Iran may prioritise cyber espionage, not attack

Wednesday, July 11, 2018

Mutual cyberattacks preceded the 2015 nuclear deal and the US withdrawal raised expectations of a resurgence

US Deputy Attorney General Rod Rosenstein speaks at a news conference with other law enforcement officials at the Justice Department to announce nine Iranians charged with conducting massive cyber theft campaign, in Washington, March 23 (Reuters/Yuri Gripas)

Israeli newspaper Haaretz on July 9 reported that a sophisticated Iranian hacker group known as 'Charming Kitten' tried to obtain user data by impersonating Israeli cybersecurity firm ClearSky as well as international media outlets. Before the US withdrawal from the Iran nuclear agreement, many observers expected Tehran to increase its use of asymmetric capabilities, especially cyber tools, in retaliation. This would affect not only the prospects for the deal itself, but also cybersecurity risks to companies and governments regionally and worldwide.

What next

Iran is unlikely drastically to alter its offensive cyber operations due to the breakdown of the nuclear deal. Instead, it will be cautious, seeking to maintain a 'below-conflict threshold'. Tehran's interests in the United States and Europe are better served by covert espionage. However, it is likely to proceed with potentially damaging cyber operations against other regional rivals, especially Saudi Arabia. Israel is relatively well defended, but oil and gas operations in the Gulf states could be at risk.

Subsidiary Impacts

- Iran will still allocate significant resources to its maturing offensive cyber capabilities.
- Top espionage targets will include European and US universities and defence sectors, as well as other sectors hit by sanctions.
- As part of their multi-pronged diplomatic and economic campaign against Iran, Washington and Tel Aviv may look at new cyber options.

Analysis

US President Donald Trump announced his country's withdrawal from the 2015 Joint Comprehensive Plan of Action (JCPOA) on May 9, claiming it was "the worst deal ever" (see IRAN: Partners will struggle to save the nuclear deal - May 9, 2018).

Since then, despite the other signatories' promises to honour the agreement, economic pressure on Tehran has been mounting (see PROSPECTS H2 2018: Iran - June 29, 2018). This has raised the question of how Iran might respond.

Cyber aspects

In the past, Iran's nuclear programme was associated with a range of cyber operations, including sabotage and espionage against the programme itself by adversaries, as well as Iranian cyber responses to the imposition of sanctions.

This association began in 2010, when the destructive Stuxnet malware -- subsequently indirectly claimed by US and Israeli officials -- was discovered in Iranian uranium enrichment facilities (see IRAN: Tehran is set to become a formidable cyber actor - December 28, 2017). The extent to which it set back Iranian enrichment is contested, but it probably had some effect.

In October 2012, the United States and EU imposed new economic sanctions in response to Iran's nuclear and ballistic weapons programmes. Around this time, distributed denial of service (DDOS) attacks against US banks were attributed to Iran by senior US government and former government officials, who believed Tehran was retaliating for the sanctions.

An alleged 'Iranian hacker collective' investigated international nuclear officials

Cyber operations were also observed to target the International Atomic Energy Agency (IAEA), responsible for monitoring Iran's compliance with the Treaty on the Non-Proliferation of Nuclear Weapons. A group calling itself 'Parastoo' (later identified by a cybersecurity firm as an 'Iranian hacker collective') in November 2012 obtained IAEA officials' personal information and technical documents.

In 2014-15, cybersecurity firm Kaspersky identified a cyber-espionage campaign targeting JCPOA negotiation venues. This campaign included an updated form of malicious software identified in 2011, which -- like Stuxnet -- used 'zero-day' vulnerabilities. It was probably conducted by Israel, given 2015 claims by anonymous US security officials that Israel had provided Congress with information about the negotiations that was only obtainable through espionage.

Offensive structure

Tehran's offensive cyber structures are characterised by diffuse chains of command and fluid groupings. The loose and transient relationships between commercial companies and military organisations are extremely different to US or Chinese arrangements.

The Parastoo example highlights that Iranian cyber activity is often not clearly attributable directly to the state. This is also the case for the most high-profile cyberattack attributed to Iran by US security officials, the Shamoon attacks against Saudi Aramco in August 2012, originally claimed by a hacktivist group called 'The Cutting Sword of Justice'.

Similarly, allegedly Iranian actors wiped thousands of servers and computers owned by the US-based Sands Casino in 2012, likely in response to comments by its owner Sheldon Adelson in favour of bombing Tehran. Dell SecureWorks, the cybersecurity company investigating the response, claimed the operation was conducted by Iranian 'hacktivists' -- and assessed this must have been with the government's knowledge.

The 2012 DDOS attacks were claimed by a group called 'Izz ad-Din al-Qassam Cyber Fighters', but the 2016 US indictment relating to this operation instead identifies seven individuals working for two Iranian firms -- ITSecTeam and Mersad -- as acting "on behalf of the Iranian government".

However, other indications suggest that at times, Iranian state direction is unclear, or that personal initiative plays an increased role. For example, one of the DDOS indictees also apparently infiltrated the control systems of an unrelated US dam, with no indication of intent to damage or disrupt its function -- which could imply an independent exploration by the hacker.

This structure, with commercial companies apparently conducting offensive cyber operations on behalf of the Iranian state, is representative of a wider pattern. Skilled individuals drawn from universities and commercial cybersecurity firms pursue cyber operations in line with the strategic goals of various state organisations, including the Islamic Revolution Guard Corps (IRGC), advancing within the structure with instruction and cooperation from these government arms.

The most recent example comes from the 2018 US indictment of nine individuals associated with Iran's Mabna Institute, which describes them as "leaders, contractors, associates, hackers-for-hire or affiliates", and connects the Mabna Institute to the IRGC. They are accused of stealing data from universities, government organisations and private firms in the United States and worldwide.

Future scope

Following a global trend, recent Iranian operations have been much more sophisticated than earlier disruptive attacks linked to the nuclear negotiations (see INTERNATIONAL: Cyber conflict will be more destructive - April 25, 2018).

However, it is unlikely that Tehran will explicitly order offensive cyber operations resulting in destruction or disruption in retaliation for Washington's JCPOA withdrawal and 'economic warfare'. Currently, Iran occupies the moral high ground from the perspective of the other signatories, and this is useful in seeking to maintain wider economic ties.

Cyber warfare would be a high-risk revenge strategy

Even if a cyberattack on US interests were designed to be deniable, claims of Iranian responsibility would be likely to emerge quickly, given the extent of Western intelligence monitoring of Tehran. This would involve an immediate loss of social capital and likely retaliation.

Nevertheless, the diffuse structure of Iranian operations means hackers can act independently of direct tasking, so a residual risk of destructive attacks remains.

Moreover, regional operations display a different dynamic. The malware used in the Shamoon attacks returned in 2016-17, wiping many Saudi government departments' data and temporarily shutting down the Civil Aviation Authority.

Also in 2017, cybersecurity company FireEye discovered a form of malware -- attributed to Iran by multiple cybersecurity companies -- on the industrial systems of a petrochemical plant in Saudi Arabia that could alter safety constraints and thereby damage the physical systems themselves, as Stuxnet did. This suggests that oil and gas sectors in the Gulf remain at risk of disruption.

Offensive options aside, Iranian cyberespionage is likely to increase after the US withdrawal. Iran will seek not only to bolster its conventional security capabilities by obtaining advanced defence technologies from its adversaries, but also to compensate for lost investment.

It may therefore obtain and replicate technology in other affected sectors, such as advanced industrial manufacturing or hydrocarbons extraction. Targets whose intellectual property are at risk may also include European organisations, as firms withdraw from Iran out of fear of US sanctions.