Recorded Future®

CYBER THREAT ANALYSIS | IRAN

Despite Infighting and Volatility, Iran Maintains Aggressive Cyber Operations Structure

By Insikt Group®

CTA-IR-2020-0409

Recorded Future's Insikt Group® is conducting ongoing research on the organizations involved in Iran's cyber program. This report serves to provide greater insight into the major military and intelligence bodies involved in Iran's offensive cyber program. Although offensive cyber capabilities include domestic attacks, we researched those organizations with declared international missions. Due to the secretive nature of some organizations and lack of verifiable information, we incorporated competing hypotheses to adhere to industry analytic standards.

For the purposes of this research, we investigated the Islamic Revolutionary Guard Corps (IRGC), including the Basij, as well as the Ministry of Intelligence and Security (MOIS), and the Ministry of Defense and Armed Force Logistics (MODAFL). Although the report suggests links between a select number of advanced persistent threat (APT) groups and certain intelligence organizations, we are unable to conclusively assign them to specific agencies due to gaps in information about each group.

The sources for our research primarily include intelligence surfaced in the Recorded Future® Platform, industry research released by Symantec, FireEye, ClearSky, and PaloAlto, among others, and open source news reports.

Executive Summary

While the Iranian cyber program remains at the forefront of Tehran's asymmetric capabilities, its intelligence apparatus is colored by various dysfunctions and seemingly destabilizing traits. In particular, the politicization of its various intelligence agencies and ensuing domestic feuds have reportedly polarized officer-level rank and file throughout the various security crises of the Islamic Republic. These crises have surfaced publicly and have acted as catalysts to drive insider threats, have lowered intelligence morale, and have increased the occurrences of leaks. Competition between the intelligence groups has also allegedly led to direct acts of sabotage between agencies.

Amid the political infighting, certain organizations have experienced significant expansions in security powers which undoubtedly includes leveraging offensive hacking tactics, techniques, and procedures (TTPs) to further their intrusions and access to victims. First among those is the Islamic Revolutionary Guard Corps — Intelligence Organization (IRGC-IO). The entity's mission has grown significantly in the last decade, so much so that it is capable of operating in direct contravention to the intelligence assessments and advice of the Islamic Republic's constitutionally mandated intelligence agency, the Ministry of Intelligence and Security (MOIS).

This is Recorded Future's third report on Iran's cyber program. In January 2019, we reported on Iran's best-known hacker forum, Ashiyane, and in March 2019, we released a report that covered Iran's cyber defense structure and associated organizations.

Key Judgments

- We assess that although there is a differentiation between Iranian agencies that execute internal and external operations, the undefined (and at times overlapping) security missions of each intelligence agency likely complicates efforts to conduct cyber-related attribution.
- We assess that the potential for disinformation by Iranian and extra-regional actors is likely to remain elevated as a result of the volatility in the intelligence establishment and overlapping responsibilities.
- Owing to the complex nature of the Iranian intelligence establishment, history of leaks, and politicization, we assess that Iran's security sphere likely remains volatile.
- Aggressive, ideologically motivated cyberattacks bear the traits of the IRGC, and in particular, its overseas operations command, the Quds Force. We assess the organization is likely to have coordinated destructive operations as part of Iran's asymmetric response capability.
- We assess that tertiary academic institutions, such as the Imam Hossein University, are highly likely to continue to assist the Iranian cyber program and enhance the capabilities of regime-aligned operators.
- We assess that Iran-based, specialized contracting groups are likely to service various government and military entities. Contracting groups are also likely to cater to agency-specific tasking depending on the threat and target of opportunity.

Background

Iran's intelligence and military-led cyber operations are influenced by a variety of factors: the complex nature of the intelligence establishment, overlapping mission sets, the rulings and interests of Supreme Leader Ali Khamenei, the influence of military organizations such as the Islamic Revolutionary Guard Corps (IRGC), and internecine politics.

The Iranian Intelligence Establishment

According to Iran's Fars News Agency, the Iranian intelligence establishment has grown since the 1979 Islamic Revolution to include at least 16 separate bodies that conduct intelligence activities. The Fars report also highlighted the role of the Council for Intelligence Coordination (Shorai-e Hamohangi Etelaat) which purportedly acts as the principle mechanism to unite all intelligence entities to coordinate efforts against a variety of domestic and international security threats.

Iranian intelligence agencies are either components of the IRGC organization, or like the Ministry of Intelligence and Security (MOIS), belong to the varying components of Iran's elected government. These entities, however, are all subordinate to the edicts of Supreme Leader Khamenei; some, such as the Islamic Revolutionary Guard Corps — Intelligence Organization (IRGC-IO) are assessed to adhere to Khamenei's interests more directly than others. MOIS, which is currently led by Mahmoud Alavi, officially leads MOIS's intelligence mission in coordination with the priorities of the elected government.

Characteristics of Iranian intelligence include overlapping tasking, targeting requirements, and operational responsibilities, which in some cases lead to competition for, or a convergence of, intelligence and military resources. For example, as discussed below, combating domestic subversion is not only reportedly executed by MOIS, but also the IRGC-IO, as well as other agencies such as Iran's Cyber Police (FATA).

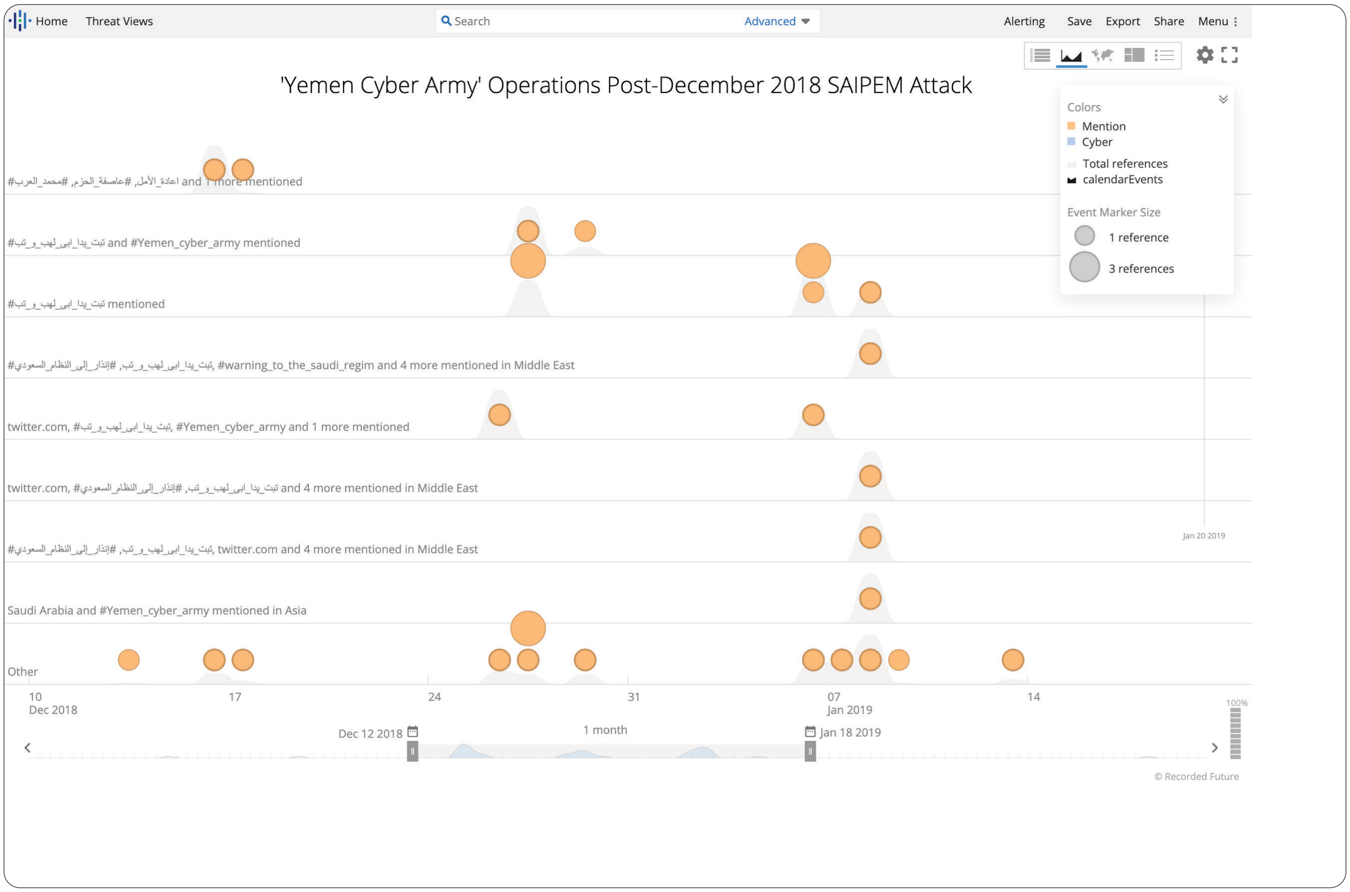
Internationally, both MOIS and the IRGC have been reported to lead independent intelligence operations, as well as cooperate in operations against national security threats. Such overlaps, in certain cases, complicate kinetic and cyber attribution efforts. Other intelligence operations, such as those cited in a February 2019 U.S. Department of Justice (U.S. DOJ) indictment against various Iranian cyber operatives, suggests that resources are shared between agencies, and operatives are likely to provide services to more than one element associated with Iranian security services.

Overlapping Cyber Missions

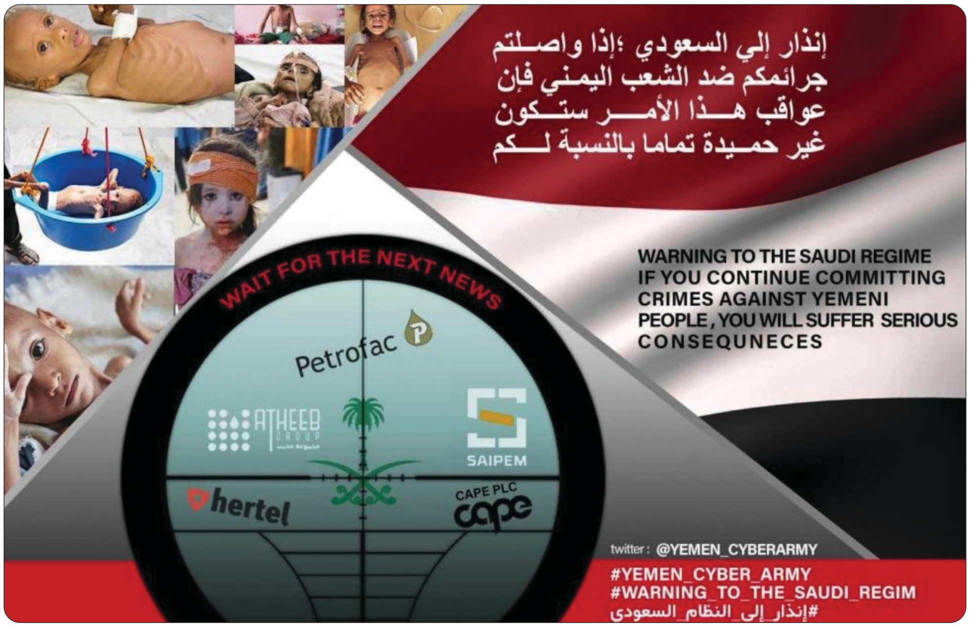
The attribution of cyber campaigns and incidents in many cases reveal the plausible strategic and tactical interests of two, if not more, intelligence organizations of the Islamic Republic. The MOIS and the IRGC remain the most pertinent entities with overlapping intelligence and security missions. APT groups also respond to the tasking requirements of both organizations, and as we highlight below, to specific sub-groups. While technical attribution is conducted by Recorded Future and the broader industry, without access to information on the composition of APT groups, including personnel and their networks' affiliations, APT attribution to specific organizations becomes more complex. Attribution necessitates the aggregation of multiple technical, organizational, and personal behavioral data sets, to enable more precise attribution.

Like other nations, strategic and tactical information is key for Iranian agencies. Political, military, and economic information is a major driver for international cyberespionage operations, including against officials from various Western and Middle Eastern governments. These operations have historically occurred during periods of elevated tensions between Tehran and the international community. Within this international area of operations, various threat actor groups have continued to support not only MOIS and the IRGC's requirements, but those of a range of government stakeholders and academic institutions, including research and development organizations associated with the Ministry of Defense and Armed Force Logistics (MODAFL).

Public reporting reveals that known Iranian threat actors have also led operations against Middle Eastern states, at times coordinating and collaborating against specific targets as part of broad computer network attack operations. Most recently this included the use of the ZeroCleare destructive malware against Bahrain. However, destructive attacks have been part of Iran's asymmetric response and attack capability since at least August 2012. In mid-December 2018, the Italian petrochemical giant, SAIPEM, was targeted, likely by pro-Iranian government actors, using an updated variant of the Shamoon(2) (Disttrack) malware. The December 2018 attack was accompanied shortly thereafter by hacktivist-style defacements and social media-based information operations executed by entities claiming to represent the Yemen Cyber Army, a collective supporting the interest of and aligned with the Houthi movement (Ansar Allah). The collaborative effort highlights the potential for mission coordination and shared resources in offensive efforts, by potentially diversified threat actor groups.


Home
Threat Views
Search
Advanced
Alerting
Save
Export
Share
Menu
'Yemen Cyber Army' Operations Post-December 2018 SAIPEM Attack
Colors
Mention
Cyber
Total references
calendarEvents
Event Marker Size
1 reference
3 references
#محمد_العرب, #عاصفة_الحزم, اعادة_الأمل and 1 more mentioned
#تبت_يدا_ابى_لهب_و_تب and #Yemen_cyber_army mentioned
#تبت_يدا_ابى_لهب_و_تب mentioned
#إنذار_إلى_النظام_السعودي, #تبت_يدا_ابى_لهب_و_تب, #warning_to_the_saudi_regim and 4 more mentioned in Middle East
twitter.com, #تبت_يدا_ابى_لهب_و_تب, #Yemen_cyber_army and 1 more mentioned
twitter.com, #إنذار_إلى_النظام_السعودي, #تبت_يدا_ابى_لهب_و_تب and 4 more mentioned in Middle East
#إنذار_إلى_النظام_السعودي, #تبت_يدا_ابى_لهب_و_تب, twitter.com and 4 more mentioned in Middle East
Saudi Arabia and #Yemen_cyber_army mentioned in Asia
Other
Jan 20 2019
10
Dec 2018
17
24
31
07
Jan 2019
14
Dec 12 2018
1 month
Jan 18 2019
100%
© Recorded Future

Recorded Future query on some of the Yemen Cyber Army's social media operations.


إنذار إلي السعودي ؛إذا واصـلتم
جرائمكم ضد الشعب اليمـني فإن
عواقب هــذا الأمـــر ستـــكون
غير حمـيدة تماما بالنسبة لـــكم
WARNING TO THE SAUDI REGIME
IF YOU CONTINUE COMMITTING
CRIMES AGAINST YEMENI
PEOPLE, YOU WILL SUFFER SERIOUS
CONSEQUNECES
WAIT FOR THE NEXT NEWS
Petrofac
ATHEEB GROUP
SAIPEM
hertel
CAPE PLC
cape
twitter: @YEMEN_CYBERARMY
#YEMEN_CYBER_ARMY
#WARNING_TO_THE_SAUDI_REGIM
#إنذار_إلى_النظام_السعودى

Imagery that accompanied the Yemen Cyber Army's social media operations listed SAIPEM, among other companies.

On the domestic front, the intelligence and security establishment, including FATA, combats a wide range of anti-regime political, militia, and extremist movements. The state's security services have been recorded conducting kinetic and cyber operations against religious minorities as well as Kurdish, Ahwazi-Arab, and Balochi ethnic separatists. For example, the threat actor group referred to as Domestic Kitten by Check Point reportedly ran an extensive cyber surveillance campaign specifically targeting dissidents, extremist groups, and ethnic minorities inside and outside of Iran. This group reportedly ran most of its operations against Farsi-, Arabic-, Turkish-, and Kurdish-speaking targets, using social engineering to trick victims into downloading malicious mobile applications.

Targets/ Organizations	Government/ Politicians	Activists*	Journalists	Mojahedin-e Khalq	Religious Minorities	Ethnic Separatists	Dual Nationals	Cybercriminal
IRGC	•	•		•		•	•	**
IRGC-IO	•	•	•	•	•	**	•	**
MOIS	**	•	•	•	**	•	•	**
FATA		•	•					•
MODAFL	**							

Known overlapping domestic security missions.[1]

In FATA's case, it too has reached beyond its purported legal mandate of countering cybercriminal activity and has targeted Iranian bloggers, such as Sattar Beheshti. We note that within the operational scope of Iranian cybercrime matters, and Iran's Computer Crimes Law specifically, the definition of a cybercriminal has practically manifested to include political activists that are caught disseminating anti-regime material or participating in online protests. Industry research has detailed various cases where political activists have been arrested and imprisoned under the Computer Crimes Law, and the flexibility embedded in such legislation to enable law enforcement entities to apply it at their discretion. As such, FATA's operations are highly likely linked to the government's crackdown on bloggers and activists that transpired following the 2009 Green Movement uprisings, but are likely to be limited to domestic security.

Iran's anti-dissident operations are also devoid of national boundaries, as Iranian cyber groups, such as APT35 (Charming Kitten), which has predominantly serviced the IRGC, and Flying Kitten have both demonstrated a penchant for targeting the Iranian diaspora throughout Europe and North America.

[1] *The activists grouping incorporates those that self-identify with specific causes and campaigns. These include, political, religious, environmental, human rights defenders, women's rights activists, labor rights activists, and ethnic nationalists (considered a cultural threat to the Islamic Republic). Reporting on the arrests of dual-nationals, religious minorities, journalists, and activists reveals the overlaps between the various security agencies.
**While we suspect the activities of these organizations in targeting the listed groups, we have not identified significant credible or verifiable information to corroborate their likely involvement in intelligence and cyber operations against those victims.

Military-related technologies, including software, also remain a top priority for a system that professes to be self-sufficient and strives to build and export its defense industry. As we expand on later in this report, entities such as MODAFL are assessed to be leading stakeholders and benefactors of computer network operations focusing on military armaments technology.

Iranian Custom Malware [2]	Foreign Governments	Aviation	Telecom	Energy	Financial/ Banking	Defense	IT/ Tech	Media	Human Rights/ Activists/ Extremist Groups[3]
BONDUPDATER	●			●					
DNSpionage	●	●							
Helminth	●				●	●	●		
STSRCheck		●		●		●	●		
INFY	●			●				●	●
POWBAT			●		●		●		
POWERSTATS	●		●	●		●			●
POSHC2	●	●		●	●			●	
POWSSHNET		●		●		●	●		
Port.exe		●		●		●	●		
POWERTON	●	●		●		●			
Remexi	●	●	●				●		●
Shamoon	●	●		●					
StoneDrill	●	●		●					
TONEDEAF	●		●	●	●				
TwoFace	●		●	●	●				
VALUEVAULT	●			●					
ZeroCleare/ DUSTMAN				●					

A list of common custom and open source malware and targeted industries[4]

[2] *Other links to operations in the Middle East that used VBScript can be found here.

[3] As noted above, the activists grouping incorporates various different entities.

[4] In some instances, reports on the sectors or victims were generic, for example, stating that the "business" sector was targeted, but did not specify which industry vertical.

Iranian Intelligence Leaks

Leaks have regularly impacted Iranian intelligence, in particular the MOIS. Throughout its history, the organization has endured multiple bouts of high-impact disclosures that have threatened to expose the system's high-ranking members and its international operations; significant cases include the "Chain Murders," the "Iran Cables," and to a lesser extent, various uncorroborated cyber leaks associated with anti-government operations. Political grievances have driven major leaks against intelligence agencies. These depict violations against fellow intelligence officers and Iranian society, corruption and cover-ups, or as the most recent Iran Cables suggests, MOIS's disdain of the IRGC-Quds Force's intelligence and military primacy and practices in Iraq.

Anti-government cyber operations predominantly materialized in the years following the 2009 Green Movement uprising and were conducted by self-declared anti-government anonymous collectives, such as Anonymous Iran. These groups aimed to expose Tehran's cyber efforts against its civilians and international targets, and have resulted in the disclosures of allegedly confidential documents, cyber projects, corruption in the Iranian government, and international operations against Middle Eastern countries. The most recent uptick in anti-government cyber operations began near the end of 2017 until the time of writing, with various groups such as Tapandegan, Lab Dookhtegan, and Aahack Security Team reportedly leading intrusions against government and military assets.

Suspected Disinformation Efforts

Our investigations on Iranian disinformation continue to identify plausible cases of misdirection, and as such, at the time of this writing, we assess the potential for disinformation by Iranian actors is likely to remain elevated in the future. This is further amplified by leaks and the potential that extra-regional actors manipulate leaked data, or degrade data categorization and attribution, to service their interests against Western cybersecurity organizations. The latter, for example, includes the use of pre-existing C2s to obfuscate an extra-regional threat actor's own operations.

Since late 2017 and throughout 2019, self-declared Iranian dissident entities have pursued comprehensive efforts to expose the Iranian intelligence and military establishments' operations in Iran and throughout the Middle Eastern region. These efforts included groups such as Lab Dookhtegan, the "Green Leakers" (Afshagaran-e Sabz), "Black Box" (Resaneh Khabari Jabeh Siah), and "Hidden Reality" (Vaghiyate Penhaan). The latter reported on the activities of an alleged contractor, the Rana Institute, which we discuss in greater detail below. As of this writing, Insikt Group has not comprehensively corroborated all the information and missions these groups claim to uphold against the Islamic Republic. While these entities purport to act against Tehran, and have disseminated extensive information against an APT group as well as Iranian intelligence, we assess it is also possible that one or more of these groups was established with the objective of executing disinformation.

Kaspersky Labs published two reports in August and December 2019 possibly linking Russian threat actors with the Rana Institute leak. Based on an analysis of the leaked materials, the infrastructure, and the dedicated website, the reports assessed that threat actors associated with the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU) were behind the link. However, at the time of this writing, Recorded Future cannot confirm the validity of this assessment.

In another case, Recorded Future reported on the alleged death of a senior member of Iran's cyber program, Mohammad Hussein Tajik, which was covered in reporting on Iran's hacker hierarchy and disinformation efforts surrounding the IRGC-IO's capture of dissident Ruhollah Zam. As of this writing, the information disseminated about Iran's cyber program to dissidents like Zam has not been corroborated. Zam has repeatedly been the subject of character defamation attacks, as well as being outed by Iranian intelligence as being a victim of their intelligence operations. We assess such activities were presumably undertaken to degrade Zam, and the confidence placed on his sources and methods. Zam's reporting on Tajik implicated Iran in international cyber operations against the U.S., Saudi Arabia, and Turkey, and also linked it to an operational facility, the Khaybar Center, from where those attacks were allegedly launched. This facility, according to Zam's accounts, operates like a fusion center with members from Iran's major intelligence group's present onsite.

While disinformation efforts emanating from Iran remain a credible threat, we assess that extra-regional actors could also be attempting to misdirect detection and attribution efforts by impersonating Iranian APT groups. We assess this may include using server infrastructure (C2) previously affiliated with Iranian threat actors, such as APT33, APT35, and MuddyWater. We highlighted this as a possible scenario in our December 2019 Operation Gamework report that revealed C2 and malware overlaps with Russian APT BlueAlpha.

Politicizing the Intelligence Establishment

Due to the Iranian intelligence establishment's history of leaks, and periods of increased politicization and factionalism, we assess that Iran's security sphere likely remains volatile.

Farsi-language open source reporting highlights how Iran's MOIS has experienced increased levels of factionalism, which has likely harmed the agency's ability to secure its scope. Public reporting further indicates that internecine politics has affected multiple layers of the intelligence establishment, pitting the head of the IRGC-IO Hossein Taeb against former MOIS leader Heydar Moslehi and various politicians, including former president Mahmoud Ahmadinejad (2005-2013) and Sadeq Larijani. The IRGC-IO leader is reported to have backed intelligence operations against Iranian political groups that had compromising evidence against the IRGC that specifically depicted cases of corruption.

Under former president Mohammad Khatami (1997-2005), MOIS is purported to have undergone a cull of hardline officers and supporters, which ultimately led to the agency's retreat from pursuing aggressive international operations and its moderation.5 Between 1997 and 1998, Supreme Leader Khamenei is reported to have promoted the IRGC's intelligence mission to that of a directorate. From that point on, the IRGC's Intelligence directorate commenced executing similar duties to those of MOIS, which we believe contributed to the overlapping efforts to address national security threats.

[5] S. Chubin, Wither Iran?: Reform, Domestic Politics and National Security, New York, Oxford University Press, 2002, P. 91.

Under former president Ahmadinejad, MOIS reportedly experienced further instability after the 2009 uprising, with IRGC-led purges against MOIS officers. Public reports also cite how Ahmadinejad attempted to leverage MOIS to accrue kompromat ("compromising material") against political rivals. Hardliner intentions to undo the Iranian reformism led by Khatami and his predecessor Rafsanjani were accurately captured in an early declaration, "The New Era and Our Responsibilities" (dowlat-e jadid va masooliat-haye ma), authored by leading members of Iran's hardline and pro-IRGC Ansar Hezbollah. The declaration issued a warning and demanded that the first government of Ahmadinejad prevent MOIS's continued drift toward Khatami-era changes, and presumably, an Iranian intelligence service less likely to execute ideologically motivated international operations.

MOIS has experienced similar instances of politicization under current President Hassan Rohani (2013-present). Iran's Intelligence Minister, Mahmoud Alavi, has been blamed for lacking intelligence and security credentials, and has subsequently been the target of politically-motivated attacks instigated by hardline elements. Similar to the Khatami presidency, Rohani commenced his term with a reform-minded agenda, which included moderating MOIS and making it more accountable. Reporting from the BBC suggests Rohani has used the agency in anti-corruption cases, which has further entrenched it in a political dogfight to evict the IRGC and its supporters from commandeering sectors of the Iranian economy.

According to a BBC report, MOIS, on at least three separate occasions, has been outmaneuvered and its rulings rejected by the parallel activities and clout of the IRGC-IO. These reportedly included arresting managers of pro-reformist Telegram Channels, the arrest of members of Rohani's Joint Comprehensive Plan of Action (JCPOA) negotiations team on espionage charges, and the arrest of environmental activists. Under Rohani, MOIS is reported to have continued to lose its powers to the IRGC-IO within the national security sphere, in particular within the counterintelligence and counter domestic subversion domains.

Impact on the Iranian Cyber Cadre

The increased level of factionalism in the Iranian intelligence establishment is likely to have impacted Iran's cyber forces. Insikt Group assesses the direct results of the political infighting is likely to have trickled down to Iranian cyber operators, which to date publicly support one side or another (MOIS or the IRGC).

Social media chatter, for example, has shed light on the disagreements and taunts between Iran-based cyber operators supporting the IRGC, such as Armin Rad (also known as "Ayoub Tightiz") and Mohammad Jorjandi, who has often criticized Rad and his support base.[6] Additionally, according to Jorjandi, who is reportedly based in the U.S., as of this writing, the hack and leak operations tied to Lab Dookhtegan are allegedly borne out of the competition between the MOIS and the IRGC, where the latter has purposefully leaked information about MOIS to damage its reputation and standing.

Although we can not corroborate Jorjandi's statements, the alleged targeting of MOIS as depicted by Lab Dookhtegan has included members of APT34, such as Yashar Shahinzadeh. Our observations of Shahinzadeh's social media chatter suggest he has sided against pro-IRGC regime hackers like Rad, and has attempted to assist members of the elected government, in particular the Minister of Information and Communications Technology, Mohammad Javad Jahromi. This assistance has predominantly centered on detecting vulnerable government databases.

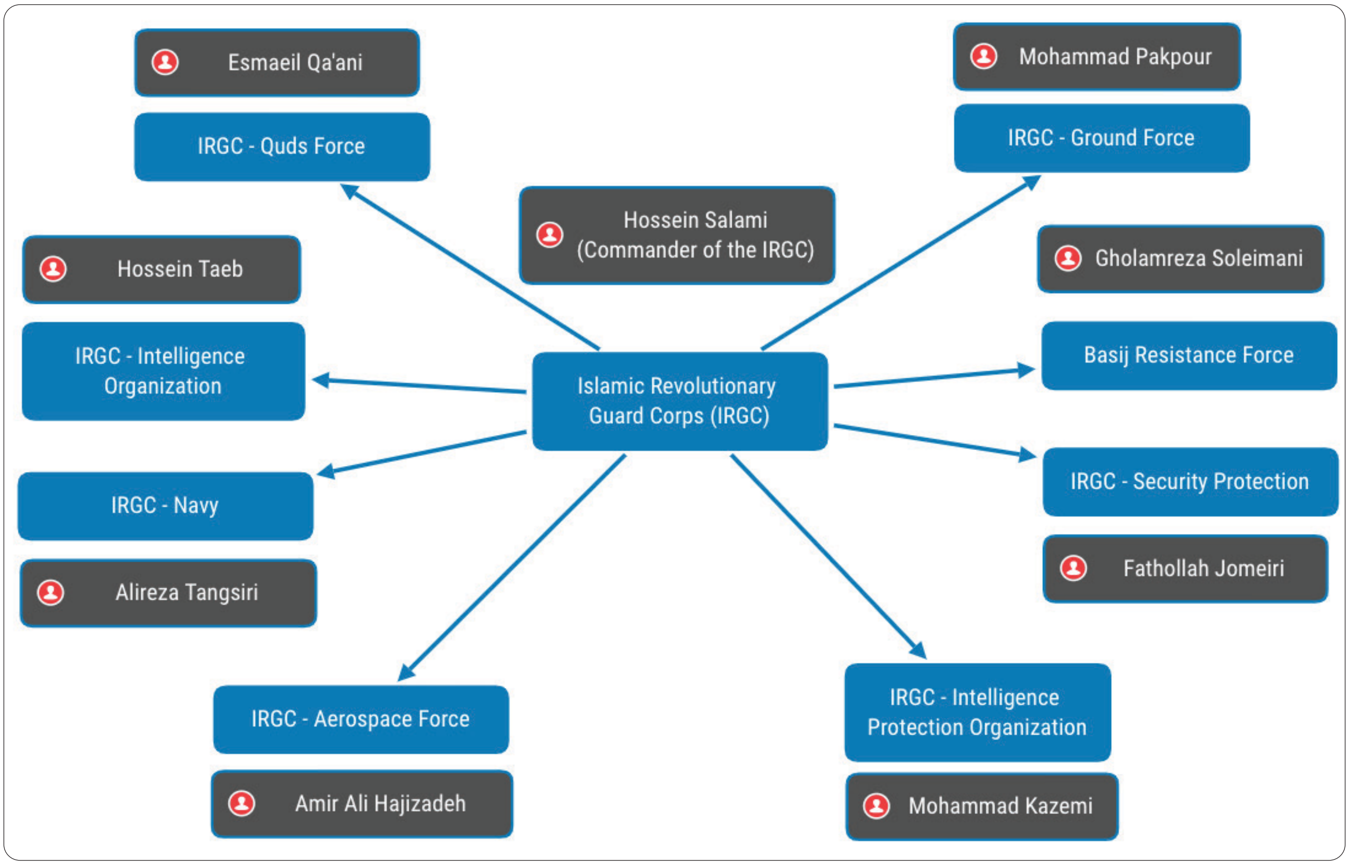
The Organizations and the Cyber Mission

The Islamic Revolutionary Guard Corps

We assess that aggressive, ideologically-motivated cyberattacks bear the traits of the IRGC, and in particular its overseas operations command, the Quds Force. The organization is likely to have coordinated international operations, including destructive operations, as part of Iran's asymmetric response capability.

[6] https[:]//www.tabnak[.]ir/fa/news/816849

The IRGC is composed of eight branches and is currently led by Commander Hossein Salami. Of the eight, we assess that at least four possess an offensive cyber capability. These include the Quds Force led by Esmaeil Qa'ani, the Intelligence Organization headed by Hossein Taeb, the Basij Force commanded by Gholamreza Soleimani, and the IRGC's Intelligence Protection Organization led by Brigadier General Mohammad Kazemi. The remaining groups, including the Ground Force, Navy, Air Force, and the Security Protection Corps (physical and site protection) are not publicly known to be executing offensive cyber operations against foreign targets.



The IRGC's command structure.

The IRGC's provincial commands, of which there are 32 throughout Iran, report to the Ground Force commander, Brigadier General Mohammad Pakpour, and are reported to work in tandem with the Basij Resistance Forces (the Basij Command) on intelligence, surveillance, and defensive cyber operations. The IRGC commander Mohsen Kazemeini claimed in March 2016 that the organization's two major bases located in central and greater Tehran, the Mohammad-Rasoolallah Corps and Seyed Shohada Corps, are home to personnel with defensive cyber capabilities. The Mohammad-Rasoolallah Corps base is reportedly dedicated to countering localized cyber dissent and information operations. Kaemeini also claimed these bases do not execute cyber operations against foreign targets. As of this writing, we cannot corroborate whether these bases have conducted international operations, but we do assess Mohammad-Rasoolallah Corps's domestic role to be credible.

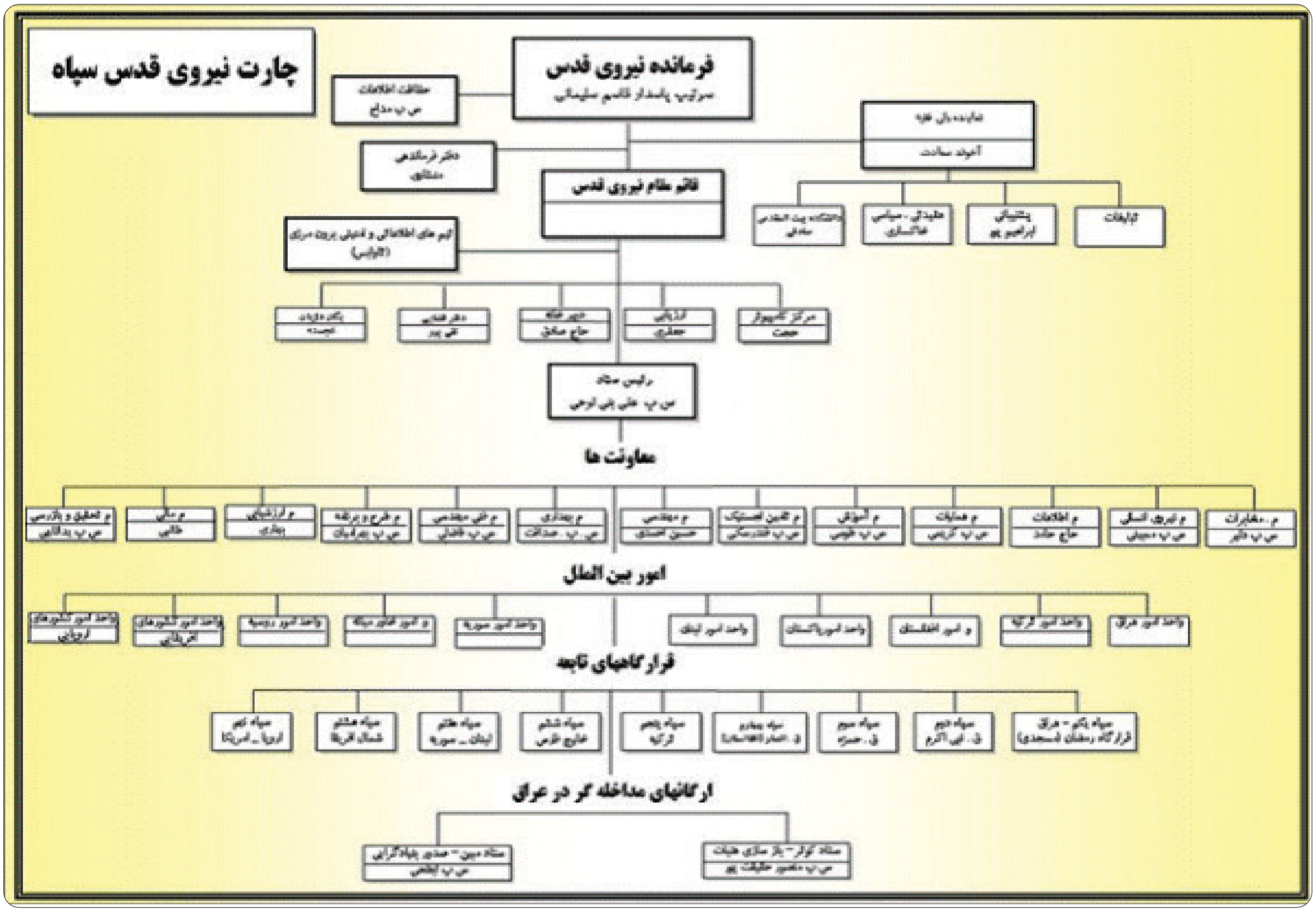
The Quds Force

Western media reporting on the Quds Force has identified it as a standalone entity within the IRGC that is directly accountable to the Supreme Leader on key strategic domains such as establishing and running the "Axis of Resistance" model throughout the Middle Eastern region. Dissident reports on the alleged structure of the organization indicate that it effectively uses its own methods to conduct international liaisons with foreign parties, intelligence activities, revenue generation and banking, its own military and special operations activities, as well as cyber operations.[7] The Quds Force's Intelligence service was, according to Farsi-language reporting, at one point headed by General Hamed Abdollahi, who is now allegedly leading "Unit 400," the special operations group.

We assess that the Quds Force under Suleimani is highly likely to have expanded its powers, and based on the Supreme Leader's reported historical responsibility of managing the IRGC's foreign operations, we assess it is highly likely the organization has enjoyed a significant amount of independence from the IRGC's military bureaucracy.

[7] https[:]//www.mojahedin[.]org/news/22762

Dissident reporting, which remains uncorroborated as of this writing, suggests that the Quds Force has at least nine operational bases, with distinct geographical areas of interest, such as "Base five," which equates to Turkey, or "Base eight," which is responsible for North Africa.[8] Within the organizational chart among the various departments, there are 10 foreign affairs directorates with assigned regions. Among the many other components of the Quds Force's organization is an alleged "Computer Center." While we are not able to corroborate the detailed aspects of the reporting emanating from dissident groups such as the Mojahedin-e Khalq Organization (MEK) on the Quds Force, we assess with medium confidence that the group is likely to have been able to collect credible information on the structure of the Quds Force's organization. This was most evident in that organization's ability to detail the activities of the Quds Force in Iraq.



Dissident claims of the IRGC-QF's structure.[9]

[8] Ibid.
[9] Ibid.

Role in Cyber

The Quds Force does not have a publicly declared cyber operations mission, but this does not preclude the organization from involvement in such operations, both on an operational and strategic level. The U.S. DOJ states that the organization conducts "unconventional warfare and intelligence activities outside Iran, including assassinations and cyber-related attacks," as specified in a February 2019 indictment associated with intrusion operations against U.S. counterintelligence officials.

We assess that the IRGC-QF was likely able to influence and support groups such as the Syrian Electronic Army (SEA) against dissidents, or potentially to act as an interlocutor between Syrian and Iranian information security professionals to aid the Syrian regime of Bashar al-Assad.

Operations in Syria

Deutsche Welle (DW) coverage of the Quds Force's Syrian operations revealed that Qa'ani specified in December 2012 to Iranian media that the Islamic Republic was involved in "military, paramilitary, and civilian operations," further specifying that "non-physical" assistance was being provided. The IRGC-QF's strategic relationship with the Syrian regime was most recently highlighted by Al-Assad's visit to Tehran in early 2019, during which Iran's Ministry of Foreign Affairs was not involved in organizing and coordinating the high-profile event.

In October 2011, the U.S. Department of the Treasury issued a press release highlighting the IRGC-QF's lead support role to the government of Bashar al-Assad, and specified it acted as a conduit to the Syrian General Intelligence Directorate (GID). There is extensive open source information which highlights the IRGC's diplomatic and military support, including through the establishment of multiple bases in Syria.

We assess that the above noted reference to the non-physical assistance is likely related to the reported cyber assistance Iran has provided Syria to help disrupt anti-government dissidents. This type of non-physical assistance likely materialized in parallel with the anti-dissident operations of a threat actor group dubbed "Group5" by Citizen Lab. Based on the TTPs used throughout operations against Syrian dissidents, Citizen Lab was able to establish a robust assessment pointing to an Iranian nexus. The research further identified plausible links to an actor from Iran's Ashiyane hacking group, Mr. Tekide.

However, we also note the alleged involvement of MOIS in the establishment of security relationships and partnerships throughout the region and in Syria, as reported by regional outlets. This relationship occurred in parallel with the IRGC-QF's mission, but predates that of the expansion of the IRGC-QF's role in Syria following the uprisings that began in March 2011.

Due to the IRGC-QFs dominating presence in Syria overlapping with interests to quash Syrian anti-government entities as declared by Qa'ani, we cannot exclude the plausible involvement of the Quds Force in some aspect of the cyber assistance that Iran is highly likely to have provided the Syrian regime.

Supporting International Movements

Dissident reporting also links the Quds Force to involvement in international cyberattack operations. One particular dissident outlet with an established track record for reporting on Iranian cyber issues, including those linked to a March 2016 U.S. DOJ indictment, claimed in October 2013 that the Quds Force was the organization responsible for the "Hilf ol-Fozoul" blog, which ran in parallel with the Operation Ababil attacks. The Hilf ol-Fozul front depicted attempts to influence hearts and minds against the U.S. government and its Middle Eastern regional allies, Saudi Arabia and Israel.

The blog regularly referenced the al-Qassam Cyber Fighters. Industry researchers who engaged in direct communications with representatives from various Palestinian groups, including alleged members of the al-Qassam Cyber fighters and Islamic Jihad, specified that their cyber operators received assistance from foreign countries with similar ideologicial objectives.[10] Although these members did not specify where they received their assistance, we assess such assistance would likely emanate from the Islamic Republic.

According to the dissident source, the Quds Force leveraged the expertise of actors from the Nasr Cultural Institute (موسسه فرهنگی نصر), which Insikt Group previously reported on in June 2019, to lead multiple international attack operations, including Ababil and al Qassam Cyber Fighters.

While no evidence was supplied by the source to corroborate the activities of Nasr, the source did supply information on the activities and membership of ITSec Team and Mersad at least two and a half years prior to the unsealing of the U.S. DOJ indictment. We assess with medium confidence that this source is likely to have maintained formal or informal correspondence with Iranian hackers, which likely explains why it was able to source such information prior to public reporting on these groups.

We do not cover all the other suspected instances where similar groups have led ideologically motivated cyberattacks, information operations, or a combination of both, such as those attributed to Ansar ul-Hijaz. However, we assess that the IRGC-QF represents the ideologically motivated element of the Islamic Republic's foreign cyber operations. This does not preclude the IRGC-QF from cooperating with other IRGC groups inside Iran, especially if it is able to task domestic organizations and contractors to conduct operations on its behalf.

[10] E. Skare. Digital Jihad: Palestinian Resistance in the Digital Era, Zed Books, London, p.120.

The Intelligence Organization of the IRGC

As of this writing, the IRGC-IO (Sazman Etelaat va Amniat Sepah Pasdaran) is run by Hossein Taeb (also known as "Meysam"), and as of May 2019, the newly promoted IRGC-IO deputy director is Brigadier General Hassan Mohaghegh. Taeb is widely considered to be a Khamenei loyalist, and has a long record in the Iranian intelligence services, beginning his career in MOIS. The IRGC-IO is reported to have gained increased powers since the 2009 Green Movement with Taeb at the helm. Khamenei expanded the IRGC-IO's powers to counter anti-government operations, and as such, the entity became an organization, which further strengthened the IRGC's position within Iran's security landscape.[11]

The National Council of Resistance of Iran (NCRI), one of the largest anti-government Iranian dissident groups, claims the IRGC-IO's organizational structure is shaped by at least 10 directorates and includes a separate IRGC cyberspace command.[12] According to the group's network inside Iran, there exist among them "Security," "Technical," and "Data Collection" directorates. Radio Zamaneh information dating to September 2012 also highlighted the existence of a Department 101, which focused on the "internet" and consisted of eight intelligence units. Department 101 is reportedly responsible for acting as a special entity within MOIS, coordinating intelligence activities. Although Insikt Group is not able to corroborate the veracity of the information supplied by Farsi-language reporting or the NCRI, we assess it is likely that the IRGC-IO has expanded and evolved into various directorates that are staffed to target political and anti-regime elements.

[11] A, Alfoneh. "ALL THE GUARD'S MEN: Iran's Silent Revolution." World Affairs 173, no. 3 (2010): 73-79.

[12] Iran: Cyber Repression How the IRGC Uses Cyberwarfare To Preserve the Theocracy, National Council of Resistance of Iran, February 2018, p.45.

The IRGC-IO's mission is widely reported to mimic that of MOIS; however, in our November 2019 report on Iranian dissident Ruhollah Zam, we also highlighted the entity's alleged politically motivated targeting. Various cases suggest political opponents, as well as figures in Rohani's government, Rohani's family, and dual nationals, were purportedly executed by members of IRGC's cyber wing or entities supporting the organization. According to media reports, threat actor groups APT35 and Rocket Kitten, among others, have been linked to cyber intrusions against President Rohani's and Zarif's email and Facebook accounts.

Although no information suggests that the IRGC-IO is the primary organization leading cyberattacks, former senior figure of Iran's MOIS Saeed Hajjarian stated that the Supreme Leader uses the powers bestowed upon the IRGC-IO like a "sword," a "shield," and a "mask." This raises the possibility that this organization is likely to be involved in major, politically-motivated cyber targeting to benefit Supreme Leader Khamenei and the hardline establishment.

Iranian dissident groups have also supported assessments on the purported domestic cyber operations of the IRGC-IO. This includes the IRGC-IO's involvement in the development and dissemination of spyware applications that mimic the Telegram messaging service.[13] Domestic contracting parties reportedly contribute to this effort and other surveillance efforts.

The Basij in the IRGC's Intelligence and Cyber Mission

The Organization for the Mobilization of the Oppressed, commonly known by its Persian-language name, the Basij (Sazman-e Basij-e Mostazafeen), is widely recognized as the street muscle of the Islamic Republic. The key functions of the security and military apparatus of the Basij are to eliminate threats to the Islamic Revolution, be they ideological, physical, or virtual.[14] The Basij reportedly maintain a vital role in cyberspace, which is inclusive of information operations.

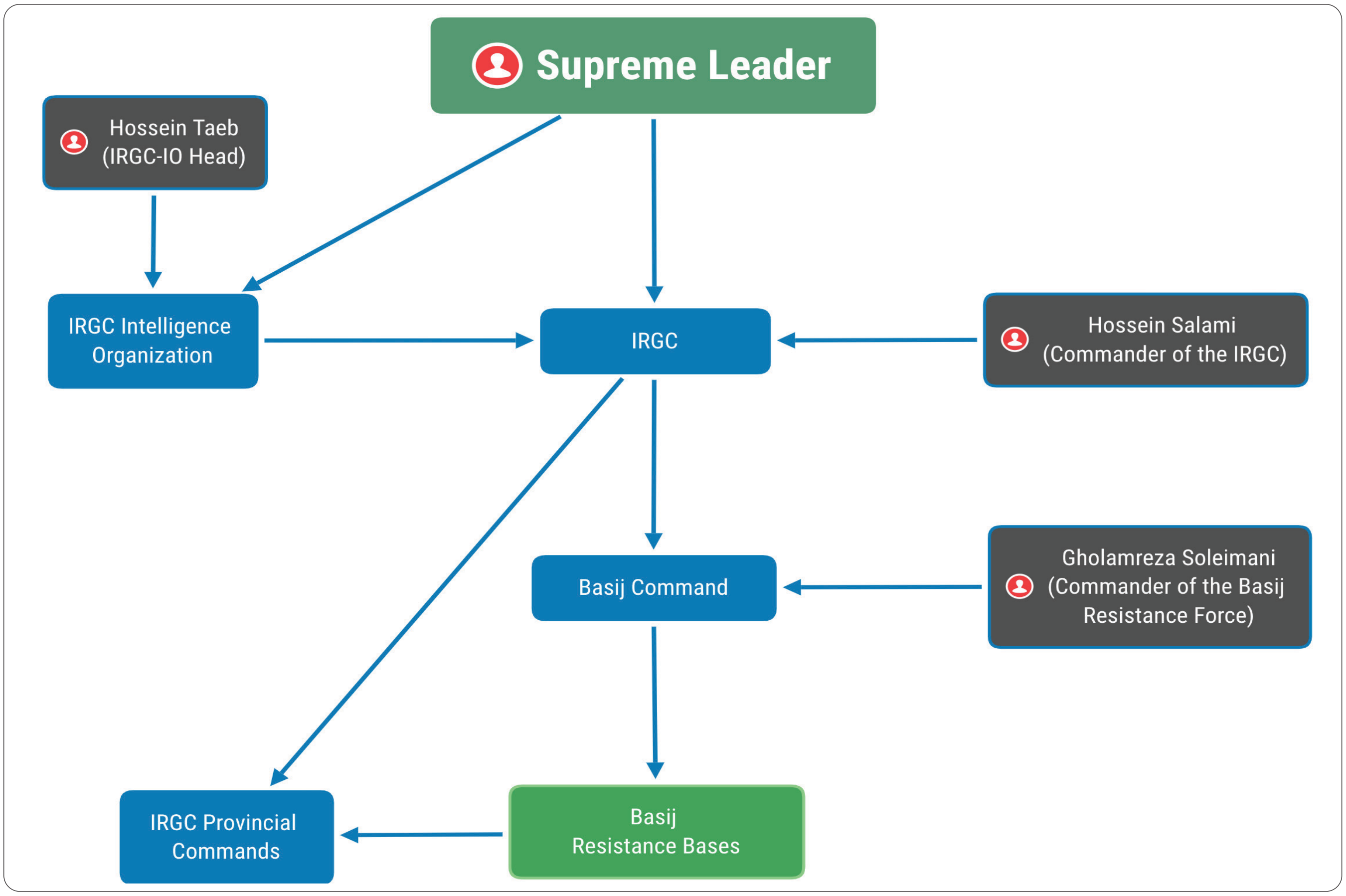
[13] Iran: Cyber Repression, p.40.

[14] S.Golkar, Captive Society: The Basij Militia and Social Control in Iran, New York, Columbia University Press, 2015, p.55.

Based on the IRGC's 2008 provincial reorganization, which resulted in the Basij command's integration into the IRGC command, the security functions of the Basij were altered and transferred to the IRGC's provincial commanders. Industry researchers highlight the relationship between each Iranian province's IRGC command and the respective coordination of activities, including intelligence and cyber, conducted by the Basij's resistance bases.[15]

After the 2009 Green Movement protests, the Basij's responsibilities shifted toward countering the so-called "Soft War" (Jang-e Narm). The Soft War is an ideological tenet backed by Supreme Leader Khamenei, which manifests as political, economic, societal, and cultural threats that can undermine the stability or alter the ethos of the Islamic Republic.[16] Industry researchers have depicted the broad nature of Tehran's cyber response to the soft war, pegging malware such as Infy to the operations of APT groups like Rocket Kitten, among others, to counter dissidents. Pro-government outlets, such as the FARS News Agency, also highlight the nature of the soft war, and how virtual media, including internet news groups like BBC-Persian and RadioFarda, as well as Persian-language satellite channels play a significant role in reaching domestic audiences to undermine the regime.[17]

[15] Ibid. p.31-35
[16] http[:]//farsi.khamenei[.]ir/newspart-index?tid=2748
[17] https[:]//www.farsnews[.]com/news/13910604001358


Supreme Leader
Hossein Taeb (IRGC-IO Head)
IRGC Intelligence Organization
IRGC
Hossein Salami (Commander of the IRGC)
Basij Command
Gholamreza Soleimani (Commander of the Basij Resistance Force)
IRGC Provincial Commands
Basij Resistance Bases

Strategic-level command structure of the Basij Resistance Forces.

The Basij's offensive cyber function was cited in a BBC report quoting former IRGC Mohammad Rasoolallah Corps (Tehran) commander Hossein Hamedani. Hamedani (also known as Abu Wahab), is reported to have directly served under Suleimani, and was responsible for all Syrian operations until his death in October 2015, in a battle near Aleppo against the Islamic State (IS). Hamedani claimed in December 2010 that Iran's Basij Cyber Council utilized members of Iran's hacker community to conduct intrusion operations, which included email compromises and website defacements. However, it is currently unclear whether cyber operations are executed at the Basij's declared operational sites.[18]

[18] https[:]//www.tasnimnews[.]com/fa/news/1395/05/21/1155366

Pro-government open source reports also cite the Basij's role in Iran's information operations under the scope of the soft war, as specified by former deputy commander of the Basij, Brigadier General Ali Fazli.[19] A cadre dubbed the "Officers of the Soft War" (Afsarane Jang-e Narm) is trained in information warfare skills across Basij military bases.[20] Among others, this effort is also supported by Iran's Seraj Cyber Organization, which reportedly helps coordinate various federal training efforts. Pro-government outlets depict the existence of an operational site dubbed the "Basirat Base" (Insight Base) from where content is purportedly developed to support Iran's information operations efforts. We assess the Basirat Base model to be one of many operational networks that contribute to Iran's information operations.

The Basij is also reported to contribute to the IRGC's overall recruitment effort as it pertains to cyber and technical capability development. Industry research indicates that the Basij's recruitment model is stratified into at least five separate tiers; these include "Special Basij," "Cadre," "Active," "Regulars," and "Potential."[21] The five tiers allegedly contribute to the IRGC's overall intelligence collection missions, and these are dubbed "Ashraf" (responsible for intelligence surveillance) and "Ayoun" (responsible for physical patrol). We assess the former is likely to contribute to the broader soft war, as they are responsible for identifying social and cultural threats.

Those recruited under the Specialist tier attend an IRGC military academy — for example, the Imam Hossein Military Academy, or the Basij's own alleged academy at Shahid Motahari University — to undergo specialized training in intelligence, counterintelligence, and information and communications technology, among other topics.[22] At the time of this writing, the Imam Hossein Military Academy is reportedly headed by Brigadier General Fazli (the former deputy commander of the Basij).

[19] http[:]//basij18karajamozesh.blogfa[.]com/post/420
[20] https[:]//www.farsnews[.]com/news/13951106000986
[21] S.Golkar, Captive Society: The Basij Militia and Social Control in Iran, New York, Columbia University Press, 2015, p.51.
[22] Ibid. 51.

University	Domain	CIDR Block	Notes
Imam Hossein University	ihu[.]ac[.]ir	217.218.175.0/24	N/A
Shahid Motahari University	motahari[.]ac[.]ir	46.209.144.0/24	Respina Networks (AS42337)

Information on Iranian universities associated with the IRGC and Basij.

Notwithstanding the activity surrounding the Basij, we have not established a link between the organization and a threat actor group as of this writing. However, we assess the recruitment from the Basij corps to the IRGC makes it likely that its members do participate in operations with, and probably staff, contracting groups that service the latter.

Ministry of Intelligence and Security (MOIS)

The Ministry of Intelligence and Security (MOIS), established in August 1984, is the primary intelligence agency in Iran. The agency, according to the Islamic Republic's Constitution, is responsible for foreign intelligence collection and countering domestic subversion. As briefly alluded to in earlier sections of this report, the agency has had to contend with the rise of the IRGC's intelligence capability, after MOIS was viewed by the hardline movement, including the Supreme Leader, as pivoting toward reformism while under former president Khatami. Although MOIS is a portfolio agency of the sitting president, like other Iranian security organizations, a representative office of the Supreme Leader exists inside the agency and ensures MOIS is within immediate reach of Khamenei. Intelligence Minister Mahmoud Alavi is a prominent stakeholder in various intra-governmental bodies including the SNSC, the Council for Intelligence Coordination, and a host of foreign intelligence councils.

Public reporting on the agency has shed light on various aspects of its organizational structure, politics, and scope. According to a 2012 report from the U.S. Library of Congress, MOIS is reported to have at least 15 directorates. Among them are a directorate for counterintelligence, technology, foreign operations, and security, which we assess are most likely to conduct or maintain oversight of international cyber operations. The information sourced by the Library of Congress is widely distributed across apparent diaspora Farsi- and Kurdish-language news websites such as "Pezhvak Iran" (پژواک ایران).

MOIS's domestic responsibilities include the oversight of ethnic minorities, the detection of dissidents, the targeting of terrorist organizations, and the trafficking of narcotics. Regarding foreign operations, MOIS is primarily responsible for gathering intelligence and conducting misinformation and propaganda campaigns. According to World Security Network, "the priorities of MOIS in foreign operations are: to monitor, infiltrate, and control dissident Iranian groups; to initiate connections and networks for an increased influence; to carry out terrorist and military operations; to identify any type of foreign threat, especially the ones connected to Iran's nuclear program and presently focusing on Israel and USA; to disseminate false intelligence (misinformation) in order to protect Iran and its future interests; to acquire new technologies for defense as well as spare parts for the existing equipment."

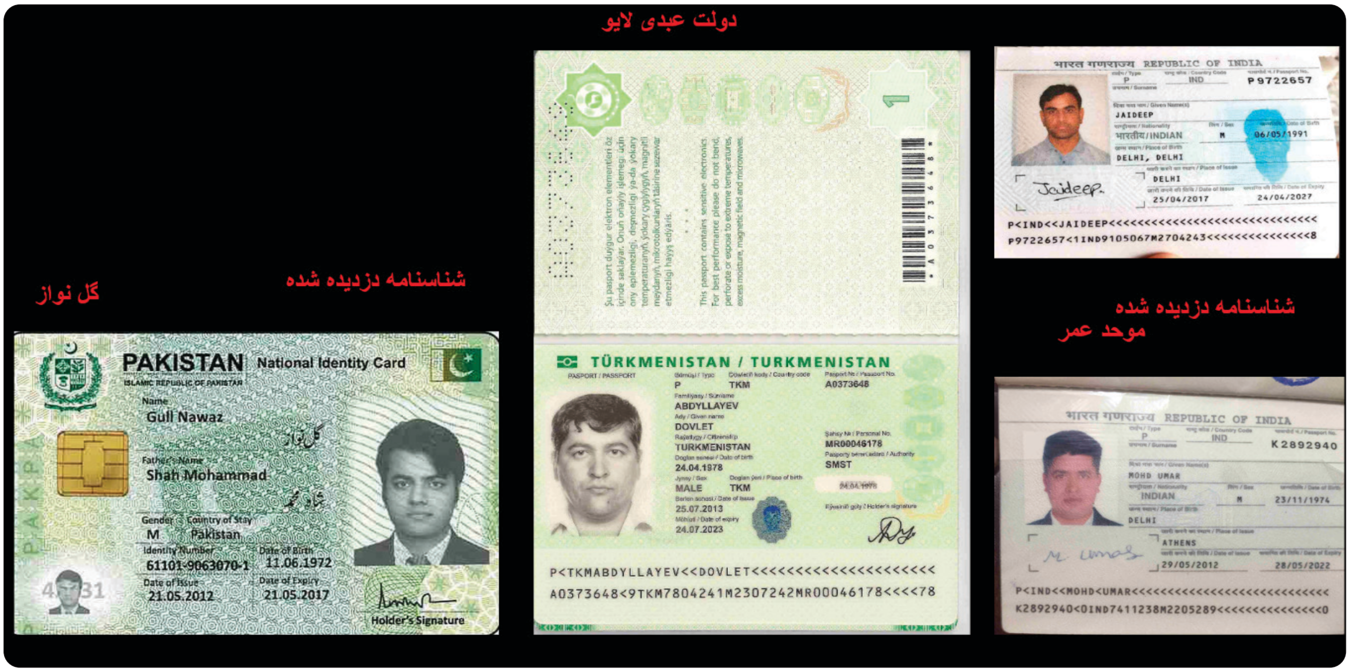
Magic Kitten

Magic Kitten is an Iranian threat actor believed to be affiliated with MOIS. Magic Kitten was first observed deploying malware in 2007, and has a record for conducting cyberespionage operations against various industry verticals. This group is believed to primarily target dissidents inside Iran, as well as the country's regional rivals. However, Magic Kitten has also been observed targeting North America, Europe, and various Middle Eastern and Southeast Asian countries. Research from the Carnegie Endowment for International Peace suggests MOIS is likely to have also collaborated with Iranian proxy force Hezbollah to pursue Lebanese targets and other victims of interest.

RANA Institute

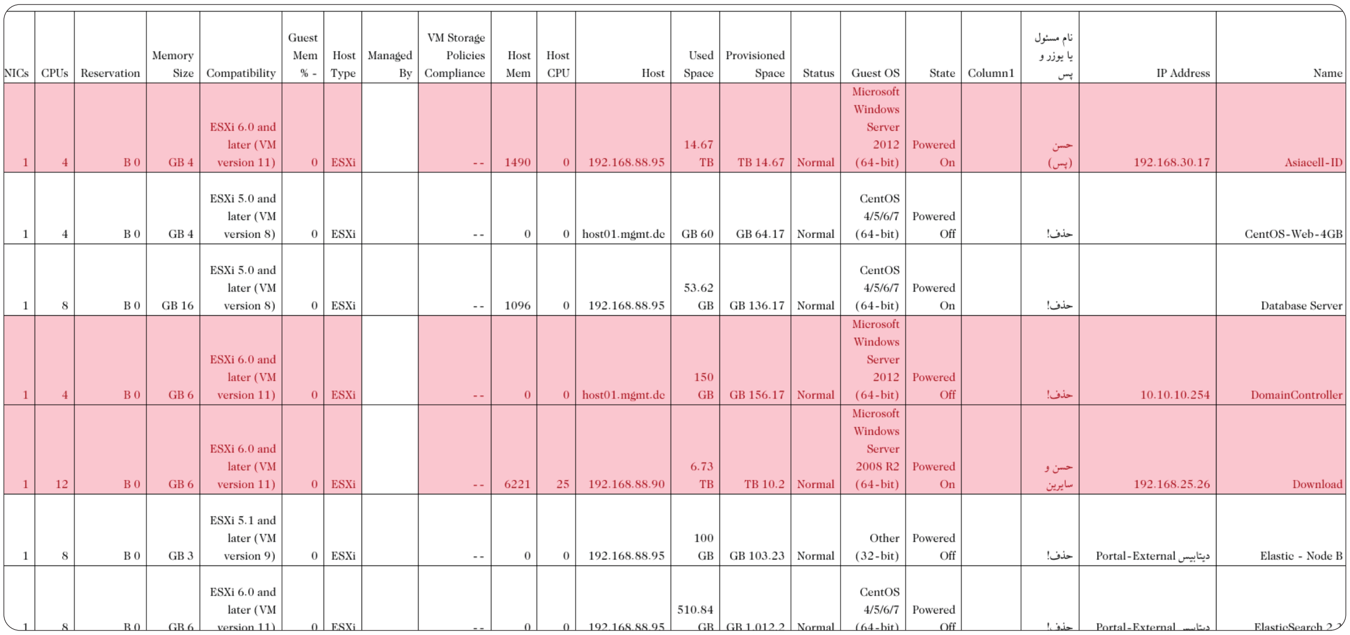
In March 2019, the entity known as Hidden Reality disclosed information on the Rana Institute, which highlighted information on the organization's reported association with the Iranian cyber program. According to leaked documents, the Rana Institute is a contracting group hired by MOIS to conduct cyberespionage operations. The leaked information suggests the Rana Institute is split into two branches. The first branch is focused on cyberespionage, and their activities primarily center on the development of malware and tools; while the second group reportedly is focused on social engineering and spearphishing targets.

Rana primarily targeted Iranian and foreign databases that were storing confidential information. Although it used a variety of TTPs, its main tactic included pilfering and using valid credentials to lead intrusions against its intended victims. Reportedly, Rana's attackers led various spearphishing and SQL injection attacks to gain initial access and acquire valid credentials. Rana was observed mainly targeting government agencies, airlines, telecommunication, and IT companies. The most affected region by Rana cyber operations was Asia, with approximately 22 countries targeted. In addition, six countries in Africa were affected along with Fiji, New Zealand, Australia, and Colombia. We also highlight that Rana is accused of targeting Iranian citizens as well. We observed various databases with personally identifiable information (PII) associated with Iranian nationals. Although we can not fully ascertain the motive for such targeting, it is possible that the collection of such information is potentially connected to counterintelligence operations.



Among the many details raised by Hidden Reality was Rana's alleged involvement in pilfering passport information from regional countries.

Based on a May 2019 report, ClearSky documented Rana's objectives, which included "developing technological knowledge and capabilities" and also "conducting a cyber and intelligence warfare with the rest of the world." Rana employees were reportedly experts in a variety of technical fields, such as encryption and malware analysis and development; they were also reportedly versed in multiple foreign languages as well as computer languages, including HTML, HTML5, CSS, PHP, Python, Scala, Ruby on Rails, SPT, .NET, Javascript, SQL server, MySQL, Oracle, and NoSQL.



NICs	CPUs	Reservation	Memory Size	Compatibility	Guest Mem % -	Host Type	Managed By	VM Storage Policies Compliance	Host Mem	Host CPU	Host	Used Space	Provisioned Space	Status	Guest OS	State	Column1	نام مسئول یا یوزر و پس	IP Address	Name
1	4	B 0	GB 4	ESXi 6.0 and later (VM version 11)	0	ESXi		--	1490	0	192.168.88.95	14.67 TB	TB 14.67	Normal	Microsoft Windows Server 2012 (64-bit)	Powered On		حسن (پس)	192.168.30.17	Asiacell-ID
1	4	B 0	GB 4	ESXi 5.0 and later (VM version 8)	0	ESXi		--	0	0	host01.mgmt.dc	GB 60	GB 64.17	Normal	CentOS 4/5/6/7 (64-bit)	Powered Off		حذف!		CentOS-Web-4GB
1	8	B 0	GB 16	ESXi 5.0 and later (VM version 8)	0	ESXi		--	1096	0	192.168.88.95	53.62 GB	GB 136.17	Normal	CentOS 4/5/6/7 (64-bit)	Powered On		حذف!		Database Server
1	4	B 0	GB 6	ESXi 6.0 and later (VM version 11)	0	ESXi		--	0	0	host01.mgmt.dc	150 GB	GB 156.17	Normal	Microsoft Windows Server 2012 (64-bit)	Powered Off		حذف!	10.10.10.254	DomainController
1	12	B 0	GB 6	ESXi 6.0 and later (VM version 11)	0	ESXi		--	6221	25	192.168.88.90	6.73 TB	TB 10.2	Normal	Microsoft Windows Server 2008 R2 (64-bit)	Powered On		حسن و سایرین	192.168.25.26	Download
1	8	B 0	GB 3	ESXi 5.1 and later (VM version 9)	0	ESXi		--	0	0	192.168.88.95	100 GB	GB 103.23	Normal	Other (32-bit)	Powered Off		حذف!	Portal-External دیتابیس	Elastic - Node B
1	8	B 0	GB 6	ESXi 6.0 and later (VM version 11)	0	ESXi		--	0	0	192.168.88.95	510.84 GB	GB 1,012.2	Normal	CentOS 4/5/6/7 (64-bit)	Powered Off		حذف!	Portal-External دیتابیس	ElasticSearch 2.2

Rana's alleged operational servers disclosed by Hidden Reality.

Although the verification of Hidden Reality's reporting on the Rana Institute remains inconclusive as of this writing, Rana's operations are at a minimum, suggestive of a highly specialized contractual relationship with MOIS, and of a multifaceted in-house malware research and development and attack capability.

RANA and Potential Links to Iranian Universities

From their May 4 postings, the predominantly Farsi-language, self-declared dissident outlet Black Box unveiled the identities of Rana Institute employees, their positions, and additional affiliations. These affiliations were mostly in connection to Iranian universities. According to the leaks, a variety of Rana employees were also faculty or previous students at these institutions; and through their proximity to students and faculty in these universities, Rana employees had the capability to conduct domestic espionage operations. Based on Black Box posts, Recorded Future analysts observed seven universities affiliated with Rana employees:

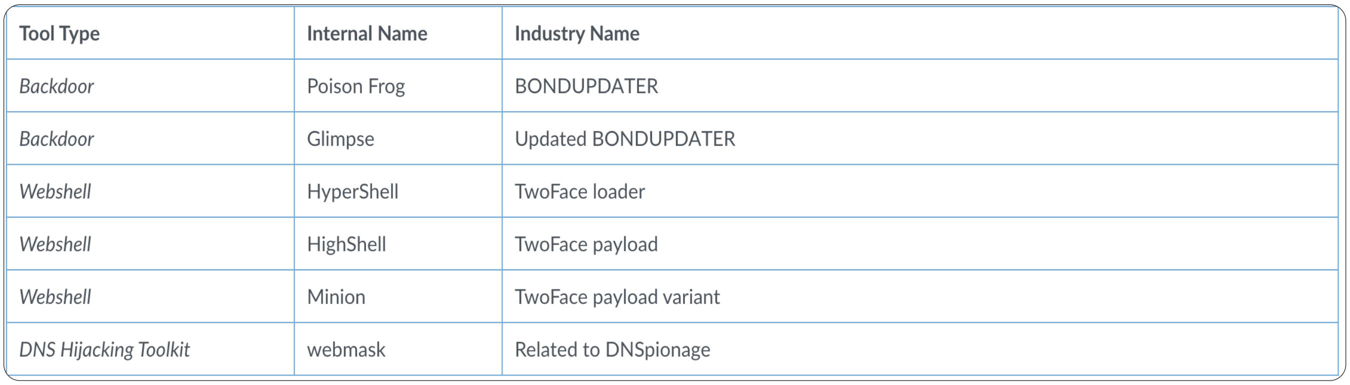
1. Urmia University
2. Isfahan University
3. Shahid Beheshti University
4. University of Tehran
5. Amirkabir University
6. Tarbiat University
7. Sharif University

University	ASN	CIDR Block	Notes
Urmia University	AS58224	78.38.25[.]0/24	N/A
Isfahan University	AS6736	94.0.0[.]0/8	IP address 94.184.92[.]211 observed communicating with malicious executable with SHA-256 hash: e61806c29c395a6683c35cd4759ffff880d2d3f1cba85cd09094846c018d3282 on September 9, 2019. According to Recorded Future and VirusTotal, this hash is associated with the Wannacry ransomware.
Shahid Beheshti University	AS56765	194.225.24[.]0/22	N/A
University of Tehran	AS29068	80.66.176[.]0/20	N/A
Amirkabir University	AS59794	185.211.88[.]0/24	N/A
Tarbiat University	AS57745	194.225.166[.]0/24	N/A
Sharif University	AS12660	81.31.186[.]0/24	N/A

Major Iranian institutions with credible links to their cyber program.

APT34 Leaks

In a March 2019 Telegram post, Lab Dookhtegan claimed that MOIS was using APT34 tools to conduct cyberattacks and espionage operations against Iran's neighboring countries. These tools included TwoFace, BONDUPDATER, and DNSpionage. In late April, Unit 42 discovered that APT34 had their own naming conventions for these tools to include names such as "Hypershell," "PoisonFrog," and "Glimpse."



Tool Type	Internal Name	Industry Name
Backdoor	Poison Frog	BONDUPDATER
Backdoor	Glimpse	Updated BONDUPDATER
Webshell	HyperShell	TwoFace loader
Webshell	HighShell	TwoFace payload
Webshell	Minion	TwoFace payload variant
DNS Hijacking Toolkit	webmask	Related to DNSpionage

APT34's naming convention.
(Source: PaloAlto Unit 42)

According to late March posts, Lab Dookthtegan revealed that MOIS deployed APT34 tools, mostly to target domains belonging to the governments of countries neighboring Iran. Most of these victims were targeted specifically for their usernames and passwords. In the table found in Appendix A, Recorded Future has provided a sample of the targeted domains found in the Lab Dookthtegan leaks. Analysts provided the domains, associated IP addresses, entities, description, and hashes. Based on our analysis, primus.com[.]jo was the only domain with links to APT34's OILRIG malware. This domain was associated with two SHA-256 hashes that were linked to OilRig as of June 4, 2019.

In addition to the aforementioned tools, security researchers also discovered APT34's use of a tool dubbed "Jason," used to hijack Microsoft Exchange email accounts. The Jason tool is a GUI utility for brute-forcing Microsoft Exchange email servers using pre-compiled lists of username and password combinations. After analyzing the Jason tool, researchers believe that it seems to be a simple brute-force attacker for use against online exchange services. In a scan performed on VirusTotal, a file with the hash 9762444b94fa6cc5a25c79c487bbf97e007cb680118afeab0f5643d211fa3f78 (Jason.exe), produced a rate of 42/71 detections.

Campaign Against the US Government

In late January 2020, Intezer researchers discovered a phishing campaign targeting U.S. federal government workers for the likely purpose of compromising government networks. This campaign has been linked to APT34, who disguised the phishing campaign as Westat surveys. According to ZDNet, "Westat is a well-known U.S. government contractor that has managed and administered surveys to more than 80 federal agencies, for at least 16 years, querying federal workers on working conditions, management, and job satisfaction."

Within the disseminated emails, APT34 actors attached malicious Excel files that contained a backdoor named TONEDEAF and a stealware named VALUEVAULT. These variants have been previously documented in a July 2019 report from FireEye. Although both malware were found in the recent 2020 campaign, researchers note that APT34 actors considerably updated TONEDEAF and VALUEVAULT from their previous forms.

The time frame of the Westat phishing campaign is unclear, according to Intezer researchers. However, they remain confident that the campaign is ongoing and possibly targeting organizations outside of the U.S. government. Specifically, Intezer suspects that APT34 is targeting commercial organizations that are affiliated with Westat services.

Fox Kitten Campaign

In an operation dubbed Fox Kitten, Iranian APT groups have been observed exploiting unpatched Fortinet, Pulse Secure, and Palo Alto Networks VPN servers, as well as Citrix remote gateways. Impacted sectors include IT, telecommunications, energy, aviation, and government agencies. ClearSky researchers reported that targets were in the U.S., Israel, Australia, Saudi Arabia, Lebanon, Kuwait, the United Arab Emirates, as well as several other European countries. The operators successfully planted backdoors in VPN servers to establish a foothold within the victim network and then steadily exfiltrated data over time.

ClearSky researchers assessed with "medium-high probability" that APT33 and APT34 shared attack infrastructure. At the time of this writing, Recorded Future analysts cannot validate the accuracy of this information; however, the alleged cooperation between APT34, APT39, and APT33 is dependent on those group's sharing of C2 infrastructure. While we have not detected overlaps between Operation Gamework (initially listed above) and the Fox Kitten campaign, our findings highlight the likelihood that APT33, APT35, and MuddyWater also shared C2s. While we do not claim the parallel observations to be conclusive, we assess the sharing of C2s to possibly indicate that these groups collaborate on operational matters, while at the same time probably responding to different tasking requirements.

Specific vulnerabilities exploited by this campaign include CVE-2019-11510 in Pulse Secure's VPN SSL servers, CVE-2018-13379 in Fortigate's SSL VPN servers, and CVE-2019-1579 in Palo Alto Network VPN servers, all of which ClearSky claims the Fox Kitten campaign is now exploiting. According to Recorded Future analysis, the TwoFace webshell has been observed exploiting CVE-2019-11510. As both APT34 and MOIS have been associated with the TwoFace webshell, Recorded Future analysts assess that either group likely used this tool in the Fox Kitten campaign.

Ministry of Defense and Armed Force Logistics (MODAFL)

The Ministry of Defense and Armed Force Logistics (MODAFL), currently headed by Brigadier General Amir Hatami, was established in 1989. This ministry was created to establish a unified structure for Iran's armed forces, but it has become well known for its control over Iran's ballistic missile program. MODAFL's mission is to organize and manage Iran's defense industries and to facilitate procurement programs in support of plans and objectives determined by the General Staff of the Armed Forces of Iran (GSAF). Unlike other procurement groups which report to the IRGC, MODAFL is a portfolio agency of the Iranian president.

MODAFL is mainly composed of the following subordinates: Iran Electronics Industries, Defense Industries Organization, Aerospace Industries Organization, Aviation Industries Organization, and Marine Industries Organization.

Iran Electronics Industries (IEI)

In late April 2016, the U.S. DOJ charged Mohammad Saeed Ajily and Mohammed Reza Rezakhah with the theft of intellectual property from Vermont-based engineering company Arrow Tech. Rezakhah, an Iranian citizen and hacker, worked under the direction of Ajily. The indictment noted that Ajily and his conspirators circumvented Western-imposed sanctions to obtain intellectual property for Iranian institutions such as Tehran University, the Malek Ashtar Defense University, Sharif Technical University, and Shiraz Electronics Industries (subsidiary of Iranian Electronics Industries).

Iranian Electronics Industries (IEI), a subsidiary of MODAFL, is a prominent producer of electronic components and systems for Iran. In 2008, the European Union linked IEI to Iran's nuclear program; however, IEI also incorporates a variety of responsibilities outside of nuclear development such as information technology, electro-optics, and satellite technology. Although a subsidiary of MODAFL, IEI has eight subsidiaries of its own:

1. Shiraz Electronics Industries
2. Iran Communication Industries
3. Electronic Components Industries
4. Information System of Iran
5. Isfahan Optics Industries
6. Iran Electronics Research Institute
7. Iran Space Industries Group
8. Security of Telecommunication and Information Technology

Aerospace Industries Organization

Iran's Aerospace Industries Organization (AIO) manages the country's missile program and is considered the industrial and military subsidy for MODAFL. According to Iran Watch, AIO has manufactured launchers, anti-aircraft guns, gyroscopes, propellants, warheads for rockets and missiles, and other missile components. They have also produced the following rockets: Haseb, Nader, Oghab, Noor, S24, Saegheh, Fateh, Zelzal, and Nazeat.

AIO has a number of subsidiaries, many of which have been sanctioned by the U.S. Department of Treasury due to their involvement with Iran's ballistic missile program. The following is a listing of AIO's subsidiaries:

- M. Babaie Industries
- Shahid Motahari Industries
- Shahid Shahabadi Industrial Complex
- Techno SANAM Industries
- Fajr Industrial Group
- Naval Defense Missile Industry Group
- Sanam Industries Group
- Shahid Bagheri Industrial Group (SBIG)
- Shahid Hemmat Industrial Group (SHIG)
- Ya Mahdi Industrial Research Complex

In addition, AIO has also been associated with the following front companies:

- Electro Sanam Company
- Ettehad Technical Group
- Helal Co.
- Joza Industrial Co.
- Mizan Machine Manufacturing Group (3MG)
- Safety Equipment Procurement Company
- Shian Co.

Possible Connection to September 2019 Saudi Aramco Attack

In a February 2020 report, Conflict Armament Research (CAR) published their discovery of a device that ties Iran to the Saudi Aramco drone attack in September 2019. In their report, CAR discovered a vertical gyroscope that appeared in the same make (not the same model) of a drone found by Saudi authorities after the Saudi Aramco attack. According to UAV experts, this type of gyroscope has “not been observed in any UAVs other than those manufactured by Iran.” As specified above, AIO primarily manages the manufacturing of military weapons and equipment to include gyroscopes. It is very likely that AIO was involved with the manufacturing of the UAV involved with the Saudi Aramco attack.

Although the September 2019 Saudi Aramco attack remains unattributed, Recorded Future assesses that it is very likely that an Iranian military organization, in particular the IRGC, was involved. As noted above, Iranian nation-state actors have historically targeted Saudi Arabian organizations, specifically Saudi Aramco. In August 2012, Saudi Aramco experienced the most extensive attack in its history when an Iran-nexus group deployed the Shamoon malware to compromise around 30,000 computers. As of late March 2019, Symantec observed APT33 targeting multiple organizations across Saudi Arabia and the U.S. In their same research, Symantec also identified attempts by APT33 to exploit CVE-2018-20250 to target the chemical sector in Saudi Arabia. Despite APT33’s history attacking Saudi Arabian organizations, Recorded Future did not find any evidence tying this threat actor to the 2019 Saudi Aramco attack, nor did analysts discover evidence tying APT33 to AIO.

Defense Contractor Relationships

Defense contractors have long held a vital position in the Islamic Republic's cyber landscape, and open source information continues to support assessments that they provide intelligence, operational, and technical support to Iran's various government and military programs. Furthermore, the system is predominantly serviced by a cadre of contractors who share ideological or organizational allegiances. Dissident sources also highlight that some Iranian information security professionals remain driven by professional ambitions and financial reward, leading them to cooperate with Iran's security services.

In addition to our reporting on Iran's hacker hierarchy, and the above noted cases, reporting points to the overlapping cooperation between contractors and multiple agencies. For example, Net Peygard Samavat Company was listed in a U.S. Department of The Treasury press release sanctioning the entity, but also revealing how it provided services to MOIS, the IRGC-Intelligence Protection Organization, and the IRGC's Electronic Warfare and Cyber Defense Organization (IRGC-EWCD). Furthering the link between contractors, official government organizations, and APT groups, Net Peygard was a company owned by Behzad Mesri ("Sokote Vahshat"). Mesri is an Iranian threat actor with links to Iran's hacker community, and according to the ClearSky group, he is highly likely associated with APT35 (Charming Kitten). Mesri was also named in an unsealed indictment by the U.S. DOJ in November 2017 for helping Iranian military elements to target Israeli infrastructure.

Self-declared anti-government sources also support similar findings which peg the operations of contractors to multiple government entities. These include linking groups such as Kavosh Center and other previously unreported contractors like the "Fater Cyber Center," "Mahak Rayan Afraz," and the "Jawad Al-aimeh Center" to the Iranian cyber program. In some instances, dissidents make assertions that Iranian centers — for example, the Nasr Cultural Center — uniquely serviced the IRGC-QF. In others, a specific contracting body linked to the IRGC-EWCD, and other undefined IRGC groups, have reportedly led an international attack operation involving the deployment of the Shamoon wiper malware. In at least one of these organizations, uniformed IRGC officers are reported to have led research and development activities.

One example is the MABNA Institute (also known as Silent Librarian, Cobalt Dickens, and TA407). Public information highlights the role this group played to illicitly procure more than 31.5 terabytes of scientific information and intellectual property to service Iranian government, military, and private interests. MABNA's actions reveal the enduring threat posed by contractors looking to operate on a for profit basis inside Iran. Groups like MABNA are likely to continue to surface as the IRGC and other elements inside the Iranian government seek to fill technology gaps through espionage operations.

Ideology is also a characteristic influencing threat actors like MABNA. One of the indicted members of the MABNA group, Abuzar Gohari Moqadam, maintained a public posture as a presumed faculty member of the Imam Sadiq University Political Science Department.[23] Moqadam was interviewed by Iranian press in June 2017, where he advocated for the reversal of the JCPOA and a return to nuclear research if other parties to the agreement reneged on their agreements.[24] Moqadam further argued against any ensuing negotiations regarding Iran's ballistic program and regional operations, which highlights his likely ideological allegiance to the IRGC. Moqadam did not contribute to the technical operations of MABNA and was an end-user of stolen credentials. His association to MABNA highlights the role that ideology can play in cybercriminal conspiracies.

While we cannot corroborate the reporting issued by dissident sources, our assessment of Iranian cyber contracting groups supports analysis suggesting they likely service multiple agencies and military organizations. Contracting groups are also likely to cater to agency-specific tasking depending on the threat and target of opportunity.

[23] https[:]//parstoday[.]com/fa/iran-i81358
[24] Ibid.

Outlook

Iran's cyber actors are uniquely placed to continue to deflect attribution attempts, primarily due to the increasing number of actors catering to Iran's different intelligence centers. Whether the IRGC-IO, the Quds Force, MODAFL, or MOIS, the entities remain at the forefront of Iranian cyber capabilities, and are able to lead international attacks. Public information also points to these entities using a community of contractors to pursue their intelligence targets, and we assess this to remain a significant characteristic of Iran's cyber ecosystem in the future.

With a more skilled cyber cadre, more effective tooling, and more robust operational security measures, including the ability to produce and distribute disinformation, Iranian cyber operations are likely to continue to swiftly target Middle Eastern nations and the international community as a whole. Iran's security services will also highly likely continue to target Iran's diaspora and ethnic minority communities, both of which pose a threat to Tehran's perceived domestic stability.

Mitigations

- Interested stakeholders should leverage structured analytic techniques, such as red hat analysis and deception detection, to aid in more refined attribution attempts, while also mitigating disinformation efforts by cyber adversaries.
- Remain abreast of political developments in Iran to observe activities that impact the intelligence landscape (such as corruption scandals, power struggles, arrests of journalists and activists, reshuffling leaders of intelligence groups, use of foreign technologies, prohibition of the use of social media, and so on).
- Farsi-language dissident reporting regularly covers activities pertinent to crackdowns against minority groups, protestors, and arrests of foreign and dual nationals. These sources also usually provide insight into the intelligence and military organizations involved in the arrests and their claimed motives.

- Iranian cyber operators maintain a relatively public presence on Instagram, and Telegram. These public sources may provide insight into the organizational developments, training, political insight, and their operational network.
- To prevent and mitigate disinformation efforts, we recommend verifying and corroborating Iranian cyber developments sourced from social media and publicly-available messaging platforms.
- Campaign tracking of Iranian APT groups will not only provide insight on the TTPs, but also the victimology, which serves to deepen understanding about organizational interests.

Appendix A — Sample of Domains Targeted by MOIS

Below is a sample of targeted domains found in the Lab Dookhtegan leaks. These leaks were disseminated in late March 2019 via Telegram. Analysts provided the domains, associated IP addresses, entities, description, and hashes.

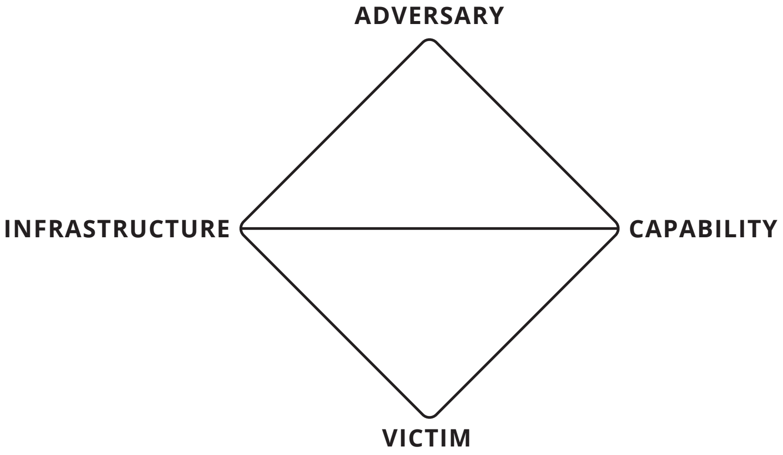
Domain	IP Address	Entity	Description of Attack	Hashes
primus.com[.]jo	143.95.251[.]23	Jordanian software company	Webshell URL	SHA-256: cb43574187ef2d102d81efe5648ab1c7e5d93f5badf856894a0fdb0d78bd495d (OILRIG trojan) SHA-256: 9da0fb8abed112d4ef75a49a3f34d69e3f7ef6e29fd0e743fdcf64615307b942 (OILRIG trojan)
mopa[.]ae	213.42.174[.]226	Ministry of Presidential Affairs	N/A	SHA-256: d175faf269eb07ea784224e9a92f6bfde5ec5c422a7b3c953b03b3bf90c7d999 (Androm trojan)
dmi[.]ae	80.227.111[.]126	Dubai Media Inc.	Gathered over 250 usernames and passwords	SHA-256: 0e733b22d26664f63044e01ed14c370294a13c247ca74f11bf7fdab8689d48b0 (Tofsee trojan) SHA-256: ee8d717457d30c46cca44e7caca9e2321e178955eed46d5e571d94501005e3d1 (Tofsee trojan) SHA-256:6fae8029a36a6353f2ba16a7cac3a6b68a795e2aaef39f7c634006f59f21c7ee (Tofsee trojan)

Domain	IP Address	Entity	Description of Attack	Hashes
nitc.gov[.]jo	193.188.66[.]185	National Information Technology Center in Jordan	Gathered server information, users, passwords, URLs, IP addresses	SHA-256: 3705a4e099cb277b1ebea39372ae47e6f62fc36f26da058fd79bf210de64cd7d (Rdn trojan) SHA-256: 22bed99dae01743535ef18d51e3ab7c5ef2248a418ae9760e21bd4fc3dc42f4c
adac[.]ae	37.218.224[.]54	Abu Dhabi airport	Webshell URL over 900 usernames and passwords	One detection of phishing; no hashes observed
etihad[.]ae	87.201.129[.]84	Etihad Airways	Webmail over 10,000 usernames and passwords	17 hashes observed — three below were from emails; however, analysts did observe hashes that were related to Tofsee and Kryptik SHA-256: 11ed7153bd6402bfba1651de928753f8af37c1c69ce9d6a90f89221a4b56f52f SHA-256: cafe4ab80f58f0363566f136ae35e1c61f2d3e101e060528ed6aa243a735a484 SHA-256: a8168b8e5f3533a39a808c8e1d8888e91c575e6d1253e7a882ad7ea624ccae6a
epc[.]ae	162.13.207[.]114	Emirates Policy Center	Passwords for admins and system users	N/A
nbrri.gov[.]ng	192.3.137[.]194	Nigerian Building and Road Research Institute	SQL injection to gather usernames and passwords	Five malicious URLs observed
nsa.gov[.]bh	193.188.115[.]251	National Security Agency of Bahrain	Gathered more than 30 users and passwords	N/A
cdhq.gov[.]ae	N/A	Ministry of Interior - UAE, MOI Abu Dhabi, MOI, United Arab Emirates	Gathered information for the IP server, usernames, and passwords	N/A
enoc[.]com	45.60.112[.]182	Emirates National Oil Co.	Use of “several mimikatz computers”	SHA-256: 2296fa9be04e48dd5057a27a1e17b09a486021e9fa8ba4c5bc797707a8332c5c SHA-256: 216a2f63af8d3b3e55340f79af25214b7815c4544f6e809d13684d2774cb36f6 (Arc Trojan) SHA-256: 5cd15abae8db8915efcbb16cb942b1bcb5cc5a434eac60394bbb51ab8c03983f (Fareit trojan) SHA-256: 3fbc4106618c7c97d664b8b3a2385de6e6a6da7006fe1cc261bd095bfe007d86 (Kryptik)

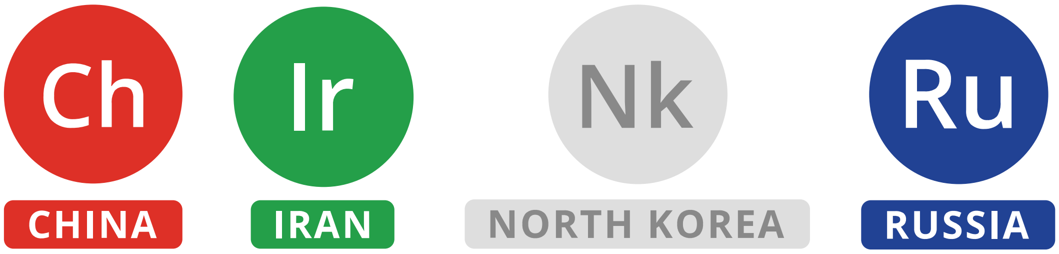
Domain	IP Address	Entity	Description of Attack	Hashes
fcsa.gov[.]ae	185.54.19[.]170	Emirates Federal Competitiveness and Statistics Authority	یارب اهدروسپ رد نارباک	N/A
da.gov[.]kw	40.113.150[.]45		Mimikatz computers	One hash related to generic malware
pmo.gov[.]ae	N/A	Emirates Prime Minister Office	Gathered usernames and passwords	One hash related to generic malware
scad[.]ae	185.66.17[.]154	Statistics Center - Abu Dhabi	Gathered passwords for administrators and IT staff	N/A
admincourt.gov[.]om	82.178.124[.]58	Oman Administrative Court	N/A	N/A

Recorded Future Ontology

Recorded Future's Insikt Group tracks threat activity associated with new and existing threat actor groups, focusing on China, Iran, Russia, and North Korea. Insikt Group only names a new threat actor group or campaign when analysts have data corresponding to at least three points on the Diamond Model of Intrusion Analysis with at least medium confidence, and only when we can point to a handle, persona, person, or organization responsible. We will write about the activity as a campaign in the absence of this level of adversary data. We use the most widely-utilized or recognized name for a particular group when reporting and researching known threat actor groups.



Insikt Group utilizes a simple color plus phonetic naming convention for new threat actor groups or campaigns; we will utilize the most common name when an actor or campaign is already known. The first word in the convention will be a color, currently corresponding to the below, with more color/nation pairings to be added as we identify and attribute new threat actor groups associated with new nations.



About Recorded Future

Recorded Future arms security teams with the only complete security intelligence solution powered by patented machine learning to lower risk. Our technology automatically collects and analyzes information from an unrivaled breadth of sources and provides invaluable context in real time and packaged for human analysis or integration with security technologies.