FINANCIAL TIMES

April 26, 2016 6:53 pm

Cyber warfare: Iran opens a new front

Sam Jones

With its nuclear programme curbed, digital weaponry has become even more central to Tehran's arsenal

The first neighbourhood they unplugged was Olaya, Riyadh's wealthiest and gaudiest central district. By the time they had finished their rampage through the computer systems behind the power grid, the infiltrators believed they had left millions without electricity, crippling hospitals and military facilities.

What the hackers, whose use of Farsi and bespoke malware gave away their Iranian origins, did not realise was that the critical computer networks they had compromised were fake.

The network, complete with Arabic scripting and precise names of individual substations and pylons, was the work of MalCrawler, a cyber security group specialising in protecting industrial computer systems. It was just one of a set of intricate digital honeytraps designed to gauge the intentions of the attackers who routinely tried to crack into the systems owned by MalCrawler's clients. Equally intricate models were made of European, American and

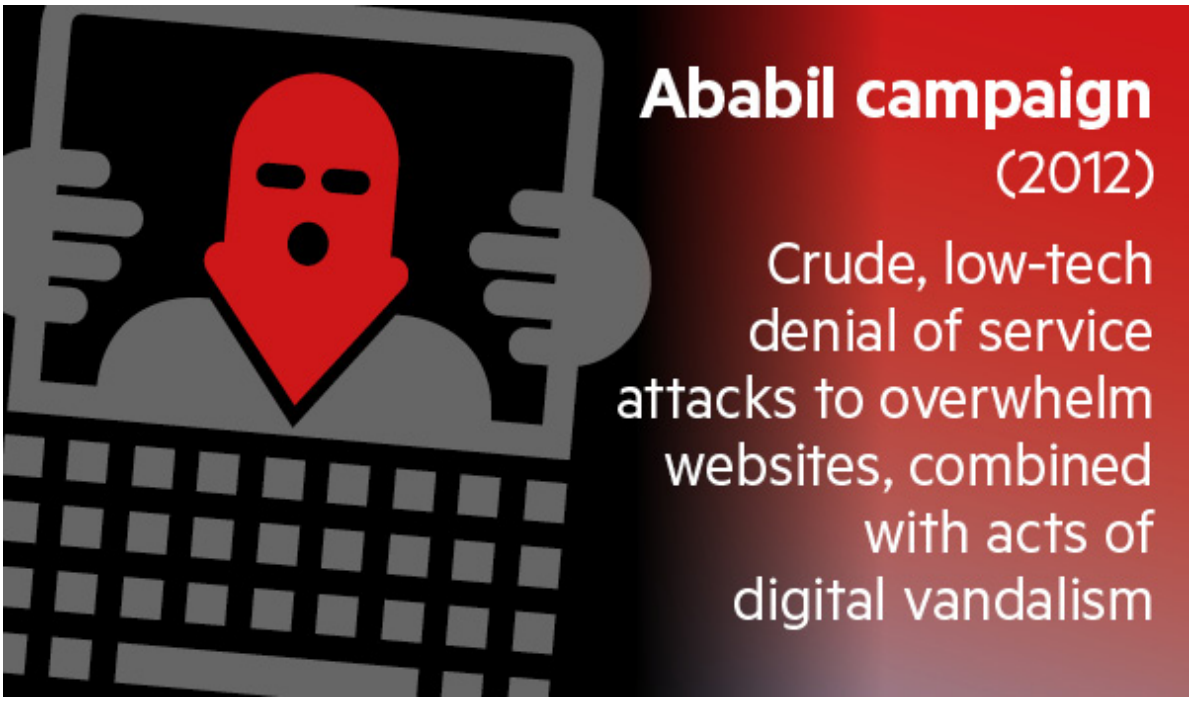
Israeli power systems.

The evidence from the models aligned. The Chinese hungrily scooped up anything that looked like novel technical information. The Russians permeated deep into systems, mapping them and implanting hard-to-find backdoor access for potential future use. But neither dared do damage — unlike Iran.

Among the world's big five cyber superpowers — the US, UK, Israel, Russia and China — MalCrawler concluded there was a digital equilibrium in military cyber offence based on assumptions over deterrence and reprisal.

"But in the Middle East, that's not the case at all," says Dewan Chowdhury, MalCrawler's chief executive. "The mindset just seemed completely different — it wasn't espionage or some kind of targeted operation necessarily, it was just to do as much damage as possible."

The model MalCrawler designed to replicate the Israeli power grid was hit just as hard as the Saudi one. The hackers, again displaying tell-tale signs of Iranian origin, fatally compromised the safety systems of what they thought was one of Israel's nuclear power stations.



Iran is rapidly emerging as the sixth member of the cyber superpower club. Denuded of its nuclear ambitions by the landmark deal struck last year to limit uranium and plutonium enrichment, some fear Tehran will wield its cyber arsenal as an equally long-range weapon with which to menace its adversaries.

"Before the [nuclear] deal, cyber was just one option they used for leverage, but now, post deal, it is even more central to their toolkit," says one senior Middle Eastern intelligence official. "Iran is poised to do something in cyber that will change the way the world looks at it . . . the US knows this. [The US] saw what they [Iran] did during the agreement and they know what they are doing after it."

Industrial sabotage

While high-tech espionage is rife — for strategic state advantage and commercial and criminal gain — destructive acts of cyber attack remain rare.

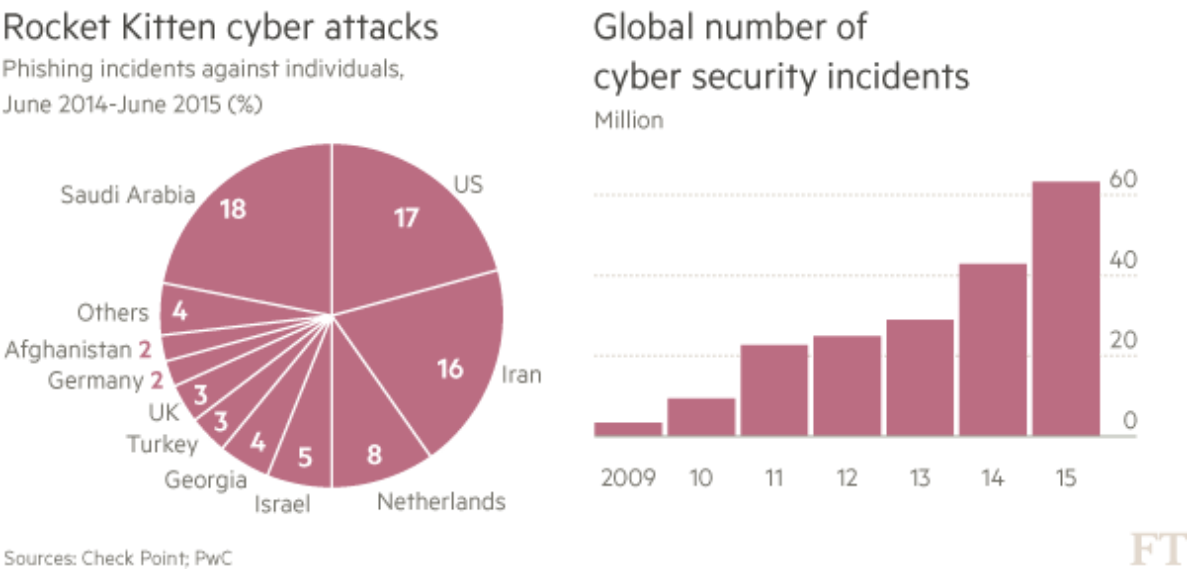
Iran is the only country that has both been on the receiving end of a major act of physical cyber-sabotage and the perpetrator of such an attack. In 2008, the Stuxnet computer worm, created by the US and Israel was unleashed on Iran's nuclear programme.

In 2012, Iranian hackers struck Saudi Arabia's national oil company, Saudi Aramco, nearly obliterating its corporate IT infrastructure, and bringing the company close to collapse.

Aramco was a wake-up call for Iran's adversaries. Nearly four years on, just how strong are Iran's cyber capabilities and what, if anything, will Tehran seek to do with them?

"Their abilities are growing fast and they are diversifying. They're getting harder and harder to track," says one senior intelligence official from within the five-eyes alliance — the digital intelligence-sharing group comprising Australia, Canada, New Zealand, the UK and US. "There is certainly a big move towards having more destructive capability. They want to be able to do more Aramcos. Right now they are researching, practising." Tehran says it spends $1bn a year on cyber programmes. By contrast GCHQ, Britain's electronic surveillance and cyber defence service, annually spends around $2bn.

While its industrial oil production systems were unaffected, Aramco was nearly fatally compromised because so much of its corporate infrastructure was destroyed. Company officials had to use typewriters and faxes to try and keep billions of dollars of oil trades from falling through. Domestically, the company gave oil away for several days following the attack because it could not process transactions.



Christina Kubecka, a cyber security expert who worked for the oil company, told CNN last year that company officials flew to Southeast Asia to acquire as many computer hard drives as they could straight off factory floors.

But the Aramco incident was also a relatively unsophisticated hack. One senior security consultant who worked for the Saudi government in 2012 told the Financial Times that during the very early stages of the operation, the Iranian infiltrators — who dubbed themselves the Cutting Sword of Justice — stumbled on a Word document saved on an IT department hard drive, entitled:

"Administrator passwords".

Iran's other big cyber operation at that time was Operation Ababil, attributed to a hacking group known as the Cyber Fighters of Izz ad-Din al-Qassam. It launched crude, but sustained attacks to try to overwhelm the websites of some of the US's largest banks including JPMorgan and Bank of America Merrill Lynch. The group claimed no allegiance, but two senior western intelligence officials and other independent cyber security experts say it was an Iranian proxy.

In March this year, the US justice department brought charges against seven Iranians who it said were responsible for the attacks. All worked for Iranian companies — fronts, said prosecutors, for Tehran's Islamic Revolutionary Guards Corps.

The attacks were "the first shot across the bow", says John Hultquist, director of cyber espionage analysis at iSight. "Since Aramco [and Ababil], we have seen significant development from Iran in terms of their operations and capabilities. I wouldn't call them top tier in sophistication yet, but if I were to list off the most important threats globally — I would put them [in] there. The [importance] of what they are going after, and their sheer aggression, that's the issue."

Lethal kittens and cleavers

Two hacking groups in particular highlight the development of Iran's cyber capabilities. The first, known as Rocket Kitten, has been closely tracked by many in the cyber security industry since 2014.

FireEye, a US digital security company, first identified it as "Ajax security team", noting its use of a spear-phishing campaign — the use of legitimate-looking emails to snare targeted victims into opening malicious attachments or following links — to target Iranian dissidents and Israeli organisations. By 2015, however, other cyber security groups realised that Rocket Kitten, as it was rechristened, was using its own customised malware, not just off-the-shelf code, and was broadening its reach.

Last November, lapses in the Rocket Kitten security procedures allowed the Check Point, an Israeli company, to access the hackers' own software platform, called "Oyun". Check Point discovered a

sophisticated user-friendly application and within it a list of more than 1,842 “projects” — individuals targeted by hackers. When they ran through the list, they came up with a comprehensive breakdown of Rocket Kitten’s targets: 18 per cent were Saudi, 17 per cent from the US, 16 per cent Iranian and 5 per cent Israeli. They ranged from defence officials and contractors, to dissidents, journalists and politicians.

Two intelligence officials, one from Europe and the other from the Middle East, separately told the FT that Rocket Kitten was linked to the IRGC, which, they both added, dominates Tehran’s cyber warfare agenda.

It is a second IRGC-backed group, however, that is of even more interest to western defence and security experts.

In December 2014, Cylance, a US cyber security firm, informed its clients of the activities of Iranian hackers engaged in a project it called Operation Cleaver. Based on a forensic analysis of the hackers’ activities, Cylance pointed to a group that dubbed itself “Tarh Andishan” — “the thinkers” in Farsi — as being behind the action. Thanks to domains, IP and residential addresses used by the hackers in Tehran the research pointed to government-backed organisations as being ultimately responsible.

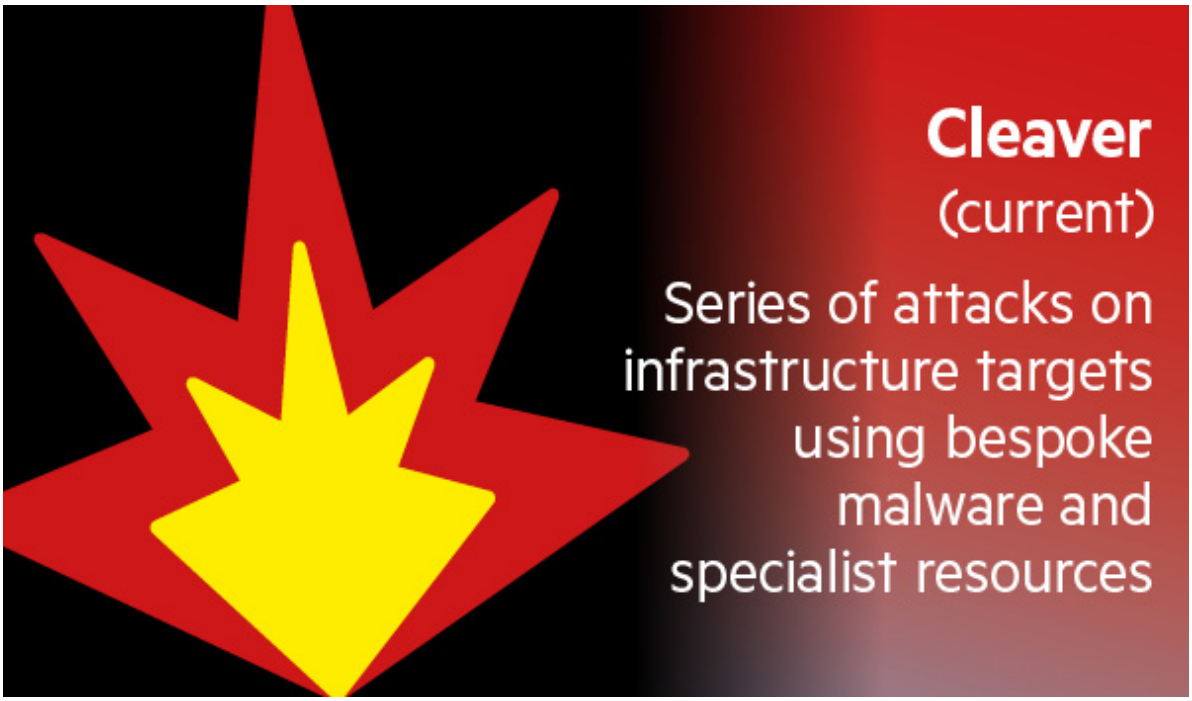
Cylance declared Iran “the new China” for its aggressive actions in cyber space. Its report detailed a sophisticated online campaign, tracked over two years, that was using custom-built malware to deliberately infect and gain access to sensitive industrial control systems and critical infrastructure in companies across the globe.

The hackers behind Cleaver successfully infected the computers of hundreds of companies and sensitive organisations, from military systems, to oil and gas production controls, to airport and airline security databases. The countries hit hardest were not just the regional and traditional foes of Iran. They included places such as South Korea and Canada.

“What Cleaver really brought to the surface was that these guys were aggressive, compromising critical infrastructure in missions that did not have any classic espionage outcome . . . the Iranians aren’t getting into airports and oil and gas companies for intelligence collection . . . these are systems to compromise in order to do harm,” says Mr Hultquist. “What was really eye-opening is that they were doing it globally.”

Complex picture

Knowing what Iran is technically capable of is only part of the picture. Since 2012, when Ayatollah Ali Khamenei, the Islamic republic’s supreme leader, established the supreme cyber council, it has been hardliners that have dominated control of it.



"[Cyber] is folded into the larger context of political and military relationships that the [Iranian] leadership has to sit down and calculate, 'When do I want to do this?'," says Jim Lewis, director of technology and public policy at the Washington-based Center for Strategic and International Studies.

Much of Iran's capability in cyber space stems from its efforts to control dissent and monitor émigrés in the wake of protests triggered by the flawed 2009 election and emergence of the Green movement. The Basij militias — the paramilitary, pro-regime forces under the direction of the IRGC — that were crucial in suppressing those protests are now a critical part of Iran's cyber force.

A second, more sophisticated and highly trained group within the guards is responsible for activities such as those seen in operation Cleaver, says one senior British security official. They make up Iran's equivalent of an elite cyber force, and are the most worrying threat for the west.

Iran's proxy cyber forces form a third component with Tehran accused of being one of the world's most active cyber "proliferators", providing damaging malware to groups such as Hizbollah, the Lebanese Shia militants. Such arrangements do raise questions over control — and just what is being done in Iran's name without explicit sanction from Tehran.

A Basij Cyber Council mobilises "hacktivists" within the Basij — often drawing from Iran's large pool of young, computer-literate students — to further the Islamic Republic's message both internally and externally. It is these groups that are responsible for much of the cruder and more belligerent activity in cyber space — defacing websites and attacking US, Saudi or Israeli companies with denial of service attacks, for example. While they are nurtured and encouraged by the IRGC, there is not necessarily a rigid command structure behind their activities. That makes them unpredictable — and difficult to deter.

In the months since the nuclear deal, MalCrawler, whose digital honeytraps are still in use, collecting data, has noticed a tail-off in Iranian activity. "We're in a period of reorganisation in cyber space," says Mr Chowdhury.

But few expect that to remain the case. "In the short term, as sanctions come off, they want

stability," says one Israeli official, "so they are rethinking their attacks. But people need to understand that they are developing capabilities for use years from now."

Cyber, he says, is as core to Iran's strategy as its ballistic missile programme.

"Before cyber they were powerless," says CSIS's Mr Lewis. "They had to sit there and take it. We had sanctions, we had aircraft carriers off their coast. Now with cyber they can strike back."

RELATED TOPICS United States of America, United Kingdom, China, Oil, Cyber Security

The US in three numbers

Money Spinners - Why didn't Prince have a will?

FirstFT – Fed global concerns ease, SpaceX mission to Mars

VIDEOS