Cybersecurity Insights

Iran's cyber and military initiatives are shaking the Middle East

CWATCH

GEOPOLITICAL CONTEXT AND NEWS: REGIONAL LEADERSHIP, AN ALTERNATIVE TO THE WESTERN PARADIGM

Regional leadership, an alternative to the western paradigm

→ Iran is a key player in the region, both geographically and geopolitically. At the crossroads of several major powers, the country is a gateway at the centre of the Middle East. For years now, the Iranian government has been adopting a strategy of resistance to regional and "Western" powers as well as extending its own zone of influence. Up against Israel, Saudi Arabia, the United Arab Emirates, Turkey, Tehran hopes to offer an alternative to the region.

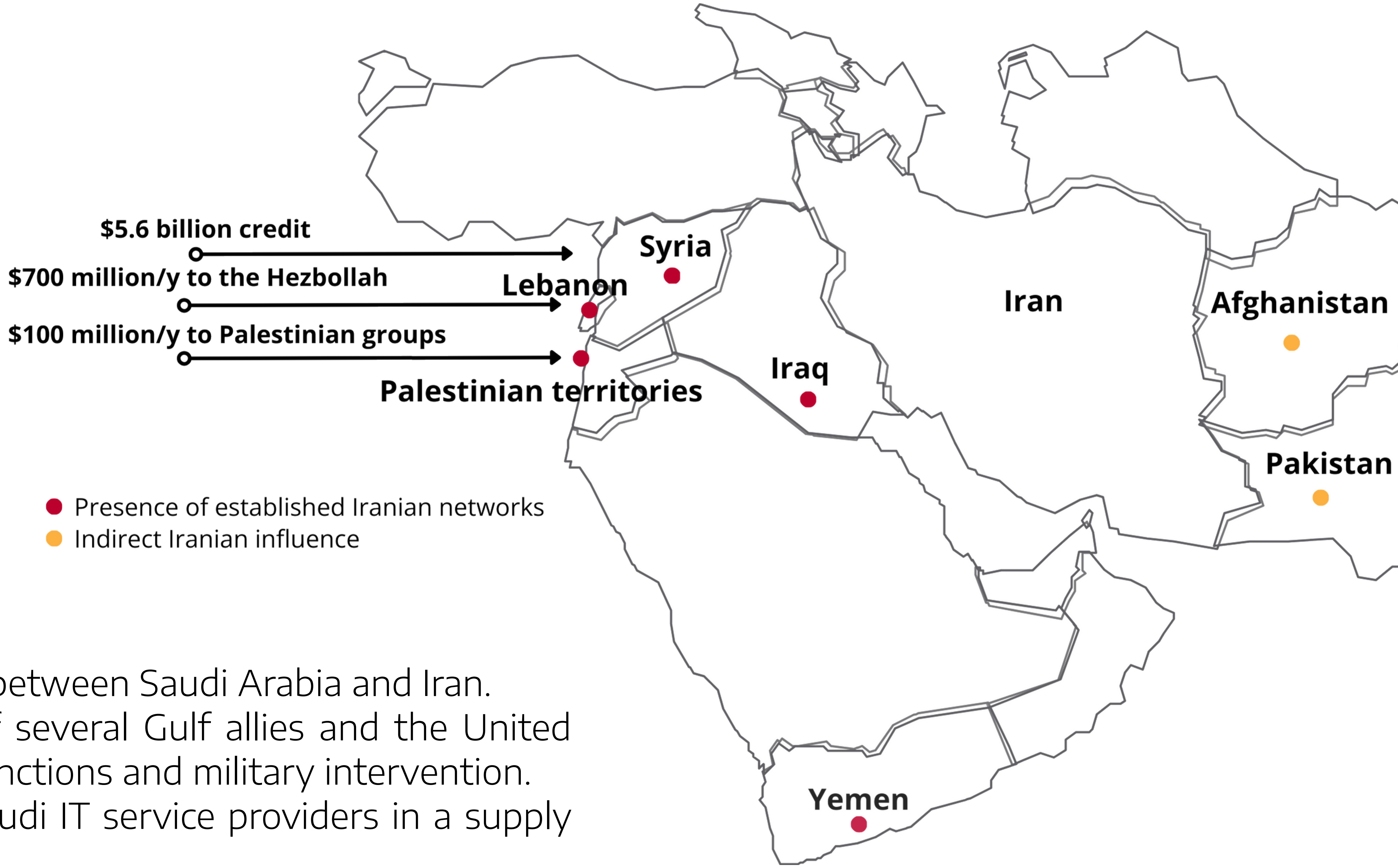
Reformer President Pezeshkian has yet to prove it can diminish diplomatic isolation (if it is his intention) in an organisation that don't allow much decision in foreign policy to the president. In the Iran government it's the Ayatollah that dictates the orientation outside of the country.

The paradigm shift in the United States, with the re-concentration of forces on other fronts, has enabled other regional powers to assert themselves and manage security, economic and energy issues.

GEOPOLITICAL CONTEXT AND NEWS:

PROXIES' STRATEGY: TEHRAN'S WEAVING ITS WEB

→ Iran has been supporting financially and with military resources multiple militias in the region like the **Hezbollah** and the **Hamas**, mostly aiming at Israel.
Since 2022, Iran's sponsored threat actors' ecosystem has been conducting multiscale influence operations. The **Storm-1084** (DEV1084) group led destructive cyberattacks and sent messages to encourage actions in response to Israel's policies towards Palestinians. The war in Yemen has been bogging down and has crystallised tensions between Saudi Arabia and Iran. Saudi Arabia has led a coalition made up of several Gulf allies and the United States to isolate Yemen through economic sanctions and military intervention.
In 2019, **Tortoiseshell** targeted nearly 11 Saudi IT service providers in a supply chain attack.


$5.6 billion credit
$700 million/y to the Hezbollah
$100 million/y to Palestinian groups
Syria
Lebanon
Palestinian territories
Iraq
Iran
Afghanistan
Pakistan
Yemen
● Presence of established Iranian networks
● Indirect Iranian influence

GEOPOLITICAL CONTEXT AND NEWS: NEW PARTNERSHIPS

→ For a time now, Tehran has been more than eyeing Russia and China as partners. Under severe economic and political sanctions from the international community (essentially meaning the North America and the European Union nations), they are seeking **strategic allies.**

2021

- A twenty-five-year Iran-China agreement centred around foreign investment in key sectors like oil.

2023

- China seized the diplomatic opportunity to act as a mediator in 2023 between Saudi Arabia and Iran for the signature of the normalisation agreement.
- The Islamic Republic of Iran officially joins the Shanghai Cooperation Organisation.

2024

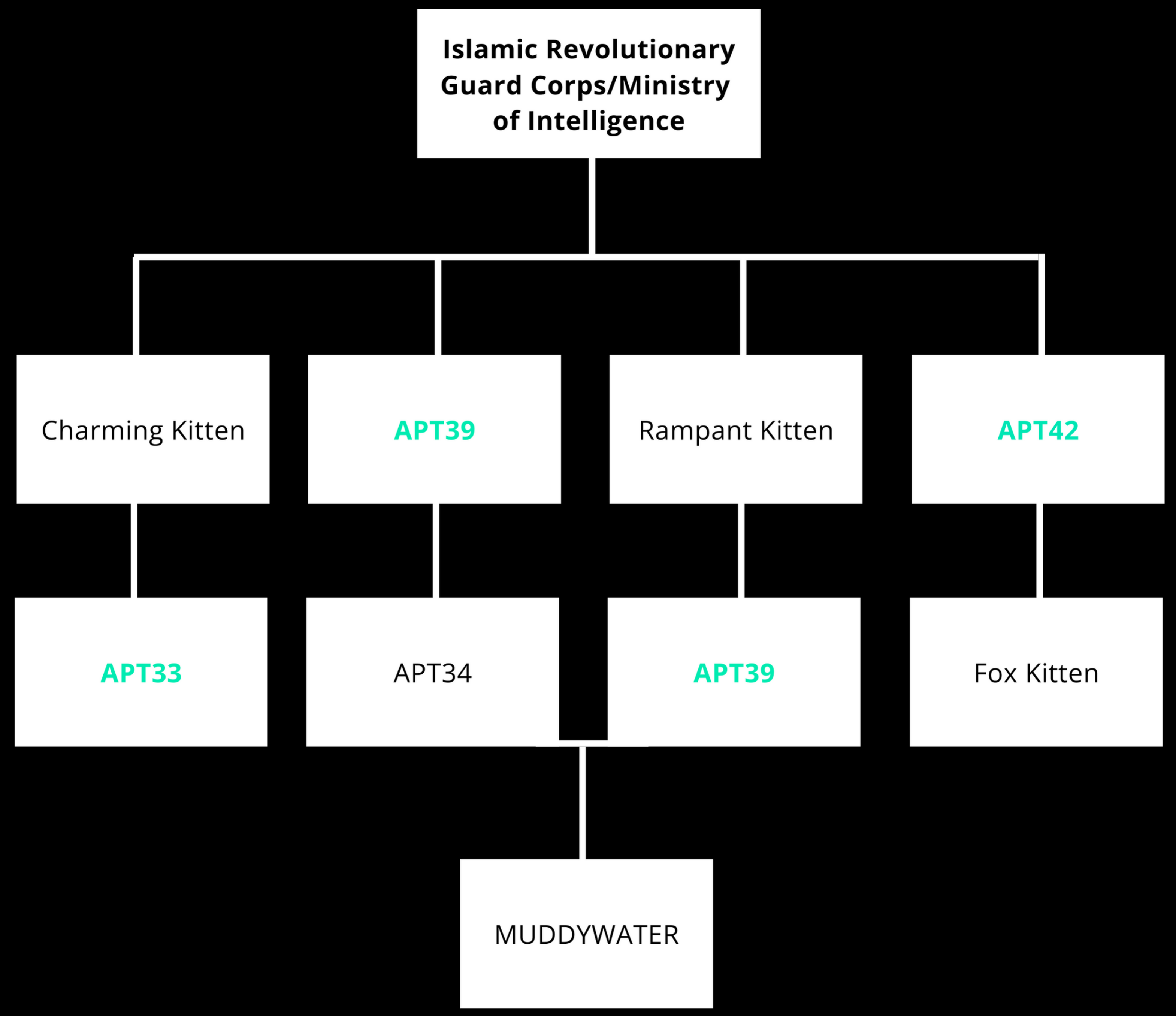
- One demonstration of these attempts to reach out to new allies is the alleged military support to Putin in the Ukrainian war denounced by Europe and the US. Even thought, Iran denies it, it's aligning with the current bilateral relation with Russia.

IRANIAN GROUPS AND CONNECTIONS WITH PROXIES

→ Tehran's position provides fertile ground for cyber threats, particularly cyber espionage. Among the threat actors are APTs associated with the Iranian government, which mainly target Middle Eastern countries and the US government, such as **APT34** and **APT42**.

There are three APT groups working under the command of the Iranian government, potentially collaborating with the Hamas. **MERCURY** (AKA MuddyWater, DarkBit, Agrius, BlackShadow) and **ShroudedSnooper** (AKA Storm-0861 Scarred Manticore) which were both attributed to Iran's Ministry of Intelligence and Security (MOIS). **Cobalt Sapling** (AKA Moses Staff, Abraham's Ax, Marigold, Sandstorm) is another group specialised in sabotage and destruction.

Finally, **Plaid rain** (AKA POLONIUM, Dark Caracal, Volatile Cedar, Tempting Cedar, Aqua Dev 1) and **Lebanese Cedar** (AKA Volatile Cedar, DeftTorero) are believed to be Lebanese APT groups maintaining close links to the MOIS and to the Hezbollah in the case of Plaid Rain.



TANGIBLE IMPACTS

If Iran is mostly targeting American companies and government bodies, its range of action goes far from beyond the United States companies and organisations from Europe and from the Middle East undergo espionage activities and cyber-operations to achieve the following objectives.

Identified objectives

Collection of data

Targeting of political opponents, journalists, researchers.

Retaliation

Attacks againts Israel are likely to escalate due to the targeting of Hezbollah in Lebanon.

Arrests, kidnappings and assassination attempts

The information collected can lead to the neutralization of individuals.

Espionage

Deployment of spyware like SpyNote.

Sabotage

Leverages cyber espionage and sabotage to advance Iran's geopolitical goals by inflicting damages and spreading fear.