Islamic Republic of Iran

January 2020

Chief of State:	Supreme Leader Ali Hoseini-Khamenei
Head of Government:	President Hasan Fereidun Rohani
Foreign Minister:	Mohammad Javad Zarif
Minister of ICT:	Mohammad-Javad Azari Jahromi
Minister of Intelligence:	Mahmoud Alavi
Current Political Party:	Moderation and Development Party
Political System:	Theocratic Republic
Executive Elections:	2021
Legislative elections:	21 February 2020
Major Religions:	Shia Muslim
Total Population:	83,024,745
Export Partners:	China 27.5%, India 15.1%, South Korea 11.4%, Turkey 11.1%, Italy 5.7%, Japan 5.3%
Major Exports:	Petroleum 60%, Chemical and Petrochemical Products, Fruits and nuts, Carpets, Cement, Ore
Import Partners:	UAE 29.8%, China 12.7%, Turkey 4.4%, South Korea 4%, Germany 4%[1]
Domestic tensions:	Civil protests
International Tensions:	International Sanctions; U.S. kills General Qasem Soleimani; JCPOA Agreement; proxy forces

Overview

International Relations

Foreign Policy for the Iranian government is influenced by a number of contentious issues; regional competition, proxy conflicts, nuclear enrichment, the petrochemical industry, a deep religious divide, and changing international power dynamics. Regional conflict and competition for influence across the Middle East is set against Israel and Saudi Arabia, but has a backdrop of other major global powers such as United States of America, Europe, Russia and China. The conflux of national security interests, which ranges from defense to economic and energy security, makes for a delicate foreign policy environment.

Iran's regional influence has been operationalized through the use of proxy military activity, information operations as well as offensive cyber activity. The military arena's in which power politics is playing out include the wars in Yemen, Syria and Iraq. Iran's international relations are also compounded by the

[1] CIA, "The World Factbook" accessed January 14 2020, published 2020, https://www.cia.gov/library/publications/the-world-factbook/geos/ir.html

interference and security requirements of other major global powers. The changing dynamics of the global economy and sentiment in the U.S. administration (for example), has contributed to the exclusion of Iran from the international economy through the use of economic sanctions. The withdrawal from the Joint Comprehensive Plan of Action (JCPOA), falls in line with current trends towards protectionist and less globally focused state behavior in the U.S. administration of President Donald Trump. Military strikes against Iranian targets within Iraq and Syria in late 2019 and early 2020 have intensified hostility in the region.

Overall Iran experiences cordial relations with South Caucasus and Central Asia, underpinned by a pragmatic outlook to not upset Moscow or Beijing. It sees Armenia as its "gateway to Europe" and Turkmenistan as its "gateway to Central Asia". Iran prioritizes relations from the Persian Gulf and Levant alongside Turkey.

National Security

Securing control of its internal political space is a top priority for the Iranian regime. The country has been cracking down on online content since 2009 after widespread protests during the Green Movement. The perceived ability to cause societal discontent through online communication channels, and generate conflict was also demonstrated by the Middle East in the aftermath of the Arab Spring in 2011. Since then, Iran has invested in internal internet governance and pursued a hard-line stance against perceived dissident or anti-revolutionary activity. The Islamic Revolutionary Guard Corps' (IRGC) website details some of the countries strategy in this area, and justifies its goals as helping to define parameters for "acceptable culture". The pursuit of internal control has led to the implementation of the National Information Network (NIN). This is based on ideas to monitor internet usage, and block subversive content, not unlike SORM of Russia and the "Great Chinese Firewall". The data captured by this national intranet can be accessed by the countries intelligence and law enforcement agencies. Freedom of expression is regularly reported as being restricted too. Iranian legislation makes many non-violent crimes punishable by death. Many ordinary users of social media have been brought to the IRGC or arrested for making comments on controversial issues (such as fashion). In 2016, Iran carried out the largest mass executions in years. Despite being considered a moderate, President Rouhani has been accused of not doing enough to counter the more hard-line actions of the judiciary or the IRGC.

In late 2019, widespread protest in over 100 locations across Iran led to a violent government crackdown according to Human Rights Watch. In November, there were reports that 1,000 people had been arrested and a number of deaths were reported. There has been significant disruption to internet availability and on November 19, connectivity was at 4 percent of its normal level. Critics and journalist have all been targeted.[2] Iran ranks 138 out of 180 countries for corruption[3], and has a status of "not fee" according to Freedom House when measuring civil and political rights.[4]

Economy

Iran is the second largest economy (after Saudi Arabia) in the Middle East and North African region (MENA), and has the second largest population after Egypt. The country relies heavily on oil revenues. Rigorous implementation of sanctions over the last several years have been hard hitting on the economy. Between 2011 and 2014 the currency took a nosedive as the Rial lost 80 percent of its value against the dollar. Iran has the second largest proven natural gas deposits globally, and could counter the impact of sanctions on oil, but foreign investments would be required. Due to the sanctions, many countries and companies have shied away from investing in Iran's gas deposits. Despite some gains under previous sanctions in the international community's eyes, present US leadership does not seem to articulate a very promising outlook. However, Europe, Russia, China and India have all voiced opposition to President Trump's unilateral stance. During 2016 Iran's economy experienced a notable recovery.

In 2017, Iran had a GDP of US $447.7 billion. The World Bank characterizes the Iranian economy to be dominated by the "hydrocarbon sector, agriculture and services sectors." By 2018 GDP growth fell to 3.8%.[5] Iran's economy is expected to slow even further (8.7%) between 2019/20 due to international fluctuations in the oil and gas sector, and the impact of current and new U.S. sanctions are imposed.[6]

[2] Human Rights Watch "Iran: Security Forces Violently Crack Down on Protesters" accessed January 14 2020, published November 19 2019, https://www.hrw.org/news/2019/11/19/iran-security-forces-violently-crack-down-protesters

[3] Transparency International, "Iran", accessed January 14 2020, published 2018, https://www.transparency.org/country/IRN

[4] Freedom House, "Iran" accessed January 14 2020, published 2019, https://freedomhouse.org/report/freedom-world/2019/iran

[5] The World Bank "Islamic Republic of Iran" accessed January 14 2020 published October 2018,, https://www.worldbank.org/en/country/iran/overview

[6] The World Bank "Iran's Economic Update — October 2019", accessed January 14 2020, published October 2019, https://www.worldbank.org/en/country/iran/publication/economic-update-october-2019

Iranian Intelligence and Cyber Services

The fast development of Iran's cyber capability has meant that a number of organizations have been either created or have developed their own subdivisions to carry out activity. The Supreme National Security Council under the auspices of the Supreme Leader Khamenei, seems to oversee all of the different intelligence services. The most prominent intelligence service seems to be the Ministry of Intelligence and Security (MOIS), which works in conduit with the Islamic Revolutionary Guard Corp's (IRGC) Quds-Force and intelligence unit.

Supreme National Security Council (SNSC)

Head:	Supreme Leader Ali Hoseini-Khamenei
President:	President Hassan Fereydoon Rouhani
Areas of Concern:	To "watch over the Islamic revolution and safeguard the Islamic Republic of Iran's national interests". To "coordinate political, intelligence, social, cultural, and economic activities".

Ministry of Intelligence and Security (MOIS)

Minister:	Seyyed Mahmoud Alavi
Headquarters:	Mehran, Tehran, Tehran Province, Iran
Type of Service:	Domestic intelligence service
Areas of Concern:	Intelligence collection and analysis, counter-intelligence, disinformation, works with Quds-Force, to identify anti-revolutionary forces, provides resources to proxy-groups (Hamas, Hezbollah etc)
Branches:	Counterintelligence Directorate, Oghab 2

Islamic Revolutionary Guard Corps (IRGC)

Chief Commander:	Maj. Gen. Hossein Salami
Areas of Concern:	Defending the regime, Military operations, HUMINT, SIGINT
Branches:	Land force, Navy, Airforce, Intelligence Unit, Quds-force (special forces), Basij (has cyberspace council)

Cyber Police (FATA)

Chief:	General Vahid Majid
Headquarters:	Police Headquarter, Attar street, Vanak Sq, Tehran, Iran
Type of Service:	Law enforcement
Areas of Concern:	Monitoring online activity including social media, combating fraud, working with international partners to combat organized crime.

Passive Defensive Organization & Cyber Defense Command

Commander:	Brigadier General Gholam-Reza Jalali
Parent Organisation:	General Staff of the Armed Forces, IRGC?

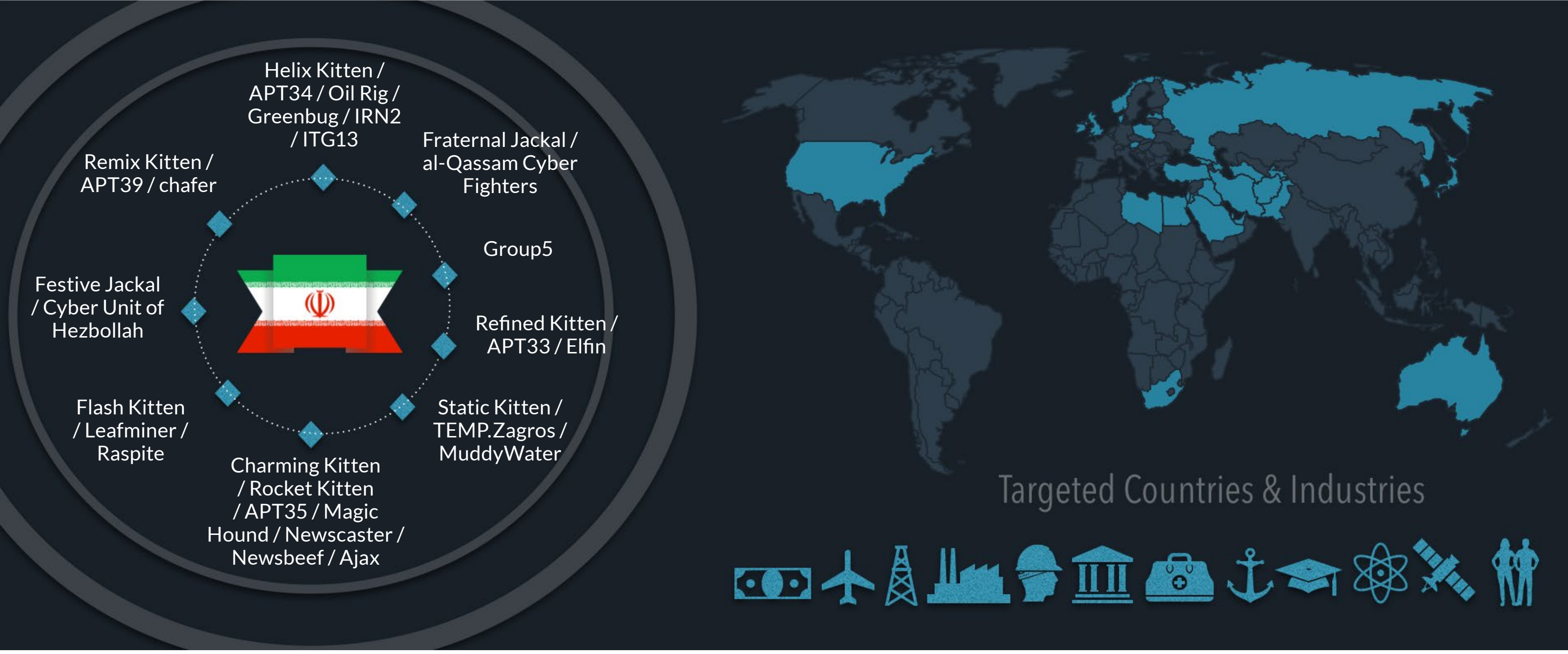

Helix Kitten / APT34 / Oil Rig / Greenbug / IRN2 / ITG13
Fraternal Jackal / al-Qassam Cyber Fighters
Group5
Refined Kitten / APT33 / Elfin
Static Kitten / TEMP.Zagros / MuddyWater
Charming Kitten / Rocket Kitten / APT35 / Magic Hound / Newscaster / Newsbeef / Ajax
Flash Kitten / Leafminer / Raspite
Festive Jackal / Cyber Unit of Hezbollah
Remix Kitten / APT39 / chafer
Targeted Countries & Industries

Figure 1: APTs & Threat Actors Backed By and Aligned With Iran

2015

ROCKET KITTEN: A CAMPAIGN WITH 9 LIVES

GROUP5 TARGETS SYRIAN OPPOSITION

2016

OILRIG ATTACKS ON SAUDI ARABIAN ORGANIZATIONS

U.S. INDICTS IRANIANS FOR HACKING MULTIPLE BANKS

SHAMOON 2.0

2017

OILRIG TARGETS IT & FINANCIALS IN UK, MIDDLE EAST AND TURKEY

MAGIC HOUND ESPIONAGE CAMPAIGN AGAINST SAUDI ARABIA

OILRIG DEVELOPS TOOLS – TARGETS GOVERNMENT ORGANIZATION IN MIDDLE EAST

CHARMING KITTEN TARGETS HUMAN RIGHTS, NGO'S, NEWS

2018

OILRIG TARGETS TECHNOLOGY SERVICE PROVIDER AND GOVERNMENT AGENCY

LEAFMINER ESPIONAGE TARGETS MIDDLE EAST GOVERNMENTS

APT33 BEHIND SHAMOON ATTACKS

2019

APT39 BEHIND THEFT OF PII

CHAFER ESPIONAGE CAMPAIGN AGAINST FOREIGN DIPLOMATS

APT33 TARGETS MULTIPLE ORGANIZATIONS IN SAUDI AND USA

APT34 TARGETS ENERGY, OIL & GAS AND GOVERNMENTS

APT35 DOMAINS SHUT DOWN BY MICROSOFT

APT35 LINKED TO ACTIVITY TARGETING PRESIDENT TRUMPS 2020 CAMPAIGN

WIPER MALWARE ZEROCLEARE TARGETS ENERGY IN MIDDLE EAST

2020

Iranian Cyber Activity: The Race for Arms

In 2009, a Western backed cyber attack using the Stuxnet worm crippled nuclear centrifuges at the Natanz nuclear facility in Iran. Since then, Iranian cyber capability has evolved measurably. Many of the attacks detailed in vendor reports between 2009 and 2013 reflect an initial demonstration of low level hactivist style campaigns such as defacements and denial of service attacks. Iranian actors in cohort with other like-minded actors or groups perpetrating attacks as part of #OpIsrael or #OpUSA. The Iranian Cyber Army hacked Twitter in 2009, and the Chinese search engine Baidu in 2010 with defacements. At the same time an important step was made in the creation and development of the first Iranian forum "Ashiyaneh" which drew in talent and interested parties. These behaviors reflect the need to connect with potential recruits and sustain a recognizable foundation for future capability.

The connections between the Iranian government and these initial demonstrations of capability remain somewhat murky, however, a 2011 EU sanctions list details the owner of the Ashiyaneh forum "Behrouz Kamalian" because of connections to a 2009 IRGC cyber crackdown on rioters. Behrouz Kamalian later claims to have been a member of the FATA Police.[7] During 2012, a group called Parastoo leaked information from the International Atomic Energy Agency (IAEA), among other targets[8], demanding the agency investigate nuclear facilities in Israel, in particular the Dimona site[9]. Between 2012 and 2013, the group, called Qassam Cyber Fighters (Izz ad-Din al-Qassam Cyber Fighters), conducted Operation Ababil, in which numerous Distributed-Denial-of-Service (DDoS) attacks were aimed at financial services organizations in the United States. These DDoS attacks were orchestrated because of a video that insulted the Prophet Muhammed. Reviewing the groups pastebin post reveals a successful attempt to get YouTube to remove the video after which the group suspended its attacks. The name "Izz ad-Din al-Qassam" relates to a prominent Palestinian muslim teacher, and is also the name of a Palestinian Hamas wing [10]. In 2013 another group name "Islamic Cyber Resistance", which Recorded Future reports to have links to Iran, claims to have worked with the Syrian Electronic Army[11]. In 2012, the first Shamoon attack is aimed at Saudi Aramco, using a sophisticated wiper. Cutting Sword of Justice claimed responsibility (later linked to APT33).

The first vendor report to highlight a dramatic shift in capability is in Operation Saffron Rose by FireEye. It highlights that the activity (now attributed to a group name "Ajax Security Team") from Iranian actors is now showing evidence of malware in its attacks. The campaign took advantage of social media, emails, and spoof sites designed for credential harvesting to socially engineer victims. The campaign heavily targeted the U.S. defense industrial base[12]. In 2014, Cylance detected Operation Cleaver. Researchers point out a particular focus on Iranian interests, but also critical infrastructure in South Korea. The researchers consider the possibility that Iran and North Korea may have been collaborating due to a technology cooperation agreement for efforts like IT and Security.[13]

Despite the leap in capability, in 2015 a collection of reports tracking "Rocket Kitten" from CheckPoint, TrendMicro and ClearSky analysts provided evidence of further domestic and international espionage campaigns. Poor operational security, exposing details of victims due to an unsecured database and a publicly used alias "Wool3n.H4t" suggested that Iran was still climbing the offensive cyber maturity ladder[14]. Surveillance of Iranian and foreign targets was also attributed Chafer and Cadelle in 2015[15]. Trend Micro's "Operation Woolen-Goldfish" report provides examples of how the

[7] Article 19, "Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran ", accessed January 14 2020, published 2017, https://www.article19.org/data/files/medialibrary/38619/Iran_report_part_2-FINAL.pdf

[8] Parastoo, "#Parastoo #IAEA #OpIsrael #Anonymous", accessed January 14 2020, published November 29 2012, https://pastebin.com/s96K4D6j

[9] Parastoo, "Parastoo - 1", accessed January 14 2020, published November 25 2012, https://pastebin.com/SdYaPUwr

[10] QassamCyberFighters, "QassamCyberFighters's Pastebin", Pastebin, accessed January 14 2020, published September 18 2012, https://pastebin.com/u/QassamCyberFighters.

[11] Chris, "'Islamic Cyber Resistance' Breaks Iranian Hacker Silence, Exposes Links to SEA", Recorded Future, accessed January 14 2020, published December 24 2013, https://www.recordedfuture.com/islamic-cyber-resistance-activity/

[12] Nart Villeneuve, Ned Moran, Thoufique Haq and Mike Scott, "Operation Saffron Rose", FireEye, accessed January 14 2020, published 2013, https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-operation-saffron-rose.pdf

[13] Cylance, "Operation Cleaver", accessed January 14 2020, published 2012, https://www.cylance.com/content/dam/cylance/pages/operation-cleaver/Cylance_Operation_Cleaver_Report.pdf

[14] CheckPoint, "Rocket Kitten: A Campaign with 9 Lives", accessed January 14 2020, published November 2015, https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf

[15] Symantec Security Response, "Iran-based attackers use back door threats to spy on Middle Eastern targets", Symantec,

GHOLE malware used by Rocket Kitten is a modified "Core Impact" product[16], which is a legitimate pentesting program and highlights capability dependency and lack of maturity. During 2015 the Yemen Cyber Army was also established.[17]

In 2016 a Pastebin post shows that the Parastoo group claims to have worked with a number of other hacking groups to attack the power grid in Turkey, successfully shutting it down to warn Turkey of its support for ISIS[18]. In November 2016, fresh variants of Shamoon (Shamoon 2.0) were spotted targeting Saudi Arabian companies.[19] In 2017 and early 2018, a number of Iranian hackers were charged with U.S. indictments for cyber espionage. Some of these hackers were associated with the Mabna Institute and the Turk Black Hat security team.[20] In late 2017 ClearSky researchers published a detailed report on Charming Kitten (the evolved Parastoo ad Ajax team and APT35) in which the actors are found to be targeting human rights activists, academic researchers and media outlets.[21] By 2018, FireEye had been reporting on three distinct APT groups: APT33, APT34 and APT35. APT33 in particular has been attributed to the destructive Shamoon malware.[22]

In 2019 FireEye also identified APT39. Its particular goals seem to be the widespread theft of information from the telecommunications and travel industries.[23] A number of fake social media profiles used for information operations were attributed to Iran, which were taken down later in the year. The UK NCSC also discovered that Russian group Turla had exploited Iranian infrastructure to hide its activities.[24] APT35 was attributed to activity targeting the 2020 U.S. elections.[25]

In 2019, there were also a number of leaks that exposed the toolset of APT34/ Helix Kitten, and the reach of the Iranian intelligence network in Iraq. Likened to the Shadow Brokers leak on the National Security Agency (NSA) of the U.S., an individual under the alias "Lab Dookhtegan" sent links to the information to various reporters and researchers throughout March and April. Source code of six hacking tools were exposed in the leaks:

- BondUpdater
- PoisonFrog
- HyperShell
- HighShell
- Fox Panel
- Webmask

Victim information was also exposed. Sixty-six victims globally were exposed alongside personal information of the officers involved in APT34 operations. The officers were linked to the Iranian Ministry of Intelligence.[26] Following a rise in tensions during the Summer of 2019, and the exchange in maritime security issues including the seizure of Iranian and British oil tankers, The Iran Cables were reported in The Intercept in November 2019. The Intercept assessed a number of confidentially sourced files described as an "unprecedented leak". The leaked documents include an expose of Iran's vast influence in Iraq. These documents describe an efficient

accessed January 14 2020, published December 7 2015, https://paper.seebug.org/papers/APT/APT_CyberCriminal_Campagin/2015/2015.12.07.Iran-based/iran-based-attackers-use-back-door-threats-spy-middle-eastern-targets.pdf

[16] Cedric Pernet and Kenney Lu, "Operation Woolen-Goldphish; When Kittens Go Phishing", Trend Micro, accessed January 14 2020, published 2015, https://www.trendmicro.com.ru/media/wp/operation-woolen-goldfish-whitepaper-en.pdf

[17] Fars News Agency, "Saudileaks 1: Yemeni Group Hacks Saudi Gov't, Releases Thousands of Top Secret Documents", accessed January 14 2020published May 21 2015,, https://en.farsnews.com/newstext.aspx?nn=13940231000544

[18] Parastoo, Parastoo RU, Sobh[.]info, "Untitled" Pastebin, accessed January 14 2020, published April 1 2016, https://pastebin.com/A9rg2Agp

[19] Jack Caravelli & Sebastian Maier, "Deciphering Iran's Cyber Activities", King Faisal Center for Research and Islamic Studies, accessed January 14 2020, published December 2016, http://www.kfcris.com/pdf/27b74972d7db3c7547badfbf7f9ddbd158c-8e256cd743.pdf

[20] NCSC, "Foreign Economic Espionage in Cyberspace", DNI, accessed 14 January 2020, published 2018, "https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf"

[21] ClearSky, "Charming Kitten; Iranian cyber espionage against human rights activists, academic researchers and media outlets - and the HBO hacker connection" ClearSky Cyber Security, accessed January 14 2020, published December 2017, https://www.clearskysec.com/wp-content/uploads/2017/12/Charming_Kitten_2017.pdf

[22] FireEye, "M-Trends 2018", accessed January 14 2020, published 2018, https://investors.fireeye.com/static-files/b7dcb16f-44a8-4cfb-927f-efeed397dd52

[23] Sarah Hawley, Ben Read, Cristiana Brafman-Kittner, Nalani Fraser, Andrew Thompson, Yuri Rozhansky, Sanaz Yashar "APT39: An Iranian Cyber Espionage Group Focused on Personal Information" accessed January 14 2020, published January 29 2019, https://www.fireeye.com/blog/threat-research/2019/01/apt39-iranian-cyber-espionage-group-focused-on-personal-information.html

[24] Insikt Group, "Operation Gamework: Infrastructure Overlaps Found Between BlueAlpha and Iranian APTs", Recorded Future, accessed January 14 2020, published December 2019, https://go.recordedfuture.com/hubfs/reports/cta-2019-1212.pdf

[25] CERT-EU, "Iran's APT35 targeting individuals tied to US 2020 elections" accessed January 14 2020, published October 9th 2019, https://media.cert.europa.eu/static/MEMO/2019/TLP-WHITE-CERT-EU-MEMO-191009-1.pdf.

[26] Caitlin Cimpanu, "Source code of Iranian cyber-espionage tools leaked on Telegram" ZDNet, accessed January 15 2020, published April 17 2019, https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/

human-intelligence network. It often reported back sensitive details about the U.S. diplomatic meetings to Iran. The report provides a damning look at a central influential figure, namely the late General Qassem Soleimani.[27] These leaks reflect the level of maturity in the Iranian intelligence apparatus, highlighting Iranian geopolitical requirements for its borders as well as some of its cyber capability. The impact of this exposure has likely harmed Iran's ability to operate as effectively as they will be better detected and they appear to have been compromised. IBM analysts, later confirmed by Saudi Arabia's National Cyber Security Authority, reported on a new destructive malware called ZeroCleare.[28]

The climate entering into 2020 has become more tense as the same figure that The Intercept pointed out as being central to the Iranian intelligence network in Iraq, was killed in a drone strike in Baghdad airport. It should come as no surprise that an individual capable of acting against the interests of the U.S. is on a target list. The inevitable consequences of such an act by the U.S. are somewhat daunting. The act was taken on foreign territory, in a proxy location, that of Iraq. The target was considered a pillar of Iran's foreign operations. This raised the questions, was this an act of war and how did the U.S. predict that Iran would behave afterwards? The current escalation in activity is a Persian-Gulf conflict and reflecting on the 2019 – 2020 incidents shows a hybrid of activity including cyber attacks. On January 4, the U.S. Department of Homeland Security (DHS) issued a temporary National Terrorism Advisory Bulletin detailing possible threats against the U.S. The bulletin advised that Iran may target the U.S. through disruptive cyber attacks, homegrown terrorism, and proxy activity through actors like Hezbollah. Although it states there is no information indicating a specific or credible threat.[29]

Iranian Objectives and Targeting

Iran often aligns its cyberattacks to support its national interests. Iran is likely to use espionage campaigns against Iranian civilians and dissidents where and when it observes anti-revolutionary sentiment. To maintain security at its borders, Iran may target regional neighbors as well. Disruptive attacks are likely where and when Iran is dealing with a provocative adversary. Iranian adversaries include those countries that act against national ambitions, such as the U.S., for its role in excluding Iran from the international system. The U.S., Saudi Arabia, Bahrain, and Israel are currently the most prominent state adversaries. Iran has demonstrated a tendency to target financial systems in retaliation due to the symbolic importance this sector has for Western culture. Iran has also shown concerted efforts to use destructive wiper malware against regional rivalries. For example, the Shamoon attacks against Saudi Arabia.

Persian-Gulf Conflict 2019 - 2020

Over the course of 2019 there was a marked escalation in tension, including direct confrontation, between Iran and the U.S. and its allies. This escalation consists of hybrid attacks, including information operations, maritime operations, offensive cyber attacks, and kinetic military strikes. Military strikes have killed targets on both sides, although Iran has suffered the most casualties. The elimination of General Qasem Soleimani by the U.S. via a drone strike is an example of a critical incident that some experts say has further deteriorated relations.

The nature of the activities and interactions appear to be retaliation, and like-for-like actions taken by each respective side. Some experts have said the strike against the general was stark and heavy-handed by comparison, others have called it justified. Iran's retaliatory strike did not appear to have been orchestrated to kill. The U.S. has stated that it will apply further sanctions on Iran and its economy.

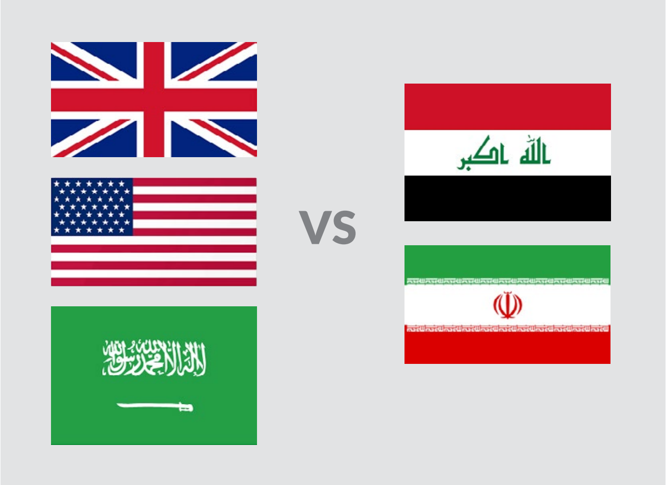
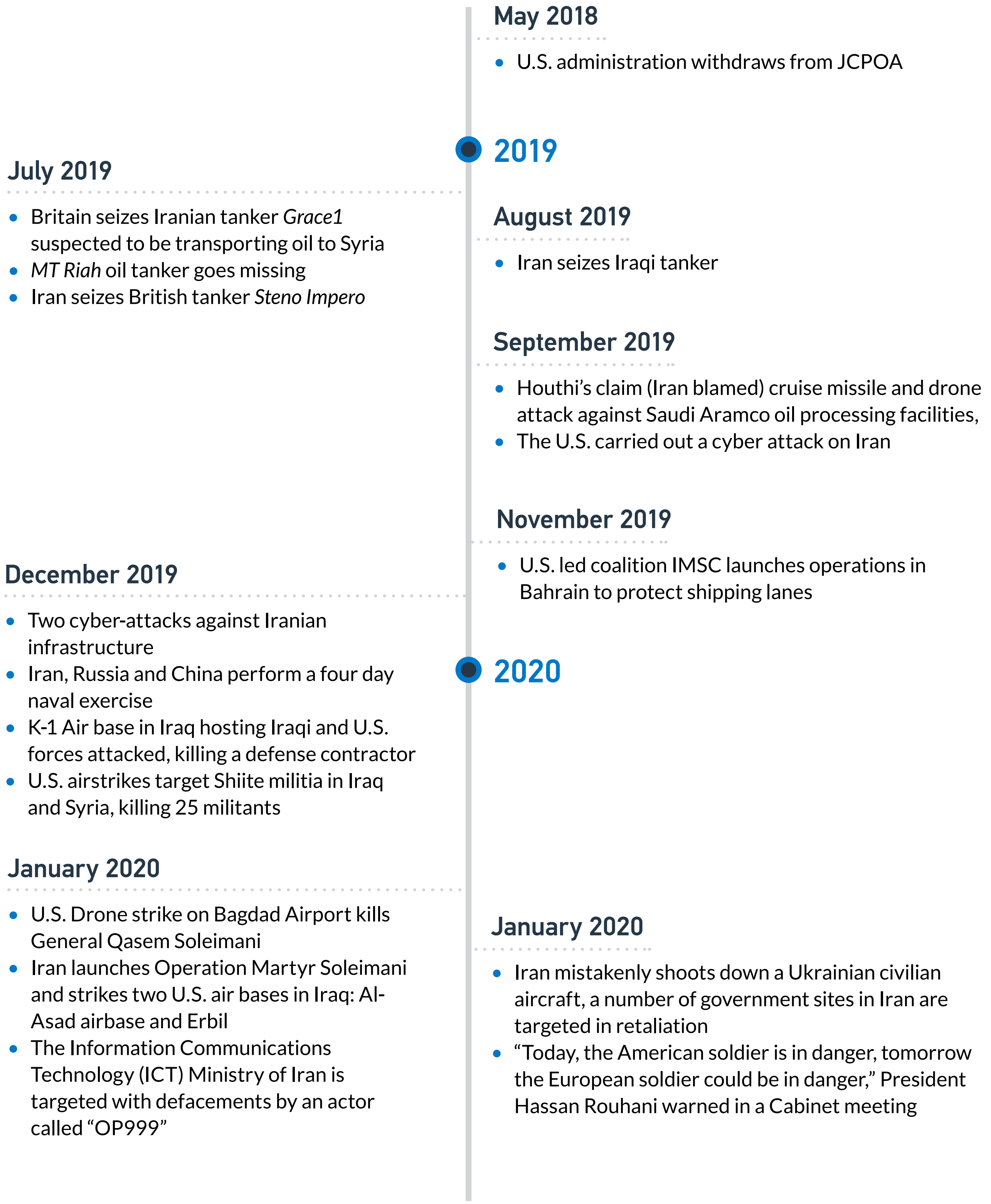


Figure 2: Adversaries in the Persian-Gulf Conflict

[27] James Risen, Tim Arango, Farnaz Fassihi, Murtaza Hussain, Ronen Bergman, "A Spy Complex Revealed", The Intercept, accessed January 15 2020, published November 18, 2019, https://theintercept.com/2019/11/18/iran-iraq-spy-cables/

[28] DHS, "National Terrorism Advisory System; Bulletin", accessed January 15th 2020, published January 4th 2020, https://www.dhs.gov/sites/default/files/ntas/alerts/20_0104_ntas_bulletin.pdf

[29] IBM Security "New Destructive Wiper "ZeroCleare" Targets Energy Sector in the Middle East", published December 2019, accessed January 15 2020, https://www.ibm.com/downloads/cas/OAJ4VZNJ



May 2018

- U.S. administration withdraws from JCPOA

2019

July 2019

- Britain seizes Iranian tanker *Grace1* suspected to be transporting oil to Syria
- *MT Riah* oil tanker goes missing
- Iran seizes British tanker *Steno Impero*

August 2019

- Iran seizes Iraqi tanker

September 2019

- Houthi's claim (Iran blamed) cruise missile and drone attack against Saudi Aramco oil processing facilities,
- The U.S. carried out a cyber attack on Iran

November 2019

- U.S. led coalition IMSC launches operations in Bahrain to protect shipping lanes

December 2019

- Two cyber-attacks against Iranian infrastructure
- Iran, Russia and China perform a four day naval exercise
- K-1 Air base in Iraq hosting Iraqi and U.S. forces attacked, killing a defense contractor
- U.S. airstrikes target Shiite militia in Iraq and Syria, killing 25 militants

2020

January 2020

- U.S. Drone strike on Bagdad Airport kills General Qasem Soleimani
- Iran launches Operation Martyr Soleimani and strikes two U.S. air bases in Iraq: Al-Asad airbase and Erbil
- The Information Communications Technology (ICT) Ministry of Iran is targeted with defacements by an actor called "OP999"

January 2020

- Iran mistakenly shoots down a Ukrainian civilian aircraft, a number of government sites in Iran are targeted in retaliation
- "Today, the American soldier is in danger, tomorrow the European soldier could be in danger," President Hassan Rouhani warned in a Cabinet meeting

Figure 3: Timeline of the Persian-Gulf Conflict

Jan. 3, 2020

General Qassem Soleimani killed by a drone strike at Baghdad airport.

Jan. 3, 2020

Jan. 3, 2020: the group shield_iran created a new Telegram channel via @shield_iran and an Instagram account at shield_iran.

Jan. 3, 2020

The campaign dubbed "Iranian Hackers" consisting of several well-known Pro-Iranian hacktivist and cybercrime groups have cooperated to deface U.S. websites following the death of Soleimani. The groups shared defacements on Telegram and

Jan. 7, 2020

Personal information was posted on the Telegram channel for the administrator of the Saudia airline website saudia.com, which included an email address, a password and a phone number.

Jan. 9, 2020

Personal information was posted on the Telegram channel for the administrator of the website of the Dubai, United Arab Emirates-based airline Emirates, which included an email address, a password and a phone number.

Jan. 9, 2020

Personal information was posted on the Telegram channel for the administrator of the U.S-based news website pravasi.us, which included an email address and password.

Jan. 10, 2020

A defacement made on website of the Sacramento, California, U.S.-based electrical contractor Vasko at vasko.com

Jan. 11, 2020

An offer was posted on @Liosion_posts to sell a leaked database from the web design site infowick.com for US $50 and there was a report of a cross-site scripting (XSS) vulnerability at the Arabian Gulf Cup soccer tournament website at gulfcup.sa in Saudi Arabia

Jan. 12, 2020

Cyber attack against the website of the Ministry of ICT of Iran. The defacement of 28 sub-domains of ict.gov.ir was documented on Zone-H defacement archive under the handle OP999

Handles displaying activity defending Iran:

- EbRaHiM-VaKeR,Mr-b3hz4d, MR_Liosion
- Sir_Max
- H43ER
- T4arik[J3N]
- NikbinHK
- ImanGorji
- Perilous Man
- BigNorouzi
- My-error
- N3TC4T
- Alihack051
- Msamiee071
- Ro0t_ahor4
- B4B4K-KH4TaR
- G0dfather
- Milad Hacking
- Ahor4
- JavidH373
- Ali Afee

Groups:

- Liosion Team
- Iran Security Group
- Storm Security Team
- IranonymousTm
- shield_iran
- Bax 026 Of Iran
- Alfa Team
- RMX Team

Handles displaying activity against Iran:

- OP999
- NI9
- cR0X
- T-117
- Want3d

Channels displaying activity defending Iran:

- Spad Security | گروه امنیتی اسپاد
- Liosion_Team
- Bax 026 Of Iran
- RMX team

Channels displaying activity against Iran:

- لب دوختگان | Lab Dookhtegan | Read My Lips
- پشت پرده - Poshteh Pardeh
- ASHRAR | اشرارتیم
- Revealer
- BLACK BOX

Iran 2020: Calendar of Events of Strategic and Cultural Importance

Jan	9	UN Security Council Meeting
	29	Martyrdom of Fatima
Feb	11	UN Security Council Meeting
	21	Martyrdom of Fatima
Mar	8	Birthday of Imam Ali
	20	March Equinox
	20–23	Norooz Holiday (Persian New Year)
	22	Prophet’s Ascension
Apr	9	Imam Mahdi’s Birthday
	24	Ramadan
May	14	Martyrdom of Imam Ali
	24	Eid-e-Fetr (End of Ramadan)
	24	Eid-e-Fetr (Additional Holiday)
Jun	17	Martyrdom of Imam Sadeq
	21	June Solstice
Jul	31	Eid-e-Ghorban (Feast of Sacrifice)
Aug	8	Eid-e-Ghadir
	28	Tassoua
	29	Ashura
Sep	22	September Equinox
Oct	8	Arbaeen
	16	Demise of Prophet Muhammad and Martyrdom of Imam Hassan
	17	Martyrdom of Imam Reza
	25	Martyrdom of Imam Hasan al-Askari
Nov	31	Birthday of Prophet Muhammad and Imam Sadeq
Dec	21	December Solstice

Future Concerns

Iraq

Iran has demonstrated a long term, vested interest in being able to influence its neighbor, Iraq. Leaked cables reported on by the Intercept highlighted the late General Qassem Soleimani’s vast network of spies and influence in the region. It is highly likely that Iraq will continue to serve as a necessary area for Iran to want to monitor and influence. Despite the Iranian human intelligence network being good, it is likely that cyber espionage campaigns may become a part of its widespread efforts to maintain security on its borders.

Israel

The creation of the state of Israel, and expansion of settlements, is a historic wound and reminder of Western interference in the region. Israel is also attributed to the deployment of the Stuxnet virus in 2009 alongside the U.S. It is highly likely that Israel will continue to feature as an adversary to Iranian interests in the region. Both espionage and disruptive attacks are likely.

United States

The United States has, alongside Israel, been a long term adversary of Iranian interests. There were hopes with the creation of the JCPOA agreement that this might change, but relations between the countries have only become more hostile. The withdrawal from the agreement has led to a further escalation in tensions culminating in missile strikes in late December 2019 and early January 2020. Iran's retaliatory tactics in the past make it highly likely that it will target the U.S. with like-for-like attacks.

United Kingdom and Europe

Although the U.K. is not responsible for the U.S. withdrawal from the JCPOA, it has been party to the seizure of Iranian tankers in the Mediterranean. The escalation in tensions will likely still influence U.K. and Iranian relations, especially if the U.K. is seen to be participating in the U.S. campaigns. If the U.K. becomes more actively involved then it is highly likely Iran will retaliate in a like-for-like manner. Iranian President Hassan Rouhani declared in early January that "U.S. troops are 'insecure' in the region today, and EU troops 'might be in danger tomorrow.'"

Saudi Arabia

The relationship between Riyadh and Tehran has been tenuous and complex at best. The two regional powers are usually discussed in context of their ideologically opposed religious affiliation, Saudi Arabia has majority Sunni population whilst Iran is Shia. Regional competition and ideological conflict between Iran and Saudi Arabia has created long-term difficulties in relations. It is highly likely that Iran will continue to use disruptive, destructive and espionage cyber campaigns against Saudi Arabia.

Bahrain

Bahrain is an ally of Saudi Arabia and has supported the U.S. sanctions against Iran. Iran supports military groups in Bahrain to disrupt local government and impose pressure. It is likely that Iran will target Bahrain with cyber espionage campaigns.