Saudi-Iranian confrontation moves to cyberspace

Jareer Elass

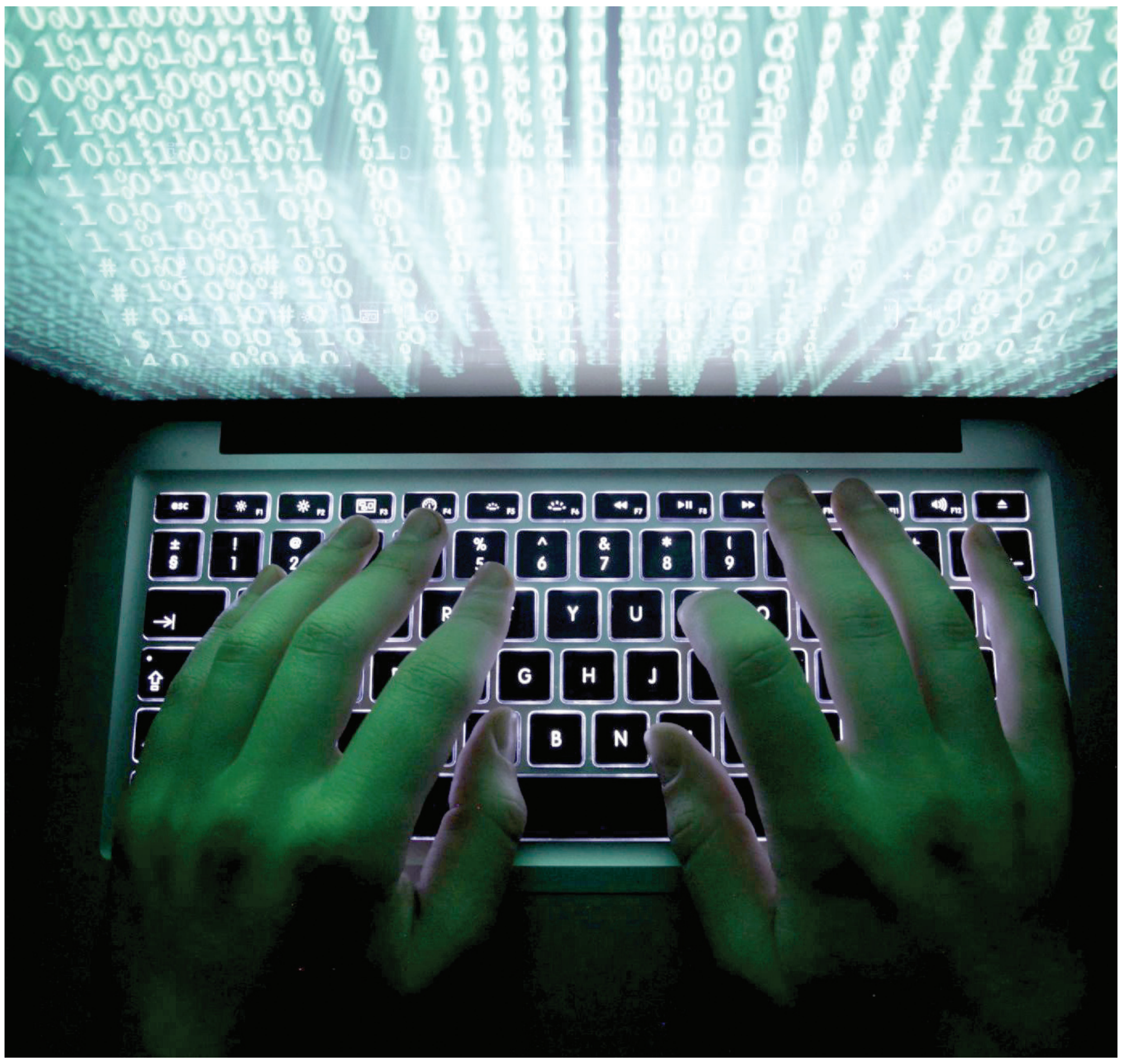
Washington

Geopolitical and ideological rivals Iran and Saudi Arabia have been engaged for several years in proxy wars in Yemen and Syria as the two countries vie for regional supremacy.

Now Tehran appears to be masterminding another form of warfare against Riyadh by supporting periodic state-sponsored cyber-strikes that are exposing strategic vulnerabilities of the kingdom. A recent cyber-attack disrupted the Saudi aviation sector.

There is growing concern in Riyadh over Tehran's ability to inflict serious damage to key operations within the kingdom through malware, which could have widespread consequences globally as well if oil production is affected. Iran clearly is determined to become a dominant cyber-power. Since 2013, Tehran has boosted its cyber-security budget 12-fold and experts put Tehran in the top five of the world's cyber-powers.

■ The latest cyber-attack against Saudi Arabia began in mid-November.



In 2012, Saudi Aramco experienced a significant breach that infected 30,000 of the state oil company's computers. There is little doubt that Iran was responsible for that incident, though Tehran vehemently denied any association with it. Even more troubling for the Saudi government was the awareness that the hackers likely had inside help from one or more Saudi Aramco employees who had high-level access to the company's computer network.

The latest cyber-attack against Saudi Arabia began in mid-November, when malware destroyed computers at a handful of government organisations, including the kingdom's aviation regulator, the General Authority of Civil Aviation (GACA). Six government agencies were reportedly struck, although two were able to fend off serious damage.

The Saudi government acknowledged that the country's cyber-security department had ascertained that a systematic attack had occurred, including against the transportation sector, but did not identify the other government bodies that were targeted. It is rumoured that the kingdom's Central Bank was also a victim of the malware.

The November cyber-attack crippled the GACA headquarters for several days by wiping out critical data on thousands of computers and halting administrative operations, though Saudi airports were seemingly unaffected. Riyadh is conducting a full assessment of the cyber-attack but digital evidence points to Iran as the instigator.

Most telling is that the malware employed in the November cyber-attack is a variation of the Shamoon virus that was effectively used in August 2012 to wipe clean the hard drives of three-quarters of Saudi Aramco's corporate computers, replacing all data with the image of a burning American flag. A group calling itself the Cutting Sword of Justice took responsibility for that breach, accusing Saudi Aramco of aiding a "corrupt" Saudi regime in carrying out "crimes and atrocities" in countries such as Syria and Bahrain through use of Muslim oil revenues.

■ Tehran appears to be masterminding another form of warfare against Riyadh.

Though Saudi Aramco's oil operations and exports remained unaffected because the malware did not reach systems software associated with technical operations, the company immediately shut down its corporate computer network to prevent the malware's spread. Saudi Aramco moved quickly to purchase 50,000 hard drives from South-East Asian computer manufacturers. The damage to Saudi Aramco's computer network is considered one of the most destructive cyber-attacks on a single business to date.

Not only did digital evidence point to Iran's involvement in that incident but the theory was that Tehran instigated the breach on Saudi Aramco as retaliation against the United States following an April 2012 cyber-attack on Iran's Oil Ministry and affiliates that forced Tehran to temporarily disconnect its main Gulf oil terminals from the internet to prevent the malware's spread. Because the Iranian oil industry is still largely mechanical and not reliant on the internet, no oil production or exports were believed to have been affected.

The biggest and most damaging cyber-attack against Iran was the Stuxnet virus that in 2010 infected computers that ran the Gulf country's main nuclear enrichment facilities, resulting in the destruction of 1,000 of Iran's 6,000 centrifuges used in enriching uranium. The United States and Israel reportedly collaborated on developing and employing the Stuxnet malware to stall Tehran's nuclear development programme.

According to Andretta Towner, a senior intelligence analyst a CrowdStrike, a security technology firm: "Stuxnet was kind of an awakening for them in cyber-security matters... So the country decided that building the national cyber capability was just the natural next step." Towner was speaking at a conference on Iranian cyber-threats sponsored by the Atlantic Council.

After Stuxnet, Iran committed to boosting its own cyber capabilities. A report issued in December 2014 by cyber-security firm Cylance said that an Iranian hacking group referred to as Operation Cleaver had victimised at least 50 companies in 15 critical industries spanning 16 countries.

Cyber experts point out that Iran's development of its cyber capabilities is two-fold; not only does it enable Tehran to gather intelligence, but it can also be employed for Iran's "other political agendas in the Middle East", Towner says.

Last March, the US Justice Department indicted seven hackers linked to the Iranian government on charges that included attacking the public websites of US banks from late 2011 to May 2013. The indictments, which marked the first time the US government has charged state-sponsored individuals with cyber-attacks aimed at disrupting the networks of a key US industry, named seven employees of two Iran-based computer security firms said to be working on behalf of Iran's Islamic Revolutionary Guards Corps.

Given the strained political relations between Tehran and Riyadh, the Saudi government may be compelled to beef up its own cyber-security skills as Iran has demonstrated its willingness to attack its foe's key industries. Also, given US President-elect Donald Trump's rhetoric suggesting frostier US-Iranian relations may be ahead, the United States also should brace for more Iranian cyber meddling.

Cyber incidents are 'business risk' in the Gulf

N.P. Krishna Kumar

Dubai

Cyber incidents targeting corporations in the Gulf region have seen a steady rise in recent years, putting major companies at increasing risk of frequent and grave attacks. Protecting data can have massive cost implications, experts said.

Shabnam Karim, a Dubai-based senior associate for global legal firm Clyde & Company, notes there has been an increase in issues related to "ransomware" – malicious software designed to block access to a computer system until money is paid – hacking and data breach across the Gulf Cooperation Council (GCC).

"Some of these incidents relate just to the theft of confidential information but there are now regular claims relating to fraudulent payment transactions, which have occurred due to hacking." Karim said.

"According to official statistics, the UAE is the eighth most targeted country globally and the first in the Middle East and Africa for spear-phishing."

"Spear-phishing" is an e-mail spoofing fraud attempt that targets a specific organisation or individual, seeking unauthorised access to confidential data.

■ The UAE is the eighth most targeted country globally and the first in MENA.

"Within the UAE, finance, insurance and real estate sectors were the most affected last year. Close to three-quarters of all attacks were directed towards companies in those sectors. We do not have accurate numbers of [the] incidents in this region. However, we have seen a real increase in the last two years in cyber incidents, across sectors," Karim added.

Gary Hibberd, managing director of AGENCI, a leading cyber-security agency in London, stressed the inability of IT departments to confront cyber threats. "With 1 million new forms of malware created every day and the proliferation of data, to expect the IT department alone to tackle this threat is a futile exercise," Hibberd said during a visit to Dubai.

"Companies at their board level need to see cyber-crime as a business risk. Cyber-security is not an IT problem or a technology issue any more. Corporate strategy and resources have to be marshalled to tackle this on a permanent basis."

Oisin Fouere, managing director of K2 Intelligence and head of the cyber-defence practice within the region, said, "A key measure to ensure that gaps are effectively remediated is to establish and maintain a dedicated and skilled cyber-security function with executive level reporting."

The sectors most at risk are companies with a large amount of customer data, such as health care and telecommunications, Karim said.

"In order to achieve a financial gain, we see hackers frequently targeting banks and exchange houses," he said. "The Bank of Muscat claim in 2013, which resulted in a multi-million-dollar theft from hacking, is a good example of the level of sophisticated criminals that companies in the UAE are dealing with."

"There are several risk mitigation steps that can be deployed. This includes setting up internal policies because cyber-data breaches are not always externally perpetrated but can result from internal actions, such as an employee accidentally clicking on a phishing link," she added.

The information overload and the arrival of the Internet of Things (IoT) with the prospect of 40 billion internet-enabled devices by 2020 will make the situation even more complex.

"A growing number of security weaknesses are being identified as a result of both smart initiatives and IoT deployment," said Fouere. "We firmly believe that until liability for security weaknesses are attributed to manufacturers that this issue will continue to pose significant cyber-security risks both for the government and individual users. Governments should introduce and maintain basic security standards for embedded devices, ensuring that manufacturers carry out adequate security testing of devices before release."

Hibberd said the introduction of IoT, smart grids and smart cities will result in a world that is increasingly interconnected and interdependent.

Asked how risks can be reduced in the future, he stressed that "fundamentally, education is the key and awareness is its close ally".

"We must educate those who create the products we use and it should be legislated that they provide privacy by design and default," he said. "It must be a feature (of the product). Authorities need to put more pressure on organisations to improve their security but, ultimately, we as the users of these devices need to take account for our own safety."

■ UAE's finance, insurance and real estate sectors were the most affected by cyber-attacks in 2016.

Legislation that imposes a requirement upon businesses to declare and report cyber-security breaches would be an effective tool, Karim argued.

"This would provide better data into where and how breaches are occurring, as incidents are often hidden from the public domain, businesses would no longer be able to adopt a *laissez-faire* approach and would have to treat cyber-security as a boardroom issue."

N.P. Krishna Kumar is a Dubai-based contributor to The Arab Weekly.