure. [my emphasis]

I’m guessing BAH’s work in KSA has a lot to do with the expanded Technical Cooperation Agreement signed with the US in January, which added a cyber component onto the previous effort to create a 35,000 person security force Mohammed bin Nayef could use to protect the kingdom’s oil infrastructure.

So if you’re bummed that BAH gets to troll American networks with abandon, rest assured that it will now be doing so in Saudi Arabia, too.