# Islamic Republic of Iran

October 2017

**Chief of State:** Supreme Leader Ali Hoseini-Khamenei

**Government:** Theocratic Republic

**Capital:** Tehran

**National Holiday:** 1st April[1]

**GDP by sector:** Agriculture (9.1%), Industry (39.9%), Services (51%)

**Export Partners:** China (22.4%), India (8.7%), Turkey (8.5%), Japan (4.5%)

**Import Partners:** UAE (39.5%), China (22.3%), South Korea (4.7%), Turkey (4.6%)

**Top Exports:** Petroleum (80%), Chemical and petrochemicals, fruit and nuts, carpets, cement, ore[2]

**Conflict areas:** Syria, Iraq, Yemen, Israeli occupation of Palestine, US interference, Saudi Arabian influence

**Major Religions:** Muslim (99.4%) — Shia (90–95%), Sunni (5–10%), other (Zoroastrian, Jewish and Christian)[3]

## Current Landscape

### International Relations

Iran's foreign policy with its neighbours and globally is entrenched in a number of issues. One that it is dominated by the petrochemical industry, nuclear enrichment, an ideological framework, regional turmoil and relative isolation[4]. Since the fall of the Soviet Union and the increased presence of US troops in the region, it has had to handle perceived existential threat from the US and its allies and a unique set of regional influences[5]. Overall Iran experiences cordial relations with South Caucasus and Central Asia, underpinned by a pragmatic outlook that does not want to upset Moscow or Beijing. It sees Armenia as its "gateway to Europe" and Turkmenistan as its "gateway to Central Asia". Iran prioritises relations from the Persian Gulf and Levant alongside Turkey. It sees Israel and Saudi Arabia as threats to its existence and its future as the dominant regional power. Iran's nuclear ambitions have been the cause for ongoing international sanctions against its financial, petrochemical, transportation and shipping sectors. Reports surrounding their enrichment program suggest the country is a long way off equipping missiles with nuclear warheads and that for the most part they have an abundance of conventional missiles[6]. However, the goal to become a nuclear power is in alignment with its regional ambitions to have better US deterrence and more regional political leverage. The Joint Comprehensive Plan of Action (JCPOA), set forth requirements for Iran to halt its uranium enrichment, and make efforts to alter regional activities, including supporting proxy groups and terrorist organisations, for some sanctions relief. The US Trump administration has adopted an oppositional outlook towards Tehran once again however, as evidenced by changing their position on the JCPOA.

### Internal security posture

Securing control of its internal political space is a top priority for the Iranian regime. The ability to cause societal discontent through online communication channels, and generate conflict was felt keenly 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 country's

1. A public holiday celebrating the establishment of the Islamic Republic in 1979
2. https://www.cia.gov/library/publications/the-world-factbook/geos/ir.html
6. https://www.cia.gov/library/publications/the-world-factbook/geos/ir.html
4. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170421_Farhi_Iranian_Power_Projection.pdf
5. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160420_Milani_IranReconnectingEurasia_Web.pdf
6. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/141218_Cordesman_IranRocketMissileForces_Web.pdf





ANOMALI®

strategy in this area, and justifies its goals as helping to define parameters for "acceptable culture"[7]. 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 country's intelligence and law enforcement agencies[8]. Freedom of expression is regularly reported as being restricted as well. 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)[9]. 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[10].

### 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[11]. 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% of its value against the dollar[12]. Iran has the second largest proven natural gas deposits globally, and could counter the impact of sanctions on oil, but it requires foreign investment. 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 Trump's unilateral stance. During 2016 the economy experienced a notable recovery.

## National Cyber-Strategy

Iran's attention was drawn to the development of its own offensive and defensive cyber capability after being attacked by the Stuxnet virus, followed by Duqu and Flame. The government pledged $1 billion investment in 2011[13], creating the Supreme Council of Cyberspace (SCC), Cyber Headquarters (under the Armed Forces General Staff), Cyber Command, the Basij cyberspace council, Cyber Police FETA and began recruiting talent into the industry. ICT ministries cooperated with the AFGS Cyber Headquarters to monitor vulnerabilities and threats to infrastructure. The SCC works with the National Center of Cyberspace under the direction of President Hassan Rouhani and Secretary Abolhassan Firouzabadi, coordinating and implementing cyberspace policy in Iran[14]. The MAHER/ Iran National CERT is responsible for incident response[15]. Since Stuxnet, Iran has matured into one of the more advanced actors globally, not afraid of being offensively oriented.

## Iranian Intelligence and Cyber Services

The fast development of Iran's cyber capability has meant that a number of organisations 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"[16] |

7. https://www.aei.org/publication/iran-comprehensive-legal-system-for-internet-and-cyberspace/
8. https://www.iranhumanrights.org/2016/10/ten-things-you-should-know-about-irans-national-internet-project/
9. https://www.hrw.org/world-report/2017/country-chapters/iran
10. https://freedomhouse.org/report/freedom-world/2017/iran
11. http://www.worldbank.org/en/country/iran/overview
12. https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/140122_Cordesman_IranSanctions_Web.pdf
13. https://www.files.ethz.ch/isn/154842/No375_15OCT2012.pdf
14. http://techrasa.com/2017/08/27/all-you-need-know-about-internet-censorship-iran/
15. https://www.files.ethz.ch/isn/154842/No375_15OCT2012.pdf
16. http://www.iranonline.com/iran/iran-info/government/Supreme-National-Security-Council.html

## Ministry of Intelligence and Security


**Minister:** Seyyed Mahmoud Alavi[17]
**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 antirevolutionary forces, provides resources to proxy-groups (Hamas, Hezbollah etc.) [18]
**Branches:** Counterintelligence Directorate, Oghab 2

## Islamic Revolutionary Guard Corps (IRGC)


**Chief Commander:** Maj. Gen. Mohammad Ali Jafari[19]
**Areas of Concern:** Defending the regime, Military operations, HUMINT, SIGINT[20]
**Branches:** Land force, Navy, Airforce, Intelligence Unit, Quds-force (special forces), Basij (has cyberspace council[21])[22]
**Associated Groups:** Iran Cyber Army (ICA)[23]/ Iran cybersecurity division[24 25 26], Ashiyane Digital Secuirty Team[27 28], Hizbullah Cyber Army, Qassam Cyber Fighters, Virtual Anonymous Jihad[29], APT33?[30], Rocket Kitten? [31 32]
**Campaigns:** Operation Cleaver, Shamoon, Operation Ababil, Saffron Rose, Newscaster, Diginotar, Comodo[33], Operation Wilted Tulip[34]

## Cyber Police FATA


**Chief:** Seyyed Kamal Hadianfar
**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 [35]
**Parent Organisation:** General Staff of the Armed Forces[36], IRGC?[37]

17. vaja.ir/Portal/Home
18. http://www.parstimes.com/history/mois_loc.pdf
19. http://theiranproject.com/blog/2017/10/12/trump-prompts-rouhani-administration-irgc-close-ranks/
20. http://www.parstimes.com/history/mois_loc.pdf
21. https://english.alarabiya.net/en/News/middle-east/2016/12/05/Iran-creates-electronic-Brigades-for-cyber-war.html
22. http://www.iranwatch.org/iranian-entities/islamic-revolutionary-guard-corps-irgc
23. https://www.mojahedin.org/newsen/45167/Opposition-Group-Iran%E2%80%99s-%E2%80%98Cyber-Army%E2%80%99-Falls-Under-the-Command-of-the-IRGC
24. http://cyberarmy.blogfa.com/
25. https://english.alarabiya.net/en/News/middle-east/2016/12/05/Iran-creates-electronic-Brigades-for-cyber-war.html
26. http://sayberi174.ir/
27. https://www.memri.org/reports/irans-cyber-war-hackers-service-regime-irgc-claims-iran-can-hack-enemys-advanced-weapons
28. ashiyane.ir
29. http://info.bayshorenetworks.com/hubfs/assets/press-releases/IDR_nov52013.pdf?t=1498223049158
30. https://www.fireeye.com/blog/threat-research/2017/09/apt33-insights-into-iranian-cyber-espionage.html
31. https://www.checkpoint.com/press/2015/new-details-rocket-kitten/
32. https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf

## Activity Overview

The Islamic Republic's revolutionary foundations have helped to orient its offensive activities (both standard and cyber) in an asymmetric fashion. This is because of the unique regional influences it has to contend with, including a number of global powers exercising direct and indirect power over its affairs. Because of the early trauma of the Stuxnet virus, Iran has been able to experience first-hand the impact of such a campaign. With investment, a sophisticated offensive cyber capability could grant Iran the leverage it craves as a US deterrent and regional power. Therefore, it is not surprising that Iran capitalized on the attack and has since aggressively pursued its own capability. They are already more mature than most of the Gulf Cooperation Council states (GCC).

One of the major worries from the international community, voiced in the implementation of sanctions over the years, has been Tehran's support of proxy-groups. Some of these groups, labelled as terrorist organisations, operate in regional conflict hotspots such as Palestine, Yemen and Syria. Iran provides training and resources to groups such as Lebanese Hezbollah, Badr Corps, Kata'ib Hezbollah and Asa'ib ahl al-Haq[38]. In a similar fashion (and not unlike other global powers), the Islamic Republic has been using hacktivist groups to support its endeavours and further their own aims. There has even been reports that Iran may has been funding the Syrian Electronic Army (SEA)[39] [40]. Its overt support for Hezbollah, Houthis and Hamas are paralleled in accusations that Iran is helping to form cyber units for proxy groups as well.

Parallels can be drawn between those countries that Iran perceives as a priority threat to the security of the republic, and attributed cyber campaigns. This is evidenced by US indictment of several Iranian individuals believed to be associated with the IRGC. The indictment is in response to denial of service attacks against US financial entities between 2011 and 2013[41]. In 2012, the destructive Shamoon virus targeted Saudi Aramco (Saudi Arabia's state-owned oil company). Saudi is a competing regional power led by a Sunni government that Iran is in direct confrontation with. This manifests in the surrounding conflicts and in the energy industry. They also share a long-term, overarching historic notion of religious superiority that is in direct conflict (Sunni vs Shia). This ideological conflict is entrenched and is unlikely to be resolved.

## Future Concerns

### 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. The conflict between the two countries was deepened more recently by a harsh anti-Iranian resolution issued at the UN in 2016, and the execution of a prominent Shia cleric Sheikh Nimr al-Nimr[42]. When Iran was given the opportunity to start participating in the international economic system again, Saudi Arabia viewed this with alarm[43]. Given the pragmatic approach Iran has displayed towards meeting its requirements in the JCPOA, some would suggest that Iran is not going to be provocative and offensive. Saudi is better financed militarily and better equipped. However, in the long-term, Iran sees itself as progressing and only becoming more influential whilst Saudi Arabia has to contend with maintaining an edge. Iran is likely to continue to use indirect means to undermine Saudi Arabia, using proxy-groups and disinformation.

### The United States

The United States has already been the at the receiving end of some of Iran's offensive activity. The US is responsible for the implementation of harsh international sanctions that have demonstrably impacted the Iranian economy. The JCPOA, agreed upon by moderate President Hassan Rouhani with the P5+1, provided some

33. https://cdn2.hubspot.net/hubfs/270968/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf
34. http://www.clearskysec.com/tulip/
35. http://www.iranwatch.org/iranian-entities/passive-defense-organization
36. https://www.files.ethz.ch/isn/154842/No375_15OCT2012.pdf
37. https://phoenixts.com/blog/the-iranian-cyber-threat-part-1-irans-total-cyber-structure/
38. https://csis-prod.s3.amazonaws.com/s3fs-public/congressional_testimony/ts161206_Dalton_Testimony.pdf
39. https://motherboard.vice.com/en_us/article/nze5nk/the-syrian-electronic-armys-most-dangerous-hack
40. http://www.reuters.com/article/us-syria-crisis-cyberspace-analysis/analysis-syria-aided-by-iran-could-strike-back-at-u-s-in-cyberspace-idUSBRE97S04Z20130829
41. https://www.fbi.gov/wanted/cyber/iranian-ddos-attacks
42. https://www.wilsoncenter.org/publication/the-iran-saudi-arabia-conflict-and-its-impact-the-organization-islamic-cooperation
43. http://yaleglobal.yale.edu/content/iran-nuclear-deal-fuels-tension-saudi-arabia-inflaming-new-conflicts

sanctions relief and this contributed to economic growth in 2016. However, the real threat of fresh and revived sanctions from the Trump administration is likely to hurt Iran's renewed optimism and hostility can already be observed. Confounded by a mixture of Anti-American sentiment based on historic regional US interference, Iran is unlikely to stop perceiving the US as an adversary in the near future. Consequently, the US is a worthy adversary to conduct asymmetric activity against. This may manifest in both direct and indirect campaigns. It is probably not a coincidence that a country under harsh sanctions against its financial sector has historically targeted the financial sector of the said persecutor (US). This might be repeated, if so then the mirror target for the IRGC would be US Cyber Command or another government/military adversary. he ability for Iran to think strategically has been observed too though. It may opt for continuing its tradition of using proxy-groups to provoke and attack larger better equipped forces it doesn't really want a full-scale war with[44].

## Israel

Iran has pursued an aggressive stance towards Israel since fall of the Soviet Union, after which it severed diplomatic relations. This may have been due in part, for the need to appeal to Arab and Muslim opinion whilst relations were redefined in that era. The then President Mahmoud Ahmadinejad used very anti-Semitic language[45]. 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 accused of being behind the Stuxnet virus alongside the US. Iran is accused of funding and equipping Palestinian paramilitary group Hamas with missiles. During Operation Protective Edge in 2014, in which 2,100 Palestinians (mostly civilians)[46] were killed by the Israel Defense Force (IDF), Iran is attributed to a number of cyber-attacks against Israeli entities[47]. This relationship is unlikely to change in the near future as Israel is viewed as a justifiable adversary to attack and undermine through any means.

## Kazakhstan

The location of Kazakhstan combined with it being the top producer of Uranium, makes this country a very important ally of Iran. Sanctions impacted economic exchanges between the two states. Diplomatic relations between the two countries have come under suspicion in the past as Iran is accused of only being interested in knowledge transfer from Kazakstan's scientists and as a source of Uranium[48]. International suspicion has led Kazakhstan to be demonstrably cautious in its dealings with Tehran. Iran's interest in Kazakhstan's scientists could be an area of intellectual theft and cyber espionage as part of achieving its nuclear ambitions.

## Syria/Iraq

Tehran supports President Bashar al-Assad along with Russia in the Syrian civil war. Continued engagement in this area is highly likely. Iran shares a border with Iraq, so the outcome of the conflict and the need for a pro-Iranian government is important. Iran is likely to continue to undermine any progress Western-backed, or Saudi-backed forces make in the area through proxy-groups, cyber-attacks and conventional military support.

## Latin America

Iran has reportedly operated an intelligence network in Latin America for decades[49]. The network is believed to be channeled through embassies, mosques and affiliation through Hezbollah. Hezbollah's presence in the region has been linked to organized crime and as a means for revenue[50]. Iran is also not shy about conducting cyber-attacks in Latin America. A recent report showed Iran, working in conduit with Venezuela, planning an attack against US systems made to look like it originated from Mexico[51]. Venezuela and Iran are both coping with oil sanctions, and are working with Syria to construct a new refinery. With this in mind, it would not be unreasonable to assume Iran will continue to penetrate Latin America for intelligence purposes, to subvert some of the constraints placed by international sanctions and as a means for proxy attacks.

## South Caucasus and Central Asia

Despite cordial relations with the majority of states in this region, Iran has to be very strategic in how it handles its relationships and access to resources. This is because of the competing influences of China and Russia. Azerbaijan has also been very close to Israel, exchanging defence technology and increased trade. This has given Iran some cause for concern. Any opportunity to understand the web of interests in this area is likely to be taken advantage of. This might indicate an area of interest for espionage campaigns.

44. http://www.soufangroup.com/tsg-intelbrief-irans-growing-cyber-capabilities/
45. http://iranprimer.usip.org/resource/iran-and-israel
46. http://www.bbc.com/news/world-middle-east-28439404
47. https://www.files.ethz.ch/isn/183365/No.%20598%20-%20Gabi%20and%20Sami%20for%20web.pdf
48. https://csis-prod.s3.amazonaws.com/s3fs-public/publication/160420_Milani_IranReconnectingEurasia_Web.pdf
49. https://www.thecipherbrief.com/column_article/iran-and-hezbollah-remain-hyperactive-in-latin-america
50. http://iranprimer.usip.org/blog/2015/mar/18/irans-influence-latin-america
51. http://www.heritage.org/middle-east/commentary/iran-conducting-anti-us-operations-latin-america