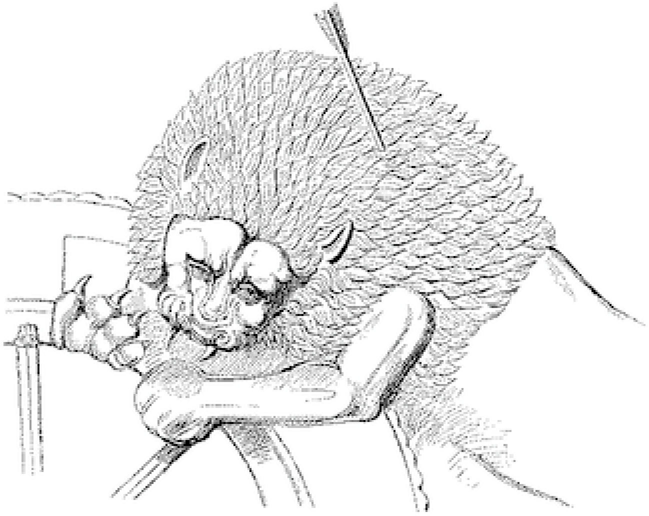
APT34 Tools Leak

blog.eutopian.io/apt34-tools-leak

June 16, 2019



Leak Summary

APT34 is an Advanced Persistent Threat group associated with the Islamic Republic of Iran. Its source code and tools were recently leaked via a Telegram channel. In addition to those tools, information was divulged about the group's targets which included companies and governments in the United Arab Emirates, Kingdom of Saudi Arabia, China, Qatar, and Turkey among others. The "Dookhtegan" group leaking APT34's information expressed particular animus towards the Iranian Ministry of Intelligence. As of mid-May 2019, the leaks continue via a Telegram channel.

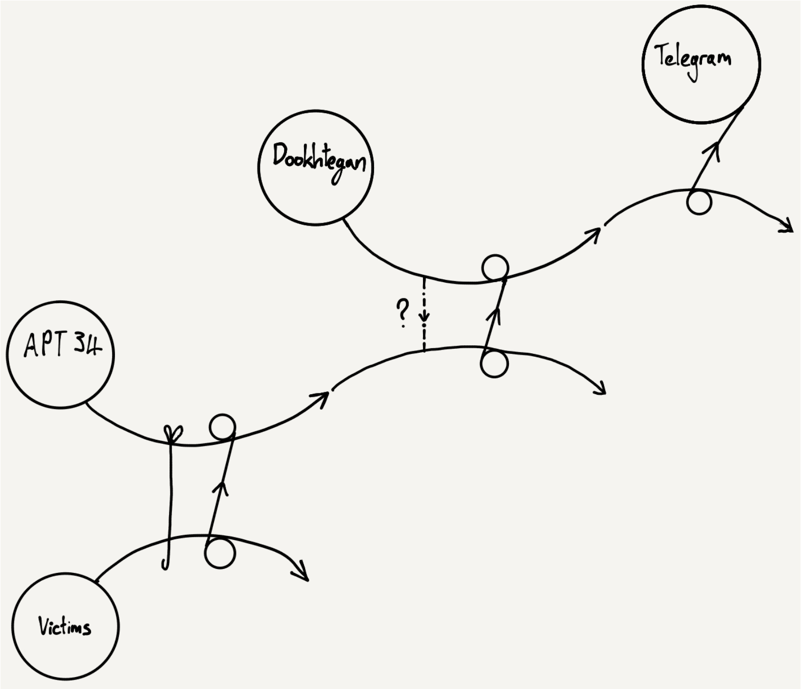
The tools themselves were unremarkable, as were the infrastructure details. What was interesting is that the details of APT34's victims were leaked. Along with the timing, this fact is *the* significant feature of this incident and one I will return to later in this post.

> Most people don't follow Cyber Security current affairs in anything other than a casual way. For them, isolated incidents come and go like waves of a fever. Commentators describe an individual leak, breach, or scandal, but these are just surface ripples. I'll reveal the deep ocean currents driving them. I'll describe why they are occurring and who they benefit. I'll help you see more clearly by understanding the context in which these events take place. - The Projectionist, April 2019.

Leak Announcement

> Source code of Iranian cyber-espionage tools leaked on Telegramhttps://t.co/guVv15igNx pic.twitter.com/QhcdzN12O5
>
> — Catalin Cimpanu (@campuscodi) April 17, 2019

H Diagram



APT34 Leak, April 2019.

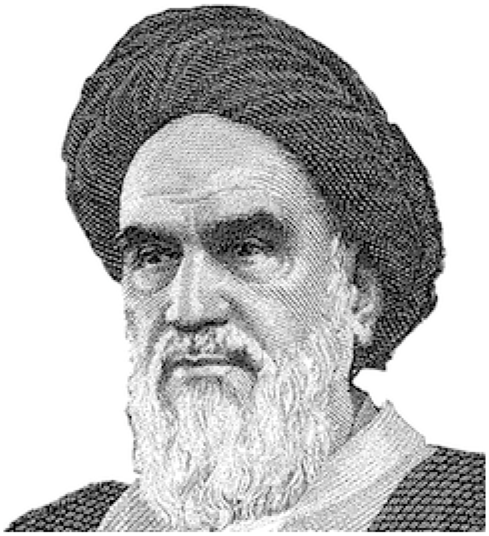
> This post is about the Geopolitical and strategic context within which these events take place. Knowing this context will help you anticipate and counter future threats and make sense of developments involving these actors or this geography.

Introduction To Iran

Iran is arguably the world's oldest country. Not only does it have one of the longest recorded histories but it has undergone huge political, social, and economic change just in the last 50 years. It has complex international relations in the region and beyond with both state and non-state actors. Iran's fabric is as intricate as a Persian carpet. Iran's society is woven out of different threads of ethnicity, language, religion, and ideology. This post examines the APT34 leak within that context. The process starts with understanding what Iran wants and why.

I've attempted to summarise Iran for those who don't know the country. That summary is necessarily quite long. If you want to skip that background and go straight to the APT34 part, click here to save yourself 10 minutes.

Iran's Aspirations

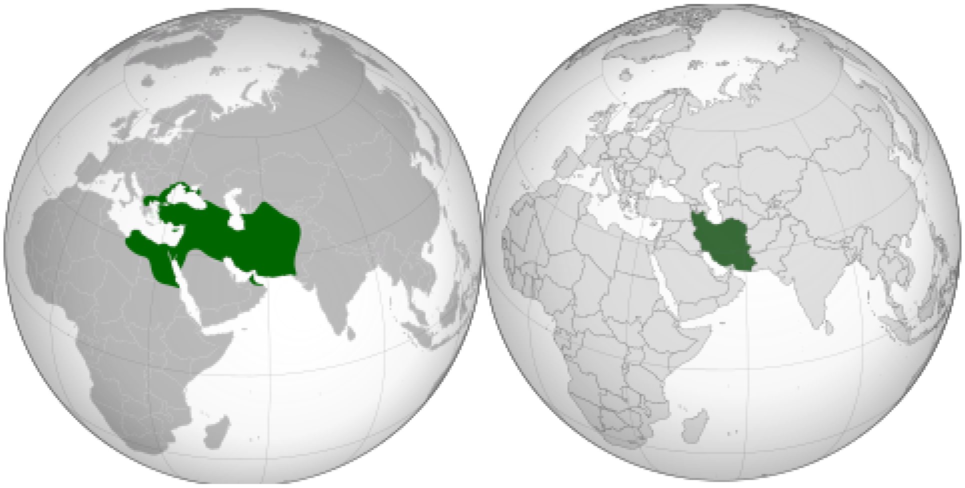


"I'm taking it back 1400 years to the times of Rasool Allah Amir and al-Mu'minin." - Ayatollah Khomeini 1902 - 1989.

Iran seeks regional hegemony. Their pathway to achieving it is:

- Grow and strengthen its sphere of influence.
- Exclude powers, proxies, and influences that oppose it.
- Control economic and strategic assets and locations.
    - Iraq, launchpad into Syria and Saudi Arabia.
    - The Saudi oil market.
    - The Persian Gulf.
    - Access to the Mediterranean.

Iran wants to realise the vision of the Islamic Revolution of 1979 as expressed in the writings and pronouncements of Ayatollah Khomeini. In a historical context, this means Iran wants a sphere of influence similar to that of the Persian Empire of 2000 years ago.



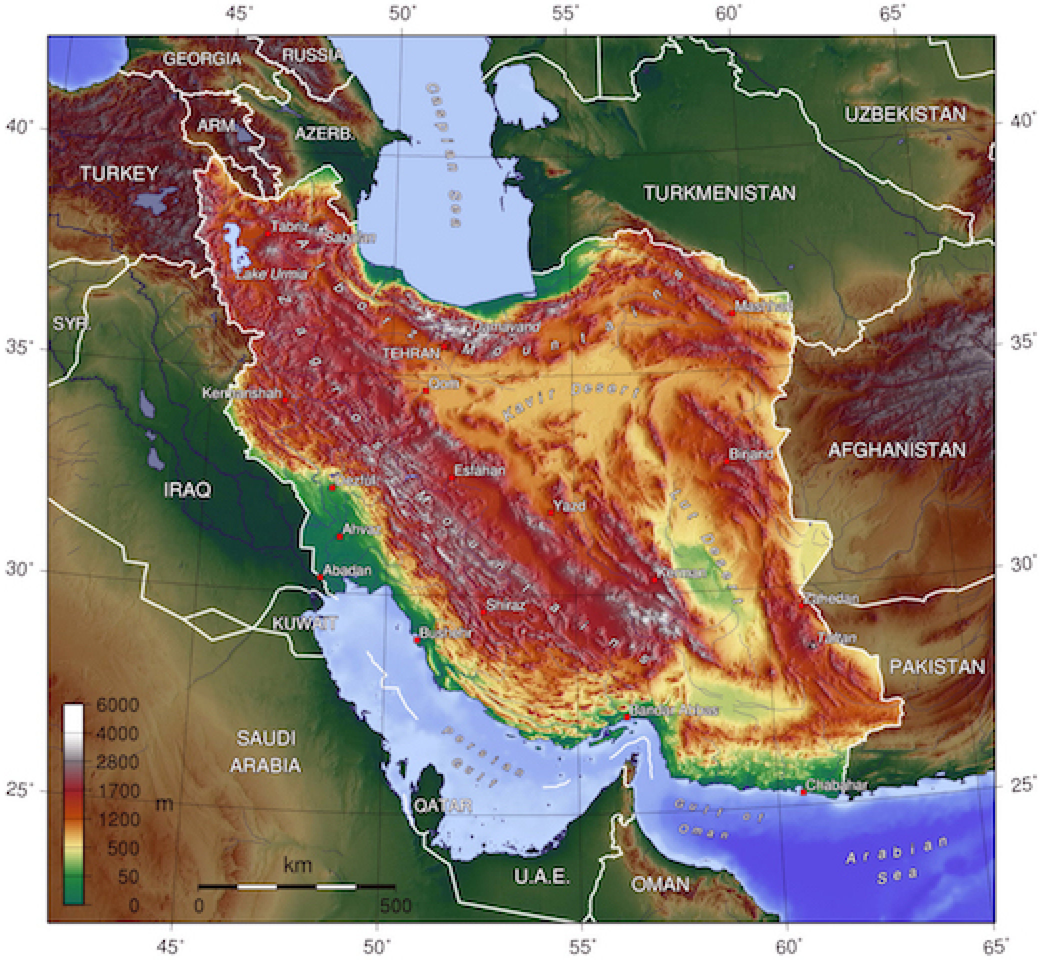
Achaemenid Empire (521 BC - 486 BC) & Iran (present day).

Iran's Geography

"Geography is destiny" - Ibn Khaldun 1332 – 1406.

Iran's borders have barely changed in 500 years and are a result of physical geography. The country is both protected and constrained by mountains and coastline. Satellite imagery shows the stark contrast between flat Iraq and mountainous Iran. Many of Iran's enemies have come to grief in the Zagros mountains which mark the western flank of the country.

Only the Khuzestan province in the South West of the country looks vulnerable, but it's partly a swamp. This makes it far less attractive for an invader than it would otherwise be. Historically this is where the border lay between Persia and Mesopotamia. This particular region presents other difficulties for Tehran as we will see later. The centre of the country is an uninhabitable wasteland.



Iran's Ethnography

"I am Darius, the son of Vishtasp. My clan is Achaemenid, my tribe is Persian, and my nation is Aryan" - Darius the Great 522 - 486 BC.

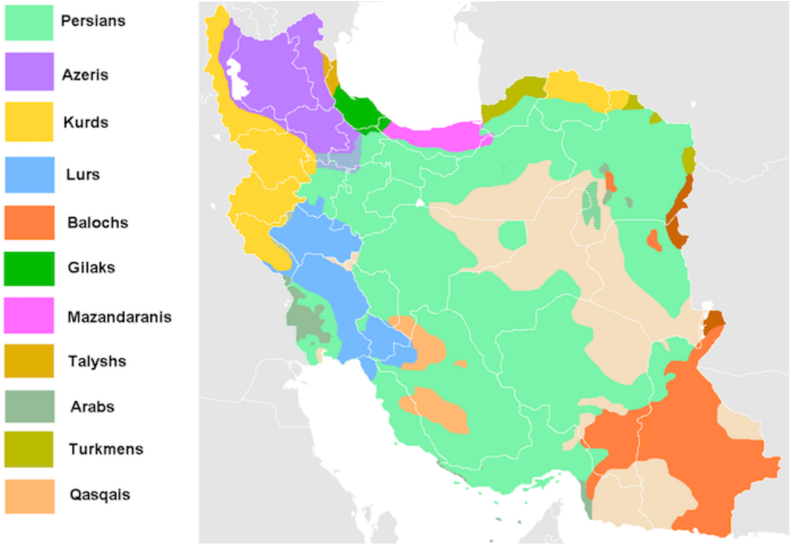
Aryan or Iran as it is now known, is home to more than half a dozen different ethnic groups and over 10 languages. The country is a remnant of a once great empire. Therefore Iranians have an understanding of a functioning nation composed of many ethnicities. Persians of the Shia sect are one of those, albeit the largest at around half of the population.

The Azeris or Azerbaijanis come from the North West. Their language is effectively banned in schools in spite of the fact they are ~20% of the total population. This area is known as Iranian Azerbaijan, not to be confused with the Republic of Azerbaijan further North.

In Khuzestan in the South West, the population is Arab, not Persian. It's also where the Shatt al-Arab waterway meets the Persian Gulf and has been the scene of several confrontations between the British Royal Navy and the Navy of the Iranian Revolutionary Guards. Khuzestan receives significant attention from the intelligence services who are always watching for secessionist sentiment or those who might encourage it.

The Balochis in the South East are Sunni Muslims, like the Azeris and some of the Khuzestan Arabs.

Finally, there are Kurds in the West who also inhabit mountainous regions of Iraq and Turkey. Like most of non-Persian Iranians, Kurds are Sunnis.



Ethnic composition of Iran (present day).

Ethnography & Secession Risk

In spite of ever-present secessionist sentiment, there's less risk of Iran splintering along ethnic lines than one might imagine. Tehran manages each group carefully through a mixture of punishment and reward and the pull factors are not that strong.

- Each group has seen what happens when a state disintegrates.
  Iraq, Syria, Libya, Afghanistan, Yemen.
- Iranian culture integrates them to a degree.
  National myths, symbols, historical figures.
- Most would-be secessionist states aren't viable.
  Particularly if Iran is to be an unfriendly neighbour.
- For regions choosing to become part of a neighbouring state, life would likely get worse, not better.
  There's no near-term prospect for a real Kurdish state.
- No external force pushing secessionist movements in a meaningful way.

Iran's Religion & Government

"We are not afraid of your science and of your technology. We are afraid of your ideas and of your customs. Which means that we fear you politically and socially. And we want this to be our country. We do not want you to interfere anymore in our politics and our economy, in our habits, our affairs. And from now on, we will go against anyone who tries to interfere – from the right or from the left, from here or from there." - Ayatollah Khomeini, interview by Oriana Fallaci, October 14th 1979.

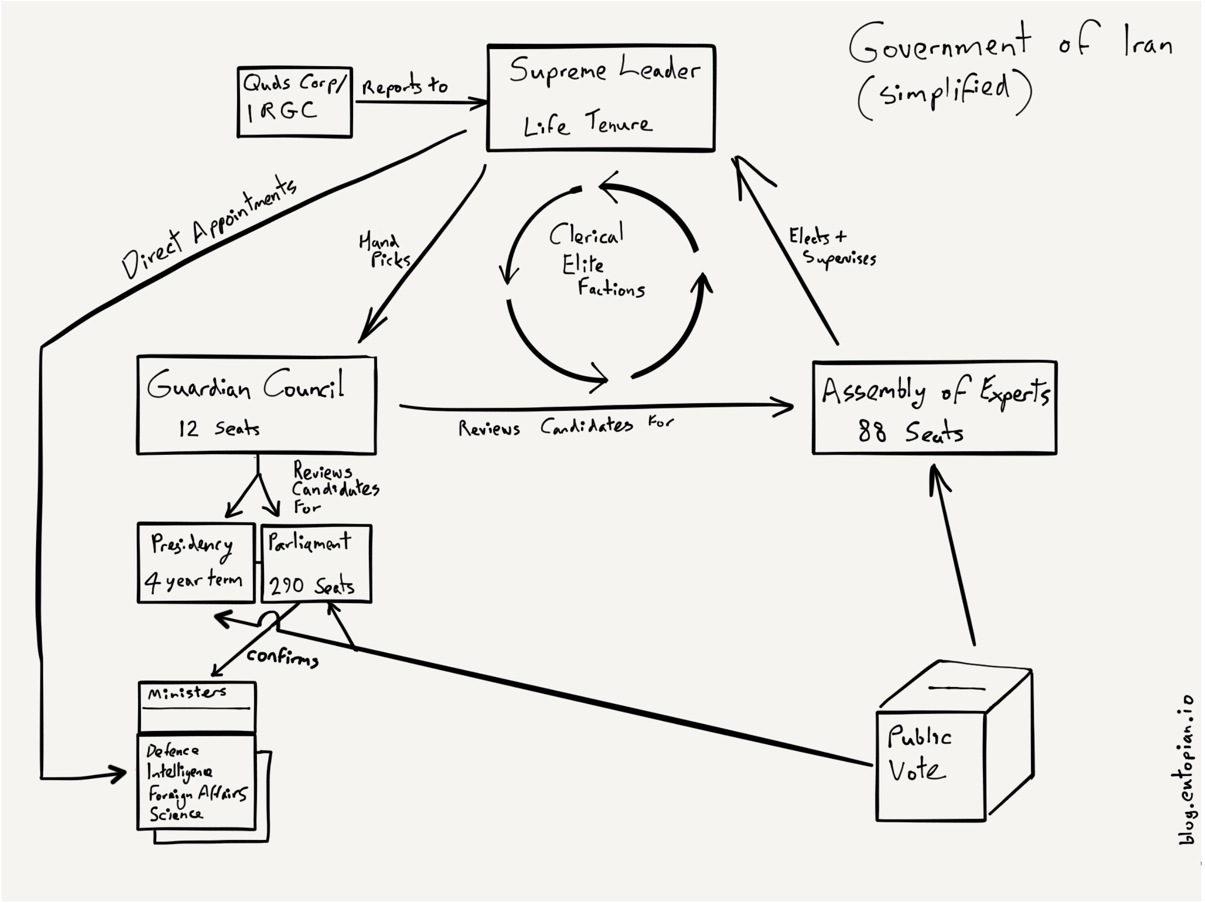
Iran is an Islamic Republic. Religion is at the centre of power in a way that casual observers in the West may struggle to understand. It's impossible to talk about Iran's government without talking about religion, and vice versa. 98% of the country is Muslim, and 90% of those Muslims are Shia. 8% are Sunni and 2% other sects. Most of the Sunnis are ethnically Kurdish, Balochi, Turkmen, or Arab.

Although it has elected institutions including a Parliament, Iran is a theocracy. This fusion of religion and democracy might have worked, but fighting between factions and institutionalised corruption has left the wider population at a disadvantage.

After the revolution of 1979, a new constitution was drafted based upon the word of Khomeini. Shortly after that time, the Iran/Iraq war provided cover for the clerical faction of the revolutionary movement to purge the republican faction and consolidate power. In 1988 alone 30,000 Iranians were executed by their own government. Institutions were suspended, cleansed, and re-constituted according to Khomeini's teachings. Thousands of teachers, doctors, lawyers, academics, scientists, writers, and artists fled the country in what became known as the Iranian Cultural Revolution.

> As a boy, every Iranian I’d ever met or heard of was either a scientist, a doctor, a scholar, or an author. I wondered what sort of a country it was that produced *only* people of such calibre. It was an early lesson in selection bias.

The constitution intertwines legislative and religious authority. While it has the superficial appearance of democracy, when these structures are fully unwound, all real power rests with the clerics. There is no transparency. A veneer of democracy gives legitimacy to the government while preventing any real change. Both the system of government and society remain locked down. Candidates are selected before any public vote can take place.



Iran’s Government (simplified).

Although the system is rigid, there are several factions and a great deal of manoeuvring. In the parliament, there are both moderates and conservatives with differing views on:

- The supremacy of constitution vs religious law.
- The degree of social reform desirable.
- The relationship with the West.
- The form of the economy.

The Political Spectrum

There are broadly 4 groups on the Iranian political spectrum. Their names and faces change over time and their fortunes rise and fall, but these divisions remain. As always when comparing political systems and groups in one country from a position within another, language and definitions can be difficult. In reality, there is a void between the Reformist movement and the Moderates, while the other factions are closer together.

	Reformist	**Moderate**	**Conservative**	**Hardline**
Faith/Law	Secularism	Elected inst. above religious authority	Religious authority above elected inst.	Religious authority
Social	More liberal	Rather conservative	Islamic social values	Literal interpretation
The West	Normalisation	Trade	Confrontation inevitable	Confrontation inevitable
Economy	Free market	Liberalisation	Liberalisation, but keep social values	Decentralised
Key Figure	Mousavi (Arrested)	Montazeri (d.2009), Rouhani (President)	Khamenei (Supreme Leader)	Mesbah-Yazdi

Upon the death of Ayatollah Khomeini in 1989, the designated successor Ayatollah Montazeri (a relative moderate) was sidelined for the conservative Ayatollah Khamenei who has ruled as Supreme Leader ever since. Elected Presidents have included moderates like Rouhani (present), Khatami, and Rafsanjani and conservatives like Ahmadinejad.

Once upon a time the key figures in the table above worked together. Many were even pictured smiling in a relaxed manner in a single frame. Today those men are divided. Undeserving of even a name-check on the Supreme Leader's Instagram.

These divisions are set against a backdrop of poor economic performance and dissatisfaction among voters. The Iranian Parliament and its various Councils and Assemblies are not representative of Iranian society. Nor will they ever be while candidates are screened and selected in the non-transparent way described in the simplified diagram above. This creates a tension in society which flares up from time to time, particularly when the public experiences adverse economic conditions.

Iran's Economy

Iran's economic growth hasn't kept pace with its population growth. This lead to a decline in the standard of living since the baby boom. Iran took drastic action to reduce the birth rate, which it did very successfully. Now they have the opposite problem, an ageing population and not enough growth at the bottom to support it. Today the government is attempting to grow family sizes again, but without much success.

Oil

Iran is rich in oil but it’s unable to take full advantage of this. The oil industry suffers from:

- Unfortunate physical location of hydrocarbons (high transport cost).
- Sanctions stunting the industry.
- Increased domestic demand since 1960s/70s.
- Inefficiency within the oil ministry.

These factors combine to produce an effect where a rise in oil prices doesn’t result in a significant rise in the standard of living for Iranians. Iran has limited capacity to refine. For this reason, it *imports* up to 30% of its gasoline. This is one factor driving Iran’s interest in the Saudi oil assets, which have a much lower breakeven price.

Inflation & Exchange

Iran relies heavily on food imports, to buy these it needs foreign exchange (US dollars). Sanctions prevent Iran from obtaining enough dollars which leads to shortages, food price inflation, and protests. The official inflation rate means very little when dollars simply cannot be obtained.

> #Iran's annual inflation rate, measured accurately this morning, is 139%, more than double the phony government rate of 51.4%. pic.twitter.com/9giTXZJMSm
>
> — Steve Hanke (@steve_hanke) May 17, 2019

Ports & The Strait Of Hormuz

The Strait of Hormuz

Iran is on the Strait of Hormuz. The strait is a narrow gateway through which 40% of the worlds sea-bourne oil passes. This strait is far more important than any nuclear programme. It’s just 32km wide at the narrowest navigable point.

Iran has one major port at Bandar Abbas and one major oil terminal at Kharg Island. Kharg handles 90% of Iran’s oil exports. The country has never been much of a maritime power.

Iran has an assortment of anti-ship missiles, mines, and aircraft easily capable of saturating this tiny span. If the straits were closed for even a few days there would be worldwide economic impact. It is Iran’s strongest card and yet also a double-edged sword. Closing the strait would be a “nuclear” option and would elicit a corresponding response.

In 2012 a pipeline was completed between Abu Dhabi and Oman bypassing the Strait of Hormuz, but capacity is limited. The strait remains a strategically important choke point for the worlds hydrocarbon supply.

Iran’s Regional Friendships

Iran exercises influence over a wide geographic range. It does this either directly or indirectly through a number of proxies. These proxies are aligned with Iran either because of religion, a common enemy, ideology, or mutually shared interest or shared fortunes. They are not wedded to Iran. While the existing power structures of the region remain in place (particularly the al-Assad government in Syria), it suits them to work with and sometimes for Iran.

- Iraq

  Iran has good relations with the Arab Shia elite currently attempting to govern in Iraq. Iraq is today as it was in antiquity, the key to greater Iranian influence throughout the region.
- Syria

  Bashar-al Assad (and the Alawite elite) have faced a mostly Sunni uprising. Syria's port on the Mediterranean is of strategic interest to Iran.
- Lebanon

  Hezbollah is a Beirut based Shia political party and militant group dedicated to harassing Israel. It was partly founded by Iran. Iran continues to provide the organisation with funding, intelligence, and weapons. If Iran is attacked, Hezbollah can be instructed to strike at Israel in return. Iran has also used Hezbollah to shore-up al-Assad's position in Syria.
- Afghanistan

  Iran has long experience with Taliban and ethnic Persians in Afghanistan. They are capable of destabilising the country if and when it suits them.
- Gaza Strip

  - Palestinian Islamic Jihad's (PIJ) objective is the destruction of the State of Israel. They're supported by Iran with intelligence, funding and weapons. The group can be instructed to strike against Israel should it suit Iran to do so. The group is an offshoot of the Muslim Brotherhood.
  - Hamas similarly wish the destruction of Israel and are Sunnis. Iran supplies them with funding, intelligence, and weapons. They can be called upon to conduct operations aligned to Iran's wishes.

Syria is particularly important because assuming al-Assad's government survives, and it looks like it will, relations between Iran and Syria will be at a historic peak. In exchange for the unconditional support Iran offered, it's reasonable to expect Iran to obtain whatever access it needs to the Mediterranean port of Tartus. Secondly, from Syria it's easy to exercise more influence over Lebanon. Doubly so with the Hezbollah connection in place.

> Iran is no tin-pot dictatorship or Banana Republic. It has extensive networks within the region which can engage in activities from destabilisation and hit-and-run attacks through to larger more organised offensives. Iran's sphere of influence runs from Turkey and Georgia all the way to India. The country is continuously fighting a low-level proxy war with Israel while Israel attempts to prevent it from obtaining nuclear weapons. Hamas, Hezbollah, and PIJ do not pose an existential threat to Israel, although they could make life a misery for Israelis. The existential threat comes from elsewhere. It comes from the Iran/Syria/Iraq configuration, a creeping non-Zionism within European policy formation, a gradual reorientation to moderate Arabist viewpoints, and over the next 50-60 years in the Arab birthrate inside Israel and the territories.

Iran And The Bomb

Iran doesn't strictly need a nuclear weapon to achieve regional hegemony. The nuclear programme is most valuable as a bargaining chip and as a repellant to ward off regime change. However if a device is assembled and tested it's reasonable to expect that a regional arms race will result. The Saudis will demand one of their own to balance Iran. A number of countries in the region already have very low-level programmes.

APT34 Leak In Context

Short Term Consequences

This incident is a minor inconvenience to APT34 and by association Iran. It forces them to do work in building new control infrastructure and discloses APT34's activities to their targets if those targets were not already aware. It may also cause individuals some problems now that they've been named as Iranian Ministry of Intelligence Officers. Particularly if they undertake projects outside of their work with the state, or travel to other countries.

Long Term Consequences

All of the organisations or states named in the leak know that they are of interest to Iran. There will be a certain amount of embarrassment because they have been compromised, but this will pass. In the long-term the leak may even have a positive effect of reminding those organisations to improve their Cyber Security in the face of increasing geopolitical tensions. Next time they may not be so easily breached.

There's no love lost between UAE, KSA, Jordan, Bahrain, Israel, and APT34's sponsor. Iran seeks regional hegemony and those countries stand to lose from that. They've been targeted in the past by Iranian proxies and partners. However, these were not the only countries where corporations and government departments were breached by APT34 and subsequently disclosed. APT34's work also included hacking into those that could loosely be defined as friends of Iran.

- Kuwait

  Kuwait's government was targeted. The country has a mixed relationship with Iran since the Islamic Revolution of 1979. It backed Iraq in the Iran/Iraq war of 1980-88 and is broadly against Iran having more influence in the region. However, Kuwait has stopped well short of the position of the other Gulf States. The fact that Iran has been caught spying on them will make it a little harder for the country to maintain this position. However, Kuwait has kept-up warm relations with Iran in spite of spying scandals in the past. The likelihood is that Kuwait will do what Kuwait does best, be a middle man.
- Qatar

  The Qatari government was targeted. Qatar shares the South Pars/North Dome Gas-Condensate field with Iran. It's the world's largest natural gas field. It also has linked oil interests. Iran came to Qatar's aid during the 2017-19 crisis with food, finance, and diplomatic assistance. That an Iranian APT has been caught targeting the government of Qatar is somewhat embarrassing but their friendly association will survive. Qatar is aligned with Iran (and Turkey) within the region. However, ultimately Qatar's security is guaranteed by the US air base it hosts.
- Turkey

  Turkish energy, construction, and government entities were targeted. Iran has good relations with Turkey, but it's not an entirely straightforward arrangement. The AKP government of Turkey supports the opposite side to Iran in both the Syrian Civil war and the war in Yemen. However, Iran was quick to voice support for the AKP government during the failed 2016 coup d'état. Both Iran and Turkey backed the Qatari's in their dispute with KSA and the UAE. Iran and Turkey also back each other against US sanctions. This is in spite of the fact Turkey hosts a US/NATO airbase US/NATO nuclear weapons.
- China

  China's energy, telecommunications, financial, and technology sectors were targeted by APT34. In the past, China has been at least partly responsible for some developments within Iran's nuclear programme and its anti-shipping missiles. Iran now relies on China's backing at the UN to reduce pressure from the US and elsewhere. China is sure to play an important role in Iran's future. Given all of this, the public disclosure of APT34 operations against China may end up being one of the more significant.

It would have been *far* more significant if Iran had been caught undermining Hezbollah, Palestinian Islamic Jihad, Hamas, the Shia elite in Iraq, or the administration in Syria. Tehran relies on these partners and proxies for influence. There was relatively little mention of Israel in this leak, although there were some web shells disclosed. This is somewhat surprising given the level of interest Iran has in Israel. Perhaps APT34 isn’t trusted with them as a target? Perhaps the leaked data was filtered and curated by Dookhtegan before release?

Allies spy on each other. The British spy on the Belgians, the French spy on the British, and the Americans spy on the Germans. The problem comes in managing public opinion. It will be slightly harder for otherwise friendly states that have been targeted by Iran, to be publicly supportive of a country caught hacking them. However, while there’s no political home for negative popular sentiment, that sentiment will pass.

Who Are Dookhtegan?

There’s scant information in the articles posted. Dookhtegan are particularly hostile towards the Iranian Intelligence Services, yet there is no ethnic, sectarian, or other charged language. They use the Farsi slogan “امروز نوبت ماست صدایتان را خاموش کنیم!” or “Today is our turn to turn off your voice”. This suggests that the group or individual feels they are routinely suppressed. Their avatar is one of a person with their lips stitched together. Other imagery and phrasing suggest they are associated with the Green Movement and the Reformist faction of the Iranian political spectrum described above.

There may be an Azeri connection. Within Iran, the Azeri language is more or less banned in schools, in spite of the fact they are 20% of the population. However, Azeris speak the Azeri Turkish language, not Farsi. Many feel unable to speak freely in Iran, be they of an ethnic, religious, demographic, or other grouping. It’s just as likely that Dookhtegan is an agent or proxy of one of the states opposed to Iran. It may be an individual with sympathies for People’s Mujahedin of Iran (MEK). That group opposes Iran’s conservative theocratic system of government. The list of suspects is long.

The disclosure of named individuals is unusual. Dookhtegan may be an insider or internal rival of these people.

Timing

Timing is one of the few facts that can be established definitively.

- We know when this leak was made.
- We know where it sits in the sequence of other Cyber Security events concerning Iran.
- We know the timeline of recent events in the Strait of Hormuz and the Iran nuclear deal.

The chances that this leak is unconnected with any of these events yet occurs at precisely this point in time, is I think unlikely. Why now?

Who Benefits?

- APT34’s domestic “competitors” may benefit, since APT34 may now have fewer assignments and its staff may be perceived as less competent.

- Those against greater Iranian influence in the region have additional evidence if any was needed, that Iran acts against commercial and state entities.

- Countries who may have otherwise adopted a more understanding approach to Iran may be expected explain to their citizens why they would continue that in the face of publicised, successful cyber attacks against their own government, companies, and national critical infrastructure by APT34.

- None of those whose data was divulged in the breach was undone in any significant way. Enough data was leaked to make the release credible, but not so much as to seriously wound APT34’s targets. There was no lasting economic harm and no serious negative 2nd order effects that we know of.

- If important organisations strengthen their Cyber Security in the wake of this leak, then they will be harder to compromise in the future. If Iran were to decide to strike at national critical infrastructure or important commercial assets, they might find those targets hardened or better prepared than before this leak.

Actions

Much is unknown. This blog is at least 3 entities removed from the source, or 4 if you count Iran as primogenitor. What actions should we take and what lessons can we learn?

- Are you a government or organisation running national critical infrastructure in a state that is *against* the expansion of Iran’s sphere of influence? You are a target for APT34 and groups like it.
- Are you a government or organisation running national critical infrastructure in a state that is *comfortable with* the expansion of Iran’s sphere of influence? You are *also* a target of APT34 and groups like it.

As of this moment, the APT34 leak includes data from government departments and infrastructure companies in the following sectors:

- Oil and gas
- Energy
- Ports and Airports
- Telecommunications
- Finance

If the threat models of these companies didn’t include adversaries like APT34 before, they surely must do now. It doesn’t matter if they are based in an aligned or unaligned country vis-à-vis the strategic goals of the Islamic Republic of Iran.

The most important lesson to be learned from this event is that your threat model can change rapidly with geopolitical developments. Either you can anticipate those changes and prepare for them, or you will have to adapt to them at a pace dictated to you by the attackers.