

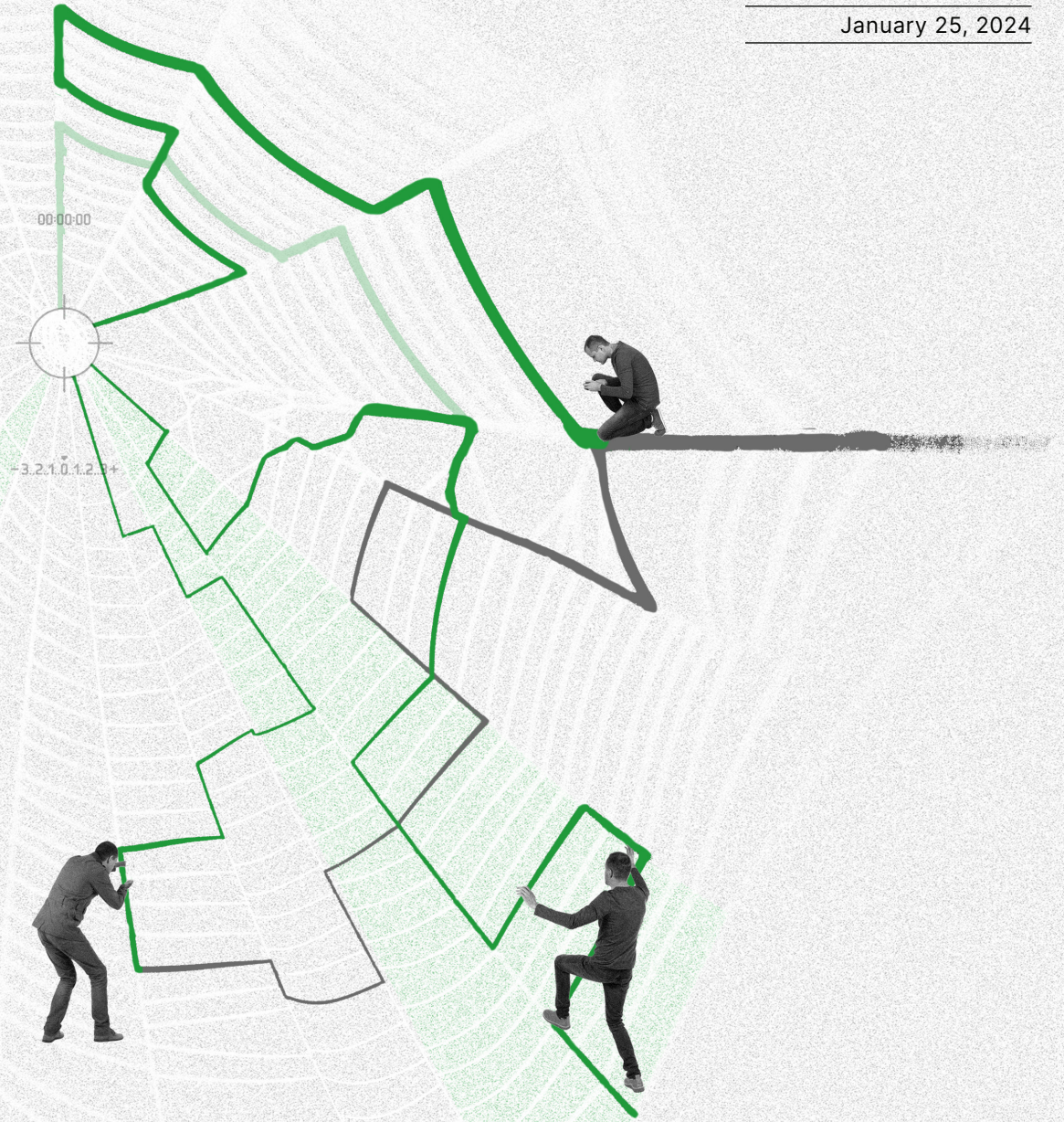
CYBER
THREAT
ANALYSIS

IRAN

Recorded Future®

By Insikt Group®

January 25, 2024



Leaks and Revelations: A Web of IRGC Networks and Cyber Companies

Executive Summary

The Iranian intelligence and military organizations, contractors, and persons of interest discussed in this report are responsible for targeting the democratic process within Western countries, such as the 2020 US presidential election. They are associated with, if not directly complicit in, the targeting of industrial control systems (ICS) in the US and around the world, they have targeted major US financial institutions, and they have led global ransomware attacks against various industries, including healthcare providers like children's hospitals. They also combine information operations with cyber intrusions to foment instability in target countries, including the targeting of Western media organizations. Moreover, some Iranian intelligence and military contractors have been linked to the development of technologies that enable surveillance activity that contributes to human rights abuses. In their totality, the activities of the contractors discussed in this report represent efforts by elements of the Iranian military and intelligence establishments, specifically the Islamic Revolutionary Guard Corps (IRGC), to use an array of cyberattack capabilities against geopolitical rivals and adversaries of Iran.

The doxxing and leaks discussed in this report have revealed a network connecting contractors with senior figures within Iranian intelligence. To date, the operations have adversely affected the operational security of contractors like "Ayandeh Sazan Sepehr Aria Company", "Sabrin Kish", "Soroush Saman Company", and other sanctioned entities like "Najee Technology Hooshmand Fater LLC (Najee Technology)" and "Emen Net Pasargad", which are reported to have been involved in international attack operations at the behest of the IRGC.

The leaks portray a long-standing relationship between intelligence and military organizations and Iran-based contractors. Public records point to an ever-growing web of front companies connected via individuals known to serve various branches of the IRGC (see **Appendix A** through **Appendix E**). We have observed overlaps between personnel members, regularly referred to as "board members", who share roles in different contracting companies. Some of the data reveals names of high-ranking IRGC officials purportedly responsible for leading and coordinating Iran's offensive cyber ecosystem. This has included affiliations with organizations like the IRGC Electronic Warfare and Cyber Defense Organization (IRGC-EWCD), the IRGC Intelligence Organization (IRGC-IO), and even the IRGC's foreign operations branch, the Quds Force (IRGC-QF).

Research on these groups has also highlighted financially motivated activities outside of Iran's borders that formalize the exportation of cyber technologies. While public information is still limited on this front, the cases identified in this research suggest that contractors rely on the IRGC-QF to penetrate the highest levels of government to engage in presumably lucrative arrangements. This has reportedly included the sale of services and technology in countries like Iraq, Syria, and Lebanon.

US government indictments and subsequent sanctions efforts continue to be an effective mechanism for pressuring Iranian contractors and associated personnel, due to the financial and legal repercussions as well as the negative public relations outcomes. The research in this report can assist governments in grasping the growing body of contracting parties and persons that are associated with the IRGC's cyber-espionage, destructive, and disruptive remits.

Key Findings

- There are 4 known intelligence and military organizations linked to the IRGC that engage with the bulk of cyber contracting parties. These include the IRGC-EWCD, the IRGC-IO, the IRGC's Intelligence Protection Organization (IPO), and the IRGC-QF.
- The concept of a "cyber center" affiliated with specific military and intelligence contractors is highlighted by various anti-government dissident groups. Insikt Group has observed specific references to centers that serve the IRGC-IO. These likely act as firewalls to guard the sponsoring organization.
- Research on the personnel links has revealed an expansive network of senior figures linked to contracting parties that are affiliated with companies and persons sanctioned by the US, the European Union, and other governments. We have observed likely high-ranking figures affiliated with the IRGC linked to cyber-related contracting parties. We assess these relationships to be driven by financial interest.
- Insikt Group research suggests that IRGC-related cyber companies are exporting their technologies both for surveillance and offensive purposes to regional governments and non-state actors. Financially motivated operations that involve the transfer of technologies and software are highly likely led by current and former IRGC personnel.
- Public records of the contracting companies researched as part of this report suggest that company rebranding (a suspected sign of evasion) is a factor. Public sources revealed that contracting parties like "Mahak Rayan Afraz" and Emen Net Pasargad will disband and rebrand in an attempt to obfuscate their activities. Both companies were reportedly liquidated, in June and August 2023, respectively.
- US government indictments are likely proving to be an effective legal and diplomatic tool that affects the public relations of Iranian contractors; this is likely why entities like Mahak Rayan Afraz and Emen Net Pasargad shutter and rebrand every so often. It is likely these efforts also adversely affect contractors' abilities to openly recruit new and skilled labor.
- Iranian anti-government threat actors, hackers, and activists continue to grow in number, and the information shared by these groups is complex yet pivotal to conducting link analysis research on Iran's broader contracting landscape.

Background

Iran's ability to implement cyberattacks and cyber-enabled psychological and influence operations has steadily progressed since Operation Ababil (OpAbabil) and the attacks on the [US financial sector](#) in 2013. At the time, 2 private sector companies were [linked](#) to the attacks: the "Mersad Company" and "ITSec Team". Both ITSecTeam and Mersad were [reported](#) to share organizational links to the Islamic Revolutionary Guard Corps (IRGC / سپاه پاسداران), a [claim](#) the dissident source Roshangarane-Asr also made in December 2015, approximately 5 months prior to the indictment being unsealed to the public.



Figure 1: Roshangarane-Asr named ITSec Team and the Mersad company as being responsible for the Ababil attacks (Source: [Roshangarane-Asr](#))

Continuation of Contractor-Led Operations

More recent examples of reported contractor-led operations include the attempted [interference](#) in the US presidential election of 2020 through the impersonation of the Proud Boys organization by threat actors linked to Emen Net Pasargad (Emennet Pasargad/ ایمن نت پاسارگاد). Since 2020, a slew of ransomware-style [operations](#) have also been launched against Israeli entities, each depicting the use of the hack-and-leak extortion model to seed panic against the targeted organizations. In May 2023, Microsoft linked some of these "fronts" to threat actors highly likely operating as [contracting parties](#) (including Emen Net Pasargad).

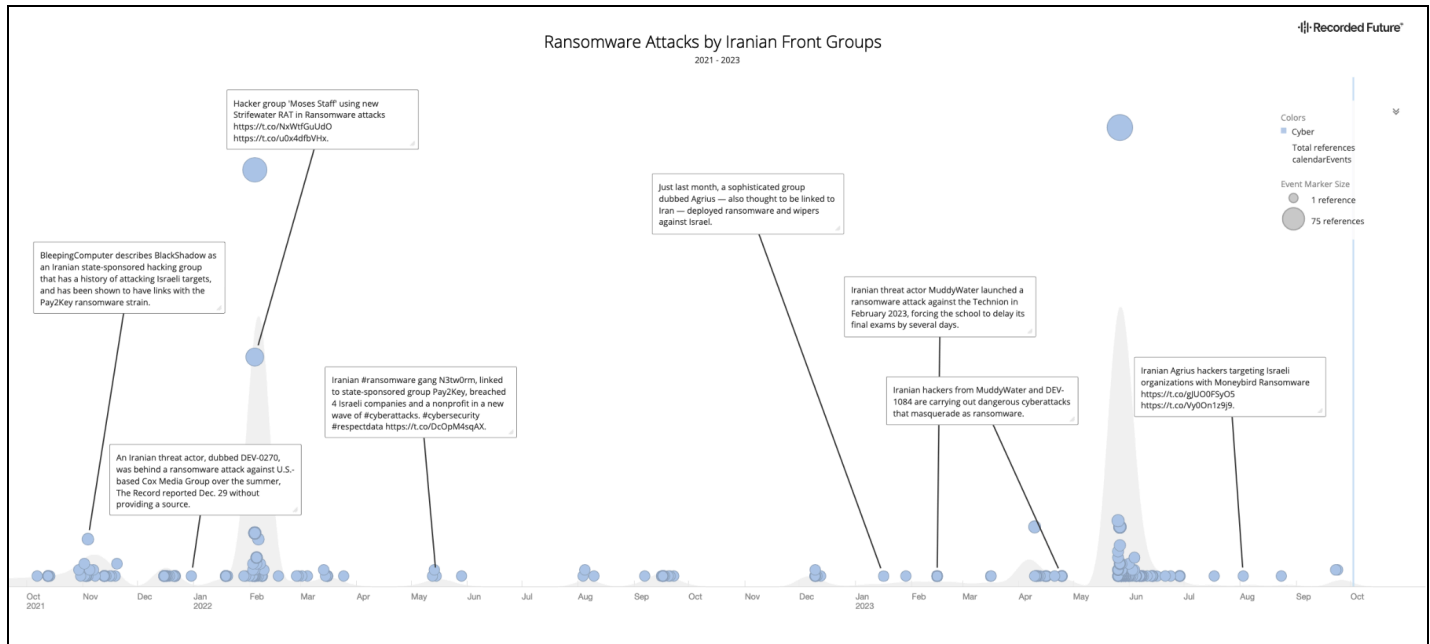


Figure 2: Major ransomware-style attacks led by pro-Iranian government fronts like Moses Staff, N3tw0rm, and Agrius (Source: Recorded Future)

The Human Factor

Since 2015, a slew of anti-Iranian government hacktivists and activists have steadily emerged. Among them are better-known groups like “Lab Dookhtegan”, “Tapandegan”, “AahackSecTeam” (now likely defunct), “Edalat-e Ali”, and “Roshangarane-Asr” (also likely defunct). Throughout 2022 and since the killing of Mahsa Amini and the ensuing anti-government uprising in 2023, new groups like “Black Reward”, “GhyamSarnegouni” (aka Ghyam ta Sarnegouni), and “Bakhtak” have arisen to lead hack-and-leak operations against Iran's government. It is highly likely that such groups will continue to form in the future as manifestations of internal discontent. These groups leak significant amounts of information about contractors and their sponsoring agencies. In some cases, the groups and activists (1, 2) are targeted by [agents](#) of the Ministry of Intelligence and Security (MOIS / وزارت اطلاعات) and the IRGC around the world. Two individuals, Masoud Molavi and Ruhollah Zam, through the reported loss of their lives (1, 2) serve as prime examples. Both cases are telling, and highlight Iran's ability to conduct [international harassment](#) campaigns, assassinations, and extraterritorial renditions, as a May 2023 [report](#) by the Atlantic Council also highlighted.

It is likely that Iranian contracting parties aid in the development of domestic and international surveillance capabilities, as was also [reported](#) by Citizen Lab in early 2023, to help Iran's government identify and track activists around the world.

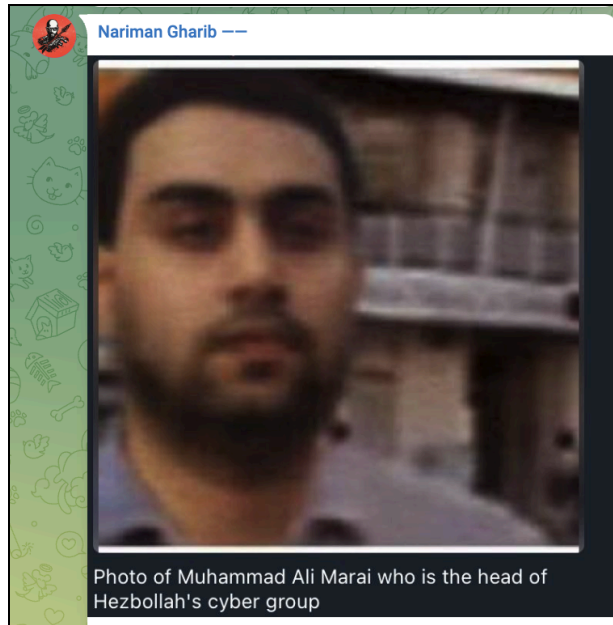


Figure 3: UK-based Iranian activist Nariman Gharib shared an image on December 18, 2023, of the [reported](#) head of Hezbollah's cyber group ("Lebanese Cedar"/"Volatile Cedar"), Mohammed Ali Marai (Source: [Telegram](#))

Sources and Methods

Sourcing and the verification of information revealed by anti-government groups and activists remain complex elements to assess. While various anti-government sources have maintained a significant reporting history, as discussed below, the information is at times conflicting, incomplete, or not verifiable, and may be susceptible to misinformation by threat actors inside Iran. For example, as noted below, the names of individuals and their alleged organizational affiliations, as well as subgroups linked to military and intelligence bodies, are presented with significant variations. In other cases, operator-level personas are linked to specific organizations with little to no corroborating evidence; such information is assumed to be provided to activists and sources by their network of informants.

Threat Analysis

Military Organizations

At least 3 intelligence organizations associated with the IRGC have been named by anti-government groups and in US government indictments. The organizations, which form the bulk of the IRGC's cyber intelligence capability, are the IRGC's Electronic Warfare and Cyber Defense Organization (EWCD) (جنگال), the IRGC's Intelligence Organization (IRGC-IO) (اطلاعات), and the IRGC's Intelligence Protection Organization (IRGC-IPO) (حفاظت), which has a specific counterintelligence remit. Each body has had specific APT groups closely associated with them; for example, in 2022, the Nemesis Kitten APT (Cobalt Mirage, UNC2448, TunnelVision, and Mint Sandstorm [formerly tracked as "DEV-0270"]) was linked via [personas](#) to the IRGC-IO by the anti-government group Lab Dookhtegan.

Another organization with a cyber capability is the IRGC's foreign operations group — the Quds Force (IRGC-QF/ نیروی قدس سپاه). Public records suggest the IRGC-QF leads offensive cyber operations, and, as highlighted below, supports Iran-based companies to develop intrusive and surveillance technologies. The QF also [supports](#) its proxies via training and technology transfer activities.

Within the Quds Force, public records indicate that Unit 300 (واحد 300) has a specific technological cyber remit, and according to Lab Dookhtegan, the head of the said unit is “Amir Lashgarian” (امیر لشگریان). We note this is one example of [conflicting identity](#) information, whereby the name Amir Lashgarian is interwoven with reporting on “Hamidreza Lashgarian”, a reported high-ranking cyber official discussed later in this report.

Unit 300 is a secret unit of Quds terrorist forces under the command of Amir Lashgarian Parst. Unit 300 intends to infiltrate and sabotage Syria, Iraq, Lebanon, Yemen, Jordan with electronic and cyber warfare. This is while these days the Islamic Republic regime is trying to normalize its relations in the region. You can see that we did not do enough to expose the cyber terrorist corps... the exposures are coming. Keep sending more confidential documents, we are willing to pay significant amounts for valuable and reliable documents. Amir Lashgarian soon you will go down.... @Lab_Dookhtegan

Post 664 of 680 by لب دوختگان | LabDookhtegan | Read My Lip... on Mar 14, 2023, 14:48

Figure 4: A Lab Dookhtegan Telegram Channel post captured by the Recorded Future® Intelligence Cloud reveals claims about Unit 300 (Source: Recorded Future)

Organizational Code Names

According to public reports, the IRGC has designated specific titles¹ with code names associated with fallen IRGC personnel to IRGC-linked cyber groups. In October 2023, Lab Dookhtegan claimed to have

¹ Most of the names identified are associated with soldiers who fought with the IRGC in specific campaigns since the organization's existence, in Syria, for example, or during the Iran-Iraq war (1980 to 1988), or against the Mujahedeen Khalq Organization (MEK). The code names are not specific to entities tied to the cyber sector and are broadly linked to other programs run by the IRGC.

[received information](#) about specific operational groups, with presumed IRGC organizational relationships that used code names (**Table 1**). Open-source reporting on this matter, much of which is influenced (1, 2, 3) by Lab Dookhtegan, Nariman Gharib, and “3ackd0or”, has revealed direct relationships between the alleged cover names and pro-IRGC cyber groups.

Since 2021, [disclosures](#) associated with the "Shahid Kaveh" (1, 2, 3) and "Shahid Shushtari" (1) cyber units have continued to transpire, with the most recent claiming that "Shahid Hemmat" is a cover name associated with the longstanding Iranian APT group Tortoiseshell (TA456, Yellow Liderc, Imperial Kitten, Crimson Sandstorm).

Code Name	Public Name	Industry Taxonomy
Shahid Kaveh Group گروه شهید کاوه	"Intelligence Team 13" (reported that other groups comprise the clustering)	Suspected Pioneer Kitten link
Shahid Shushtari Group گروه شهید شتری	Emen Net Pasargad	Suspected Cotton Sandstorm, ViceLeaker link
Shahid Hemmat Group گروه شهید همت	Mahak Rayan Afraz (MRA) (unknown if other groups comprise the clustering)	Suspected Tortoiseshell, TA456, Yellow Liderc, Imperial Kitten, Crimson Sandstorm link
Shahid Toosi Group گروه شهید طوسی		
Shahid Zein ad-Din Group گروه شهید زین الدین		
Qadr Group گروه قدر		
Shahid Fotros Group گروه شهید فطرس		
Shahid Babaei Group گروه شهید بابایی		
Shahid Saheb al Amr Group گروه شهید صاحب الامر		

Table 1: A cluster of operations groups listed by names reportedly referenced among IRGC cadre (Source: Lab Dookhtegan)



Figure 5: Nariman Gharib shares information associated with a doxxed individual linked to Intelligence Team 13 (Source: [Social Media](#))

In October 2022, the Shahid Kaveh and Shushtari operational groups were, [according](#) to Lab Dookhtegan (**Figure 6**), reported to collaborate, and are alleged to have assisted "Office 210" (210 معاونت / اداره ۲۱۰), which is reportedly led by "Ali Karimi". As noted in the subsequent section this persona is reportedly affiliated with the IRGC-IPO.



Figure 6: Lab Dookhtegan claims an operational link between Shahid Shushtari and Kaveh with the IRGC Intelligence Protection Organization (Source: [Social Media](#))

IRGC Intelligence Protection Organization

While we cannot corroborate the claim, Roshangarane-Asr alleged in March 2021 that threat actors linked to Pioneer Kitten operated under the command of the IRGC's IPO. According to the source, a commander named "Ali Karimi" was at the time of writing the officer in charge of "Office 217" (اداره ۲۱۷), which handled threat actors linked to Pioneer Kitten. Additionally, the name Ali Karimi is reportedly a pseudonym for "Hassan Mostafa Mandeh-Ali" (حسن مصطفی مانده علی). We have not identified any additional information associated with either name.

اجازه بفرمایید که اول راجع به اداره 210 و اداره 217 ساحفاسا صحبت کنیم که اینها کی هستند و چرا به راهشان که سپاه را بیش از پیش به زمین خواهد کشید ادامه می دهند؟ که خرها و دوسای، مستقمشان، کسان، هستند که اصلا ما را به سمت اینکه نگاه عمیقتری به ساحفاسا بیاندازیم هدایت کردند تا ببینیم چه کسانی پشت سر آنها هستند. Pioneer Kitten توسط اداره 217 ساحفاسا و شخص علی کریمی پیش برده می شود. اما این فقط یک اسم مستعار است تا نقش او در این شرم آوری ملی برای مردم ایران در سطح جهانی را پنهان کند. علی کریمی همان حسن مصطفی مانده علی است. ما امارتو داریم داش حسن! خودت می دانی که داری کار اشتباهی را انجام می دهی بخاطر همین هم است که پشت یک هویت مستعار خودت را قلم کرده ای! خوب شاید ما یک زنگی به حسن بزنیم و درباره کارش در ساحفاسا صحبت کنیم، اما شاید او ترجیح دهد که شما خوانندگان گرامی با او تماس بگیرید.... 09122191192

Figure 7: Pioneer Kitten Linked to Office 217 of the IPO and listed to be under the management of "Ali Karimi" (Source: Roshangarane-Asr)

In February 2021, Roshangarane-asr commenced disclosing information on the existence of an Office 210, in addition to "Office 240" (معاونت 240 / اداره ۲۴۰) of the IPO. The source claimed both groups were under the direct control of 2 IRGC officers, "Amir Tavakoli" (aka "Masoud Tavakoli"), and "Ali Dari". In April 2021, it was reported that both "Amir Tavakoli" and "Masoud Tavakoli" were pseudonyms, and that the officer's alleged real name was listed as "Amir Yariab" (امیر یاریاب).



Figure 8: Suspected image of Amir Yariab (Source: Roshangarane-Asr)

The IRGC-IO's Cyber Centers

"Center 2060" (مرکز 2060) was pegged to the IRGC-IO by Lab Dookhtegan in 2023. The center is purportedly run by "Ahmad Movahed" (احمد موحد) (aka "Esfandi"), who, according to Lab Dookhtegan, reports to "Cyber Base 2000" (قرارگاه سایبری ۲۰۰۰) commanded by "Reza Nemati" (رضا نعمتی) (aka "Naeemi" / نعیمی). Open-source [information](#) indicates that "Hamidreza Nemati" (حمیدرضا نعمتی) is the head of Cyber Base 2000. Center 2060 is described by Lab Dookhtegan as a hacking and infiltration center affiliated with the IRGC-IO.



Figure 9: Hamidreza "Naeemi" Nemati (Left) was identified as the leader of Cyber Base 2000; Ahmad (Esfandi) Movahed (Right) was deemed responsible for Center 2060 (Source: GFATF [1](#), [2](#))

"Ahmad Khatibi Aghda" (احمد خطیبي عفا) and Afkar Systems — as well as the co-sanctioned entity Najee Technology, run by "Mansur Ahmadi" (aka SECNERD) (منصور احمدی) — have been linked ([1](#), [2](#)) to Center 2000 by Lab Dookhtegan and in other [open-source](#) reports. Furthermore, Lab Dookhtegan [reported](#) that Khatibi, via Afkar Systems, provided unspecified cyber services to Center 2060.

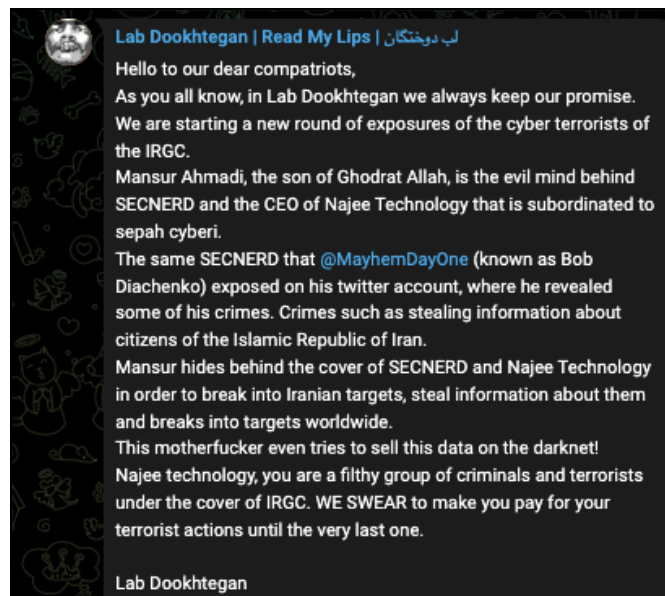


Figure 10: Lab Dookhtegan claimed via its Telegram Channel in 2022 that Ahmadi was the head of Najee Technology and used SECNERD as a moniker (Source: Telegram)

Naeem vs. Naeemi

The executed anti-government source Ruhollah Zam, who was [captured](#) in October 2019 by the IRGC-IO, [highlighted](#) in a November 2016 report that a senior ranking figure in the IRGC's cyber program was called "Naeem" (نعيم). Insikt Group covered the peculiarities of Ruhollah Zam's case following his arrest in 2019. While we cannot confirm Zam's statements, we assess the overlap cited by him to be credible.

Zam's interview covered the existence and reported assassination of a former IRGC cyber army commander, Mohammad Hossein Tajik, who allegedly became an informant of Zam. Ruhollah Zam's reports suggest that in addition to "Naeem", other senior figures in the cyber program used the pseudonyms "Shayan" (شایان) and "Masoud" (مسعود). Shayan and Masoud were allegedly deputies of Naeem in the IRGC-IO's cyber branch.

Insikt Group research suggests that a member of the IRGC-linked contracting entity, the Kavosh Center, "Malek Mohammadi Nejad" (مالک محمدی نژاد), was [referred](#) to as "Shayan" according to Roshangarane-Asr. We identified a second anti-government source that also [reported](#) the existence of Malek Mohammadi Nejad, and further noted that he was an enlisted member of the IRGC ("پاسدار"), and the CEO of the Kavosh Center. Insikt Group is not able to confirm that the two references are to the same person. However, we assess that due to the timing of the dissident reports between 2016 and 2018, and Mohammadi Nejad being an enlisted member of the IRGC, as well as reportedly being the head of the Kavosh Center, Mohammadi Nejad may have, in fact, been senior enough to be a deputy figure to Hamidreza Nemati (Naeem/ Naeemi).

Western Infiltration Plot

We observed another report that mentioned the name "Naeem" being linked to "IRGC intelligence". A "Mr Hamid Naeem" was referred to in a message [issued](#) on social media by another former reported anti-government activist — Masoud Molavi — who, as noted above, was reportedly [assassinated](#) by members of Iran's intelligence services in Turkey.

In Molavi's claim, "Naeem" is linked to a broader IRGC-IO infiltration project against Iranian diaspora opposition groups located in the West, which envisioned the creation and use of a fake dissident outlet to penetrate Iranian diaspora organizations. Most tellingly, Molavi claimed that Ruhollah Zam's news outlet, Amad News, would be used as the alleged lure to attract opposition groups (**Figure 11**). Other ranking officers, such as Tajik, were allegedly involved in the plot.

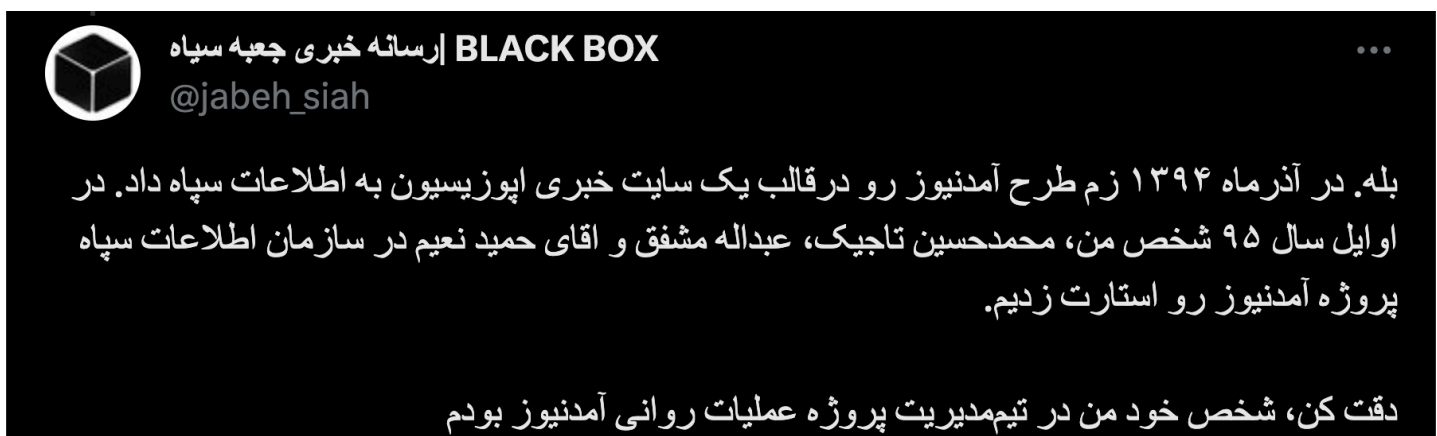


Figure 11: Masoud Molavi's Black Box outlet identifies individuals, including a "Hamid Naeem", linked to the IRGC-IO and alleges the group planned an infiltration operation in the West using Amad News (Source: [Social Media](#))

Financial Motives

According to Lab Dookhtegan, Khatibi allegedly used his access to target Iran-based mining entities for self-enrichment. Farsi-language public records suggest that Khatibi does have a stake in mining groups inside Iran and that, therefore, he could use confidential data associated with Iran-based mining companies for his personal financial interests. On May 22, 2023, Lab Dookhtegan claimed that Khatibi was responsible for

... hacking the country's targets (the site of the Ministry of Mines, hacking into the email of the Ministry of Foreign Affairs, Khava Cement, Iran Khodro, Zanzan and Yazd Electricity Department, Saderat Bank, our insurance) and hacking countries like Saudi Arabia, UAE, Israel, Russia, Germany, France, Italy, America, European countries ... But one of the incredible investments of this villain is buying and selling mines!! his company hacked the mining registration site (*cadastre.mimt[.]gov[.]ir*) related to the Ministry of Industry and Mining and stole a lot of information. Later, he got a lot of income by receiving significant amounts from mine buyers, who were mostly political and influential people, and in return for information. He then communicated with the Ministry of Privacy and reported the vulnerability to the Ministry of Mines. Later, he started buying and selling mines with insider information.

Khatibi's cyber group (Afkar Systems) is highly likely the APT group tracked as Nemesis Kitten. Nemesis Kitten was [cited](#) in US, UK, and Australian government indictments and [alerts](#), respectively, for leading global cyber intrusions. This included the rapid adoption and exploitation of CVEs and remote access and disk encryption tools, as noted by the US Cybersecurity and Infrastructure Security Agency (CISA), [Microsoft](#) (Nemesis Kitten is referred to as a "mature subgroup" of Mint Sandstorm), and [Secureworks](#), among others.



Figure 12: Images of Khatibi issued in open sources (Left, Center); Mansur Ahmadi (Right) (Sources: FBI [1](#), [2](#), and [GFATF](#))

A Counterintelligence Remit?

Another alleged operation executed on behalf of Center 2060 includes the targeting of the Russian diplomatic mission in Tehran. According to Lab Dookhtegan, the intrusion occurred around the time of Iran's 2021 presidential election. If verified this would be the second publicly reported instance of such targeting by Iran-based APTs. In 2019 Kaspersky researchers observed² threat activity they attributed to APT39 (Rana Intelligence Computing Company), a MOIS-affiliated entity, targeting foreign diplomatic missions inside Iran.

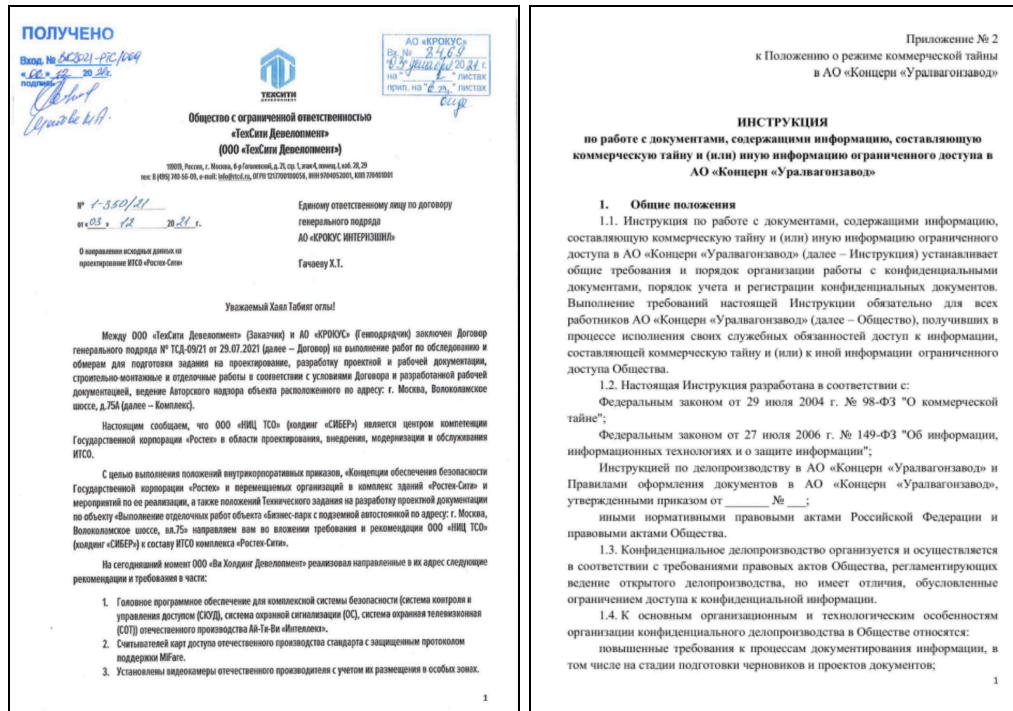


Figure 13: Lab Dookhtegan revealed Russian-language documentation allegedly exfiltrated by Center 2060 (Source: Lab Dookhtegan)

² <https://securelist.com/chafer-used-remexi-malware/89538/>

Contracting Companies

As cited in different US government indictments (1, 2, 3, 4), Iranian intelligence and military establishments receive support from private security companies and threat actors (contractors) to execute cyber research, training, and cyberattack operations. A cohort of contracting companies are publicly listed entities,³ and efforts by governments, anti-government activists, and cyber researchers led to the identification of direct links to specific intelligence groups. Company names, memberships, and the locations of the headquarters of the contracting parties are regularly doxxed.

Among the more notable aspects of Insikt Group's link analysis research is the observed overlapping relationship between Iran-based nationals and their roles (they are regularly referred to as "board members") in multiple contracting companies. It is highly likely that many of the individuals use pseudonyms, which is common among individuals linked to this research, to evade detection and sanctions implications.

We observed multiple, likely related, contracting entities use legitimate and unofficial names as well. For example, one such [publicized](#) relationship exists between sanctioned members of the IRGC-linked Emen Net (Emennet) Pasargad company and Mahak Rayan Afraz (MRA). As discussed below, we suspect another entity — Parnian Telecommunication and Electronic Company — uses an unofficial name when advertising jobs in Iranian career portals.

In some cases, entities identified in this report use similar names, such as "Eleyanet Gostar Iranian" (ایلیان نت گستر ایرانیان) and "Eleyanet Gostar Atiq" (ایلیان نت گستر عتیق). In that particular case, they are assessed to be one and the same company, but in several other cases, the linkages are far less evident. Moreover, public records suggest that company rebranding is also a factor. For example, Eleyanet evolved to be known as Emen Net Pasargad, and [according](#) to the US Department of Justice (US DoJ) and the Department of The Treasury (US DoT), was the front company previously known as "Net Peygard Samavat" (شرکت نت پیگرد سماوات).



Figure 14: US 2020 "Election Project" interference operation launched by Eleyanet Gostar Iranian (Emen Net Pasargad) (Source: Lab Dookhtegan)

³ Public records on Iranian companies are identified as both "authentic" or "unverified" on websites like [rasm\[.\]io](#). As such, some of the information collected for this report could not be verified.

Ayandeh Sazan Sepher Aria Company (شرکت مهندسی آینده سازان سپهر آریا)

According to information disclosed by Lab Dookhtegan in 2023, Ayandeh Sazan Sepher Aria is a front company and allegedly an evolution or close association of Emen Net Pasargad. Lab Dookhtegan claimed that Ayandeh Sazan was formed by persons associated with “Mohammad Bagher Shirinkar” (aka Mojtaba Tehrani / محمد باقر شیرینکار). Lab Dookhtegan claimed that Shirinkar allegedly supervises the company.

Open-source information suggests Ayandeh Sazan has 5 key members: Abdolreza Alborzi (CEO) (عبدالرضا البرزی), Seyyed Mojtaba Sajjadi (سید مجتبی سجادى), Seyyed Mohammadreza Sajjadi (سید محمدرضا سجادى), Omid Ebadi (امید عبادى), and Ali Mohammadi (علی محمدی). While there is limited information on these individuals, public reports suggest that Mohammadreza Sajjadi and Mojtaba Sajjadi are board members of another organization called the Hafeez Avran Institute (موسسه نظم آوران حفیظ). As of this writing, we have [identified](#) a website linked to the entity, which suggests it focuses on providing a variety of physical and protection security services and training. The website also confirmed the role of Mojtaba Sajjadi in the company.

Reported Company Evolution

Open-source and US government reporting have revealed a consistent pattern of apparent evasion by Net Peygard Samavat Company and all those that ensued thereafter. Net Peygard was first identified in February 2019 in a US DoT sanctions [press release](#), where Shirinkar and the infamous threat actor Behzad Mesri were both named. In a subsequent November 2021 indictment and sanctions press release, US government reporting [highlighted](#) that the company had rebranded to Emen Net Pasargad. Across the various anti-government sources, like Lab Dookhtegan, Eleyanet Gostar is pegged to Emen Net Pasargad. As of October 15, 2023, Ayandeh Sazan is reported to be the latest evolution of Emen Net Pasargad (**Figure 15**).

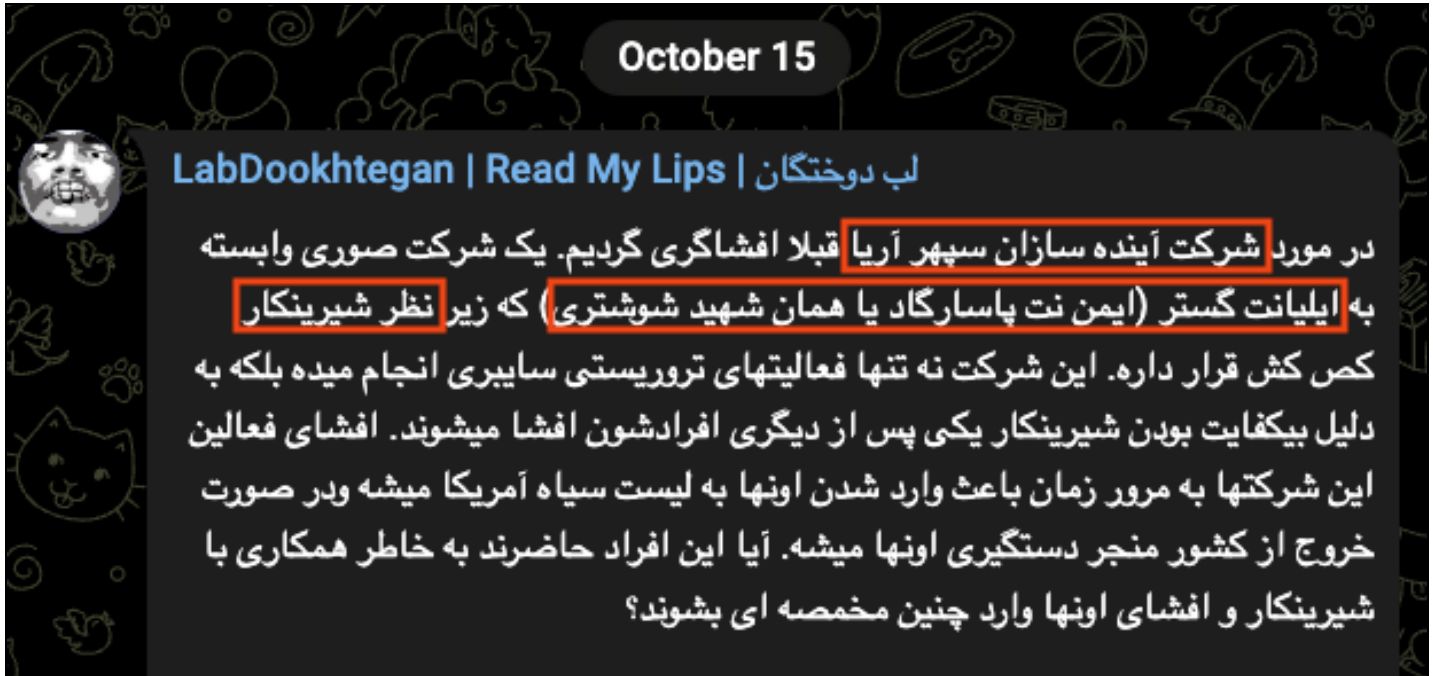


Figure 15: Ayandeh Sazan is linked to the Eleyanet Gostar company and allegedly managed by Shirinkar (Source: Lab Dookhtegan)

Emen Net Pasargad Liquidated

Farsi-language public reports suggest that the Emen Net Pasargad company was liquidated on August 10, 2023, and that the [sanctioned](#) member of company board — Mostafa Sarmadi (مصطفی سارمدی) — was listed as the liquidating party.



Figure 16: Notification of Emen Net Pasargad liquidation also listing Mostafa Sarmadi as the liquidating party (Source: [rasml.io](#))

Front Arises as Company Liquidated

Just prior to the reported liquidation of Emen Net Pasargad, in late July 2023 open-source [reports highlighted](#) that a group calling itself "AnzuTeam" led an intrusion against the networks of Sweden's Police service (Figure 17). Lab Dookhtegan [reported](#) that the front specifically operated at the behest

of Emen Net Pasargad. The group's last Telegram post was issued on August 5, 2023, 5 days prior to the reported liquidation of its sponsoring company.

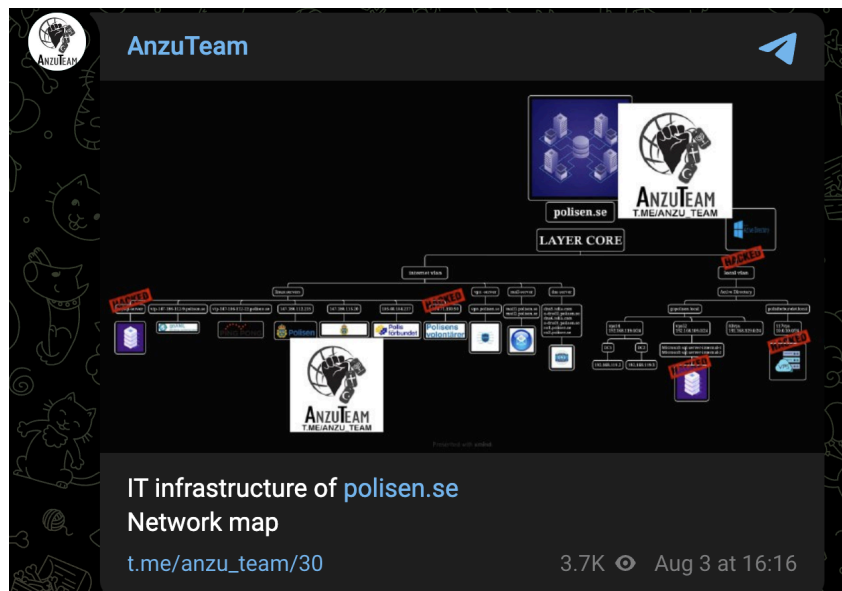


Figure 17: AnzuTeam claims to have led an intrusion against Sweden's Police service (Source: [Telegram](#))

DSPRI (موسسه داده سنجی پیشرفته)

In March 2023, Lab Dookhtegan claimed it received information about an Iranian contracting party — the DSP Research Institute (DSPRI) — linking it to the IRGC Quds Force-Unit 300. According to the source, Unit 300 is responsible for offensive cyber activity throughout the Middle East including in Syria, Lebanon, Jordan, Iraq, and Yemen.

The DSPRI allegedly conducts research on signals, intercepting and breaking encrypted traffic, and jamming. Lab Dookhtegan claimed that the DSPRI's work is being used to conduct large-scale surveillance. According to Farsi-language open-source records of DSPRI, 3 members of the board are Massoud Ghanbari (مسعود قنبری), Seyyed Mahmoud Qutbani (سید محمود قطبانی), and the same Hamidreza Lashgarian referenced above. Open-source [information](#) issued in late July 2023 listed Mohsen Bahgarian (محسن بگریان) as an electronic warfare specialist in DSPRI.



Figure 18: Bagharian is identified as a "senior figure" in Quds Force Unit 300 (Source: [GFATF](#))

Public records also [revealed](#) that several members of this contractor maintain public profiles, including Seyed Hossein Raja (سیدحسین رجاء), Ruhollah Rastagi (روح الله رستاقی), and Morteza Babaei (مرتضی بابایی), among others. Raja is also [listed](#) as an author of multiple Farsi-language programming books on Linux, Linux Security, and SQL.


	نام و نام خانوادگی سیدحسین رجاء
	تاریخ تولد 1362/01/07
	سنتل کارشناس ارشد شبکه و امنیت شبکه
	سویکارایی سیدحسین رجاء کارشناس ارشد فناوری اطلاعات (IT) موسسه تحقیقاتی داده‌سنجی پیشرفته می‌باشد. وی حدوداً 14 سال فعالیت در زمینه‌های مختلف IT من جمله نرم‌افزار، برنامه‌نویسی، شبکه، امنیت شبکه، پایگاه داده، معماری سرور، سیستم‌های لینوکس، ویندوز و اسیل سرور را تجربه کرده است. از جمله مدارک علمی ایشان می‌توان به: CCIE R&S, CCIE Service Provider, CCIP, CCSP, CCDP, CCNP, CCNA, RHCE, RHCA, RHSS, Mikrotik MTNA, MCSE, MCITP, ISA SERVER, CEH, VCP, SQL Server 2008 Design&Implementation&Administration, PHP, MySQL, VB.net, Python, LPI 1,2,3, (Open Ldap-Mixed Environment-Security-Mail), C#, ASP.net, C++, Builder, Delphi, Visual C++ (MFC) اشاره کرد. وی در زمینه امنیت انترنیتی، شبکه، راه‌اندازی و مدیریت سرورهای Exchange Server و Exim مقاله از ایشان در کنفرانس‌ها و ژورنال‌های داخلی و خارجی به چاپ رسیده است.
	علاقه‌مندی‌ها شبکه - امنیت - لینوکس - ویندوز - سیستم‌ها - برنامه‌نویسی - اسیل سرور - معماری سرور
	تحصیلات CCNP-CCSP-CCIP-CCDP-CCIE R&S-CCIE Service Provider-Server 2007-MSCE-MCITP-Exchange Design&Implementation&Administration-ISA SERVER 2006-SQL Server 2008 Design&Implementation&Administration-RHCE-RHSS-Linux LPI 1,2,3-(Open Ldap-Mixed Environment-Security-Mail)-Qmail-Postfix-Sendmail-Exim-OpenPGP-PAM-Squid-Selinux-IP Tables-BPF-mysql 5-Bash Scripting- Perl-Regexp- PHP-Python-Awk & Sed-TC-Visual Basic.net-Visual C#-Website Programming with ASP.net - Borland C++-Builder-Delphi-Visual C++-net(MFC)-CEH
	ایمیل hosseinraja@dsprl.com

Figure 19: Images of Seyed Hossein Raja and his CV are disclosed in open sources (Source: [GFATF](#) and [Social Media](#))

DSPRI is reported to cooperate with another contracting party called "Sabrin Kish" (شرکت صابرین کیش); information on Sabrin (Saberin) Kish was leaked to Farsi-language [mainstream](#) media throughout 2022.

Sabrin (Saberin) Kish Company

In 2022, Sabrin Kish was reported as an entity associated with the IRGC to Iran International, a newsgroup that regularly reports on various matters associated with the Iranian government, domestic corruption, the IRGC, MOIS, and so on. Iran International regularly finds itself at the center of some form of targeting or threat of targeting (1, 2, 3) by agents of the Iranian government. Lab Dookhtegan reported to Iran International that Sabrin Kish was responsible for developing tools used to sniff network traffic and for penetration testing. These tools were reportedly sold to the IRGC and its affiliates.



Figure 20: Capability reportedly linked to Sabrin Kish (Source: Lab Dookhtegan)

[Public records](#) of the company [suggest](#) that multiple individuals are linked to Sabrin Kish, including Hamid Torbatifard (CEO) (حمید تربتی فرد), Mohammad Dehghany (محمد دهقانی), Masoud Mehrdadi (مسعود مهردادای), Mohammad Hossein Rahdan (محمدحسین راهدان), Mehdi Molazadeh Golmahaleh (مهدی ملازاده گل محله), and Esmail Rahimi (اسمعیل رحیمی).

We observed that members are also listed as representatives of a similarly named entity, Sabrin Horizon Engineering Company (شرکت مهندسی افق توسعه صابرین). Additionally, other affiliated companies include Moj Nasr Gostar Telecommunications Company (شرکت مخابراتی و الکترونیکی موج نصر گستر) and Baharan Gostar Kish (شرکت بهاران گستر کیش). Among the more notable personnel linked to the aforementioned companies is Esmail Rahimi, who was listed as a board member of MRA and Eleyanet Gostar Iranian. Additionally, we observed that a Sabrin Kish board member — Mehdi Molazadeh Golmahaleh — was [identified](#) in open sources by anti-government activist Nariman Gharib, and linked to the development of a scholarly article at Imam Hossein University.

Masoud Mehrdadi is also another notable board member of Sabrin Kish. According to [public records](#), he is affiliated with the sanctioned [IRGC Cooperative Foundation](#), which is associated with various companies, including the Sabrin Horizon Engineering Company. Mehrdadi is highly likely the individual cited in open sources ([1](#), [2](#)) to be one of the masterminds guiding the financial system supporting the IRGC. Open-source records [indicate](#) he holds a stake in or is a sitting member of at least 22 other registered organizations inside Iran. US DoT has [indicated](#) that the Cooperative Foundation serves as an entity to fund the "IRGC's military adventures abroad, including into the pockets of militant groups associated with the IRGC's external operations arm, the IRGC-Qods [Quds] Force".

Foreign Operations

Public reports issued by Lab Dookhtegan revealed documentation suggesting that Sabrin Kish is involved in the exportation of its software and technologies to overseas clients (**Figure 21**). In one

instance of a reported sale of software, hardware, or services, a Sabrin Kish representative — Mohammad Dehghany (محمد دهقانی) — is listed as a signatory in an agreement (albeit unverified) with the Iraqi government. The Iraqi counterpart is listed as "Faleh Al-Fayyadh", described in the documentation as the "National Security Advisor for the Republic of Iraq".

According to open sources (1, 2), Al-Fayyadh was [sanctioned](#) by the US government in 2021; he is listed as a high-ranking member of the Iraqi government and the Chair of Iraq's Popular Mobilization Forces ("hashed al-Shaabi"). According to an Iranian [anti-government organization](#), Al-Fayyadh reportedly maintained very close ties with former and current members of the IRGC-QF, including Qassem Suleimani and Abu Mahdi al-Muhandis.

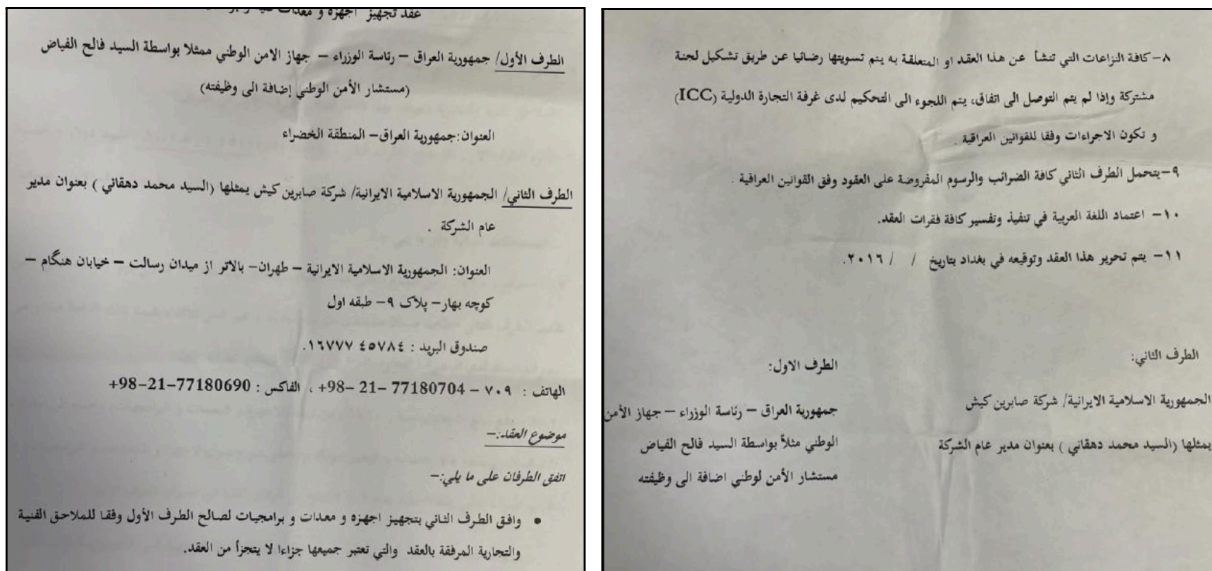


Figure 21: Sabrin Kish is allegedly linked to a service deal with the Iraqi government (Source: Lab Dookhtegan)

شركة مخابراتي و الكترونيكي توسعه سروس سامان) Soroush Saman Company

During the development of this report, [information](#) was released that established another link between the IRGC-QF Unit 300, Amir Lashgarian, and the Iranian contracting space, specifically via an entity called the Soroush Saman Telecommunication and Electronic Development Company. Open-source reporting [alleges](#) this group helped Lebanese Hezbollah build its capabilities.

According to a Telegram Channel post issued in June 2023, Lab Dookhtegan stated that Unit 300 used a cover term — "Haidar Karrar" — for its projects tied to Syria and Lebanon. As stated above, the Recorded Future Intelligence Cloud captured chatter on Unit 300, the alleged travel of Lashgarian to Syria (Figure 4), the work of Unit 300, and other reported members of QF Unit 300.

پروژه های واحد 300 مربوط به حزب الله با نام "حیدر کرار".

Figure 22: Lab Dookhtegan states Unit 300's projects associated with Hezbollah are called "Haidar Karrar" (Source: Lab Dookhtegan)

Public reports indicate there are 4 members of the board, 2 of whom have been cited in open sources: Hassan Khadem Kalan (حسن خادم کلان) and Mohammad Hossein Rahdan. The latter is the same individual listed as a board member of Sabrin Kish. The remaining 2 members are Qassem Rahimi (CEO) (قاسم رحیمی) and Masoud Kamiab Farahbakhsh (مسعود کامیاب فرح بخش).

A career [web portal](#) suggests the Soroush Saman Company operates in the field of advanced telecommunications and electronics. Coincidentally, information released via the Israel-based source IntelliTimes, citing information shared by Lab Dookhtegan, claimed Unit 300 has a very specific offensive cyber remit that includes "information warfare and electronics for access to mobile phones, identification through artificial intelligence and electronic warfare tools".

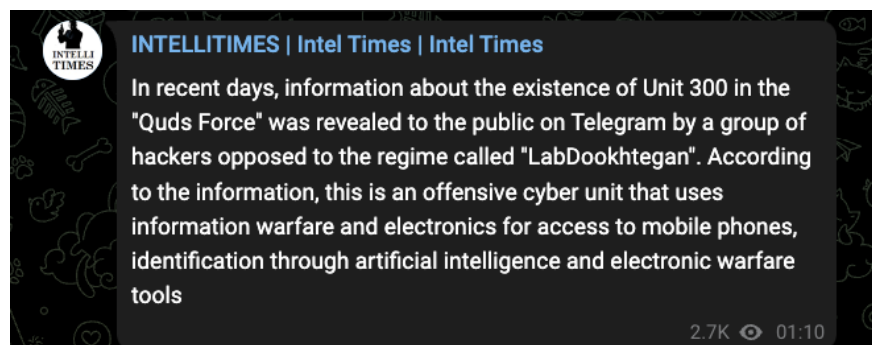


Figure 23: Unit 300's remit divulged by Lab Dookhtegan and cited by Israeli intelligence channel IntelliTimes (Source: IntelliTimes)

Mahak Rayan Afraz (محک رایان افراز)

Insikt Group [first reported](#) on Mahak Rayan Afraz (MRA) in April 2020. [According](#) to dissident accounts, MRA was previously known as "Dehkadeh Telecommunication and Security Company" (شرکت مخابراتی دهکده امن), among other names, and according to [public reports](#), was established in March 2012. MRA is widely cited ([1](#), [2](#)) by other cybersecurity vendors to be an IRGC contracting party.

Roshangarane-Asr reported in October 2019 that 3 operators were responsible for malware development activities: Mohammad Hadi Ghorbani (محمد هادی قربانی), Mohsen Imani (محسن ایمانی), and Mojtaba Khalash (مجتبی خلش) (**Figure 24**). Significant information has surfaced that has established technical [links](#) to malware authorship tied to MRA that, in turn, were pegged to the Tortoiseshell APT group.



Figure 24: MRA operators are linked to "Gol Rokh" and "Hazm" projects (Source: Roshangarane-Asr)

Allegedly, these malware developers were responsible for 2 projects, including one facial recognition project called "Gol Rokh" that has been used by the IRGC for surveillance purposes. A second project focusing on Persian natural-language processing was listed as "Hazm", which we identified in a GitHub repository. The profiles (1, 2, 3) of the above-named individuals are listed among a handful of other contributors.

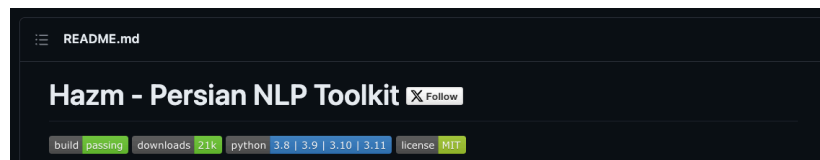


Figure 25: Hazm project listed on GitHub (Source: GitHub)

We also observed that the project is associated with an Iranian artificial intelligence company called "Roshan" (*roshan-ai[.]jir*). This entity is highly likely responsible for the Hazm project, and we observed a page [dedicated](#) to the project hosted on *hazm.roshan-ai[.]jir*. We assess that Roshan's official name, according to Iranian public records, is "Rahkar Pardazesh Zharf" (راهکار پردازش ژرف), and that Mohsen Imani (likely Mohsen Imani Farahani) is a company board member.

Information on MRA also led to the identification of another related entity which is listed below — Parnian Telecommunication and Electronic Company (شرکت مخابراتی و الکترونیکی پرینان). Parnian is connected to MRA through an [associated](#) member of the board — "Mohammad Agahi" (محمد آگهی).

[Public reports](#) on MRA suggest the company was liquidated in June 2023. Whether MRA remains active, has rebranded (as it allegedly already did), or has, in fact, been dissolved in its entirety is unknown as of this writing.



Figure 26: Announcement on MRA liquidation listed in June 2023 (Source: rasmf.jio)

Parnian Telecommunication and Electronic Company

(شرکت مخابراتی و الکترونیکی پرنیان)

Official records [suggest](#) the Parnian Telecommunication and Electronic Company was established in January 2016 and is located in central Tehran. The currently listed board members are Seyed Hamza Esmail (سید حمزه اسماعیل), Mohsen Sheikh Hosseini (محسن شیخ حسینی), Hossein Hashemifar (حسین هاشمیفار), Seyed Mostafa Musavi Malvajerdi (سید مصطفی موسوی مالواجردی), and, as noted above, the member that linked this company to MRA, Mohammad Agahi. Beyond the official records, we identified no pertinent information on Parnian.

However, we identified a similarly named entity — Parnian Research Center (مرکز تحقیقاتی پرنیان) — which focuses on information security matters. We have [identified](#) multiple job roles advertised on Farsi-language recruitment websites that seek individuals educated in information security, penetration testing, artificial intelligence, computer programming languages, and the English language (for translation purposes). All roles are geographically located in Tehran; however, unlike other Iranian companies investigated in this report, we have not identified any official record related to this second entity. We identified 1 email address that is possibly linked to this second entity — [info@parnian\[.\]net](mailto:info@parnian[.]net).

Additionally, we have not identified an active presence of employees listing the company on LinkedIn profiles, nor have we identified any company presence on other networking sites. The company logo is generic and not unique to the Parnian Research Center and is widely accessible across the internet.

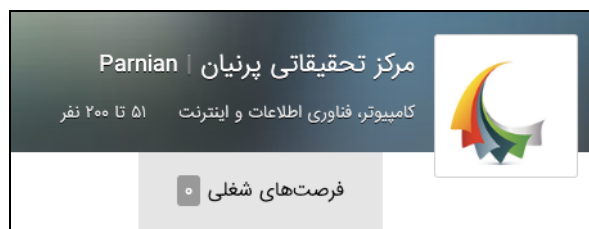


Figure 27: Parnian is listed as having between 51 and 200 employees (Source: Iranian job website)

We assess it is likely that jobs are being advertised under an unofficial name associated with Parnian Telecommunication and Electronic company. The lack of public information linked to employees is potentially related to increased operational security measures to prevent their identification.

Elements in the Cyber Leadership

US government reports have highlighted the role of the threat actors and personas, which through indictments and sanctions, have linked them to Iran's cyber program. Anti-government hacktivists have equally established extensive reporting histories on individuals with alleged associations with military and intelligence organizations, cyber projects, and international attack operations. Open sources link these individuals to the IRGC-EWCD, the IRGC-IO, the IRGC-IPO, and a slew of contracting organizations.

دوستان و همکاران عزیز،
از تشویق و استقبال شما عزیزان بعد از پست اخیرمون درباره حمیدرضا لشگریان و علی مقدسی و کامنت ها، نظرات و اطلاعاتی که فرستادین متشکریم! اخیرا مقدار قابل توجهی اطلاعات درباره مرکز تحقیقات کاوش جمع کردیم. مرکز کاوش یکی از منابع اصلی ابزار سایبری سازمان جنگال است. این رابطه اخیرا در گزارش بد افزار استون دریل و نقش آن در حملات سایبری علیه عربستان درج شده و ما هم البته در بلاگمون به این حمله اشاره کردیم و در آخرین پست مان، رهبران سایبری

Figure 28: Hamidreza Lashgarian and Col. Ali Maghdesi are both linked to the IRGC-EWCD's Kavosh Center and cyberattacks against Saudi Arabia (Source: Roshangarane-Asr)

Information about specific personas is not comprehensive, and in many cases information passed by sources is allegedly acquired via their own informants inside specific contracting parties. As part of our analysis we have observed these individuals use multiple names and identities. Among the most widely cited individuals are Hamidreza Lashgarian and Mohammad Bagher Shirinkar (aka Mojtaba Tehrani).

Gen. Hamidreza Lashgarian (aka Ebrahim Qazizadeh / ابراهیم قاضی زاده)

In June 2017 Roshangarane-Asr first reported the existence of Hamidreza Lashgarian, and claimed he was a high-ranking IRGC cyber official. Since then, reporting highlighted his role as a senior figure of the IRGC-EWCD specifically, and linked him to countless contracting parties. These entities included the MRA, the Kavosh Center, the Hafeez Center, Eleyanet Gostar Iranian, the Nasr Center, and, as noted above, DSPRI. Public records [indicate](#) that Lashgarian currently presides over other Iran-based companies, such as "Kousar Com Research Group" (گروه تحقیقات کوثر کام) and "Deep Com Asia Company" (شرکت ژرف کام آسیا).

In 2022, the same Lashgarian was surprisingly identified by a dual Australian-British national, Dr. Kylie Moore-Gilbert, who was [arrested](#) on [espionage charges](#) by an intelligence wing of the IRGC and detained in Ward 2A of Iran's Evin Prison. While detained she reportedly came into contact with a person named Lashgarian who also used the pseudonym "Ebrahim Qazizadeh"; during this period, there was also a [reported](#) attempt to recruit Moore-Gilbert as a double agent. While she could not verify if it was Hamidreza Lashgarian or another person, Moore-Gilbert described his physical similarities and claimed he was linked to the IRGC's intelligence service and Iranian academic institutions.



Figure 29: Dr. Moore-Gilbert, a former captive in Iran's Evin Prison, highlighted the links between the Lashgarians and the IRGC (Source: [Social Media](#))

Furthermore, according to different reports issued by Lab Dookhtegan, Lashgarian has traveled to Syria in the presence of IRGC-QF commander Esmail Ghaani (Qaani) to conduct unspecified activities with IRGC-QF Unit 600. This would suggest that Lashgarian is connected to at least 2 QF units based on research presented in this report (Unit 300 and Unit 600).

Familial Link

Sources reporting on Roshangarane-Asr have also highlighted that Hamidreza has allegedly positioned a nephew — "Mehdi Lashgarian" (مهدی لشگریان) — as the head of the IRGC-EWCD-linked outlet, the "Cyberban Institute" (موسسه سایبریان). Public reports suggest that a Mehdi Lashgarian is referenced in an Iranian company's membership records, but as of this writing, without any additional context, we assess that this is a low-confidence link.

"Amir" vs "Hamidreza" Lashgarian

As discussed throughout this report, there are at least 2 references to a "Lashgarian" who is reported to be a high-ranking member of the IRGC's cyber organizations. One is associated with the Quds Force and the other with the IRGC-EWCD. According to Dr. Moore-Gilbert's [reports](#), a Lashgarian who shares the same features has also had some involvement in the interrogation of foreign prisoners, including herself, at Evin Prison.

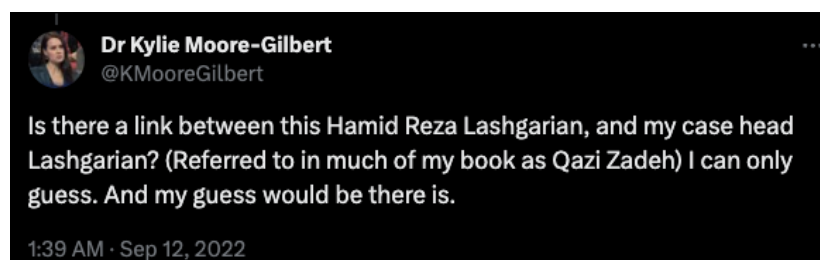


Figure 30: Dr. Moore-Gilbert suggests Hamidreza Lashgarian is linked to her case (Source: [Social Media](#))

The names of both Amir Lashgarian and Hamidreza Lashgarian have been cited extensively in anti-government sources, although the reporting history on Hamidreza dates back to 2017. Insikt has also noted that Lashgarian is linked to multiple contracting companies serving the IRGC's offensive efforts, as noted throughout this report. The interchangeable use of the names Amir Lashgarian and Hamidreza Lashgarian, along with side-by-side images of the same individual (**Figure 31**), is possibly

indicative of the same persona; however, as of this writing, we assess it is likely these are 2 separate individuals.

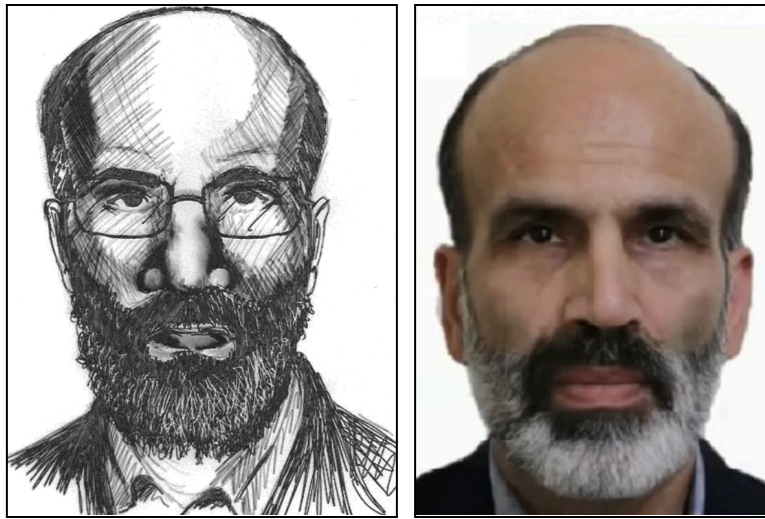


Figure 31: Sketch of Hamidreza Lashgarian from June 2017 (Left) and image released by Lab Dookhtegan in 2022 (Right)
(Sources: Roshangarane-Asr and Lab Dookhtegan)

Mohammad Bagher Shirinkar (aka Mojtaba Tehrani)

Mohammad Bagher Shirinkar's record is significantly longer than other known Iran-based individuals associated with the IRGC's cyber program, appearing in at least 2 ([1](#), [2](#)) US government sanctions listings. Shirinkar's relationship with the IRGC is reported to be strongest with the IRGC-EWCD, even though Roshangarane-Asr also claimed he operated at the behest of the IRGC-IPO for some time. He is among the first known members of the [sanctioned](#) entity, Net Peygard Samavat Company.

Among anti-government hacktivist networks, Shirinkar's links to the IRGC's cyber program date to August 2016, when information about him shared by Roshangarane-Asr suggested he worked for the IRGC-IPO.

Familial Link

As observed with the Lashgarian case, Shirinkar is also flanked by a family member, Mohammad Hossein Shirinkar, who [reportedly](#) holds a cyber position at the IRGC-IPO. While there is less information about Mohammad Hossein in open sources, he was allegedly linked to a "Project Sayad" that [involved cyberattacks](#) against Albania's Tirana International Airport in mid-2022.



Figure 32: Images of Mohammad Bagher Shirinkar and Mohammad Hossein Shirinkar released in public reports
(Source: [Iran International](#))

Mehdi Dehghany (مهدي دهقانی)

Mehdi Dehghany is another persona linked to the Iranian cyber program and highly likely associated with the Lashgarian network of contracting companies, according to the anti-government source Roshangarane-Asr. While we have not identified any corroborating information, the source claimed Dehghany was directly responsible for managing the Nasr Electronic Research Center (پژوهشگاه مخابرات و الکترونیک نصر), which at the time was referenced as an "important facility" linked to the IRGC-EWCD and research associated with surveillance and espionage tools and technologies.

Like Lashgarian, Mehdi Dehghany has also been linked to Imam Hussein University via an email address — mdehghany@ihu.ac.ir — shared by Roshangarane-Asr, and has [authored](#) cyber-related [research](#) at that educational institution.

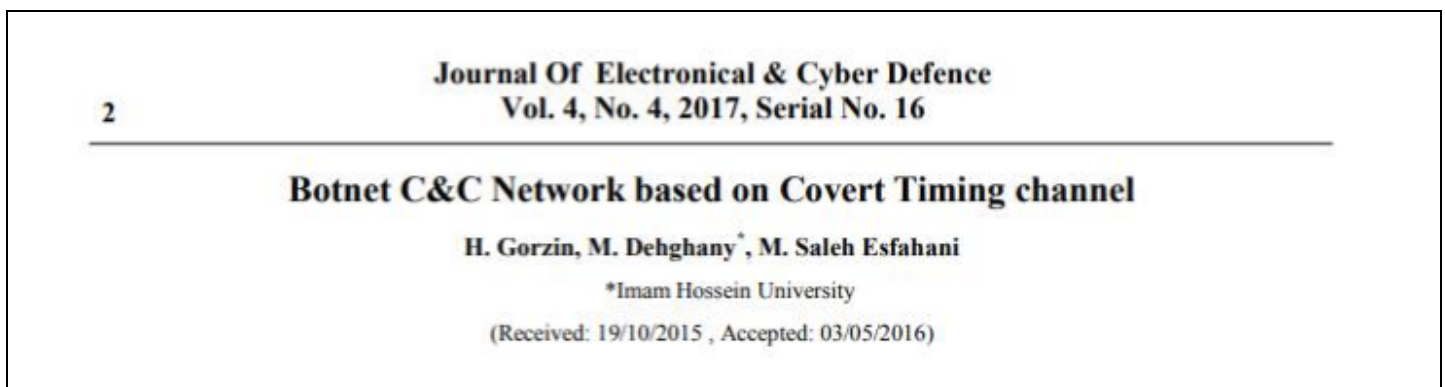


Figure 33: Academic research allegedly associated with Mehdi Dehghany (Source: Roshangarane-Asr)

There is significant reporting on the existence of a "Nasr Center" or "Nasr Institute", [covered](#) by Insikt Group as well as the broader [cyber research community](#). This reporting has often linked personas from

the research center to cyberattack capabilities generally attributed to Iran's APT33 (Peach Sandstorm, Elfin, Holmium, Refined Kitten).

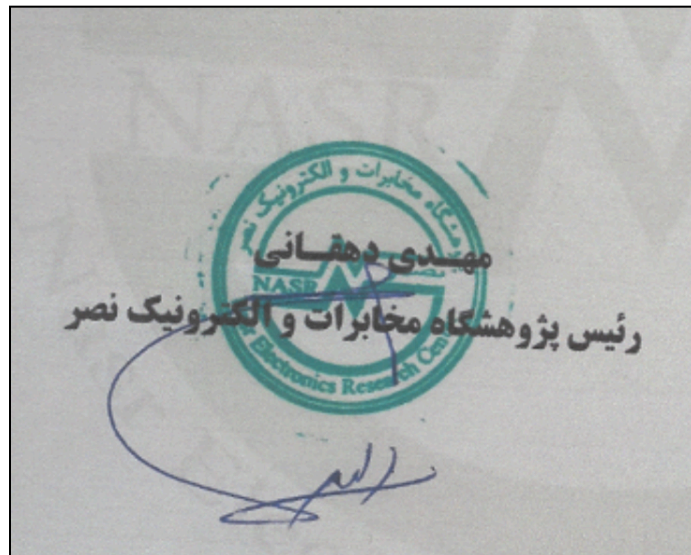


Figure 34: Document linked to the infamous Nasr Electronic Research Center signed by Mehdi Dehghany
(Source: Roshangarane-Asr)

Outlook

This report focused on an interconnected network of individuals associated with the IRGC's cyber program who were doxxed by anti-government fronts like Roshangarane-Asr and Lab Dookhtegan. The results of the research suggest that Iranian contracting companies are established and run by a tight-knit network of personas, who, in some cases, represent the contractors as board members. The individuals are closely associated with the IRGC, and in some cases, are even representatives of sanctioned entities (such as the IRGC Cooperative Foundation).

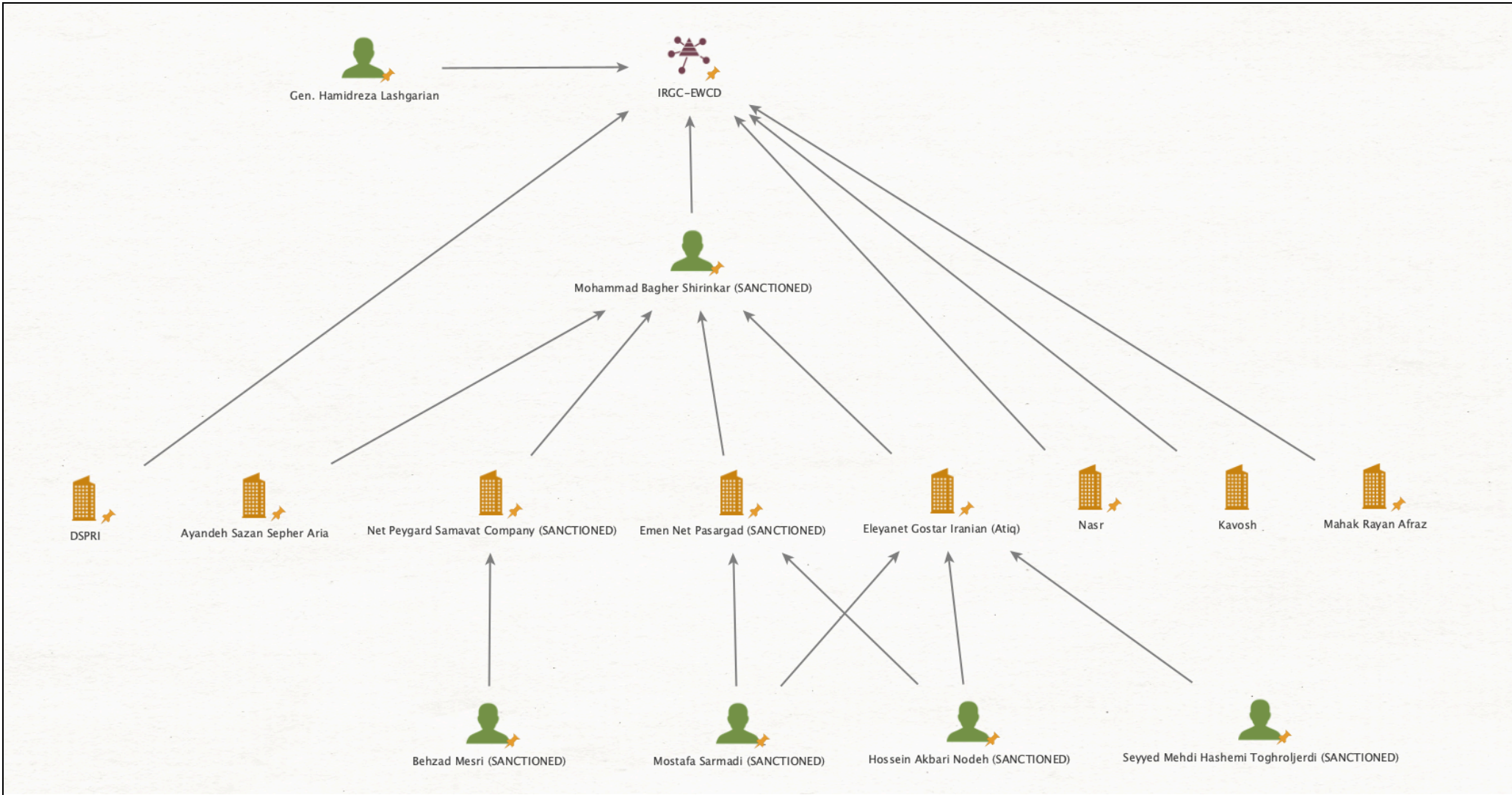
As part of our research, we observed known overlaps between sanctioned individuals and their associations with specific contracting parties. However, in other cases, individuals who shared links to multiple contracting parties could only be identified by name and position, as is the case with Esmail Rahimi (**Appendix D**). It is unknown how senior a figure Rahimi is, but his associations with at least 3 reported cyber contractors are suggestive of a relationship in line with managers like Shirinkar.

The IRGC's Quds Force is reportedly well-positioned to export technological services and capabilities tied to electronic warfare and offensive cyber via a network of contracting companies located in Iran. The entities conducting international sales, as was alleged with Sabrin Kish, for example, are also the beneficiaries of the relationships built between IRGC-QF and members of various regionally dispersed proxy groups. The cases of Sabrin Kish and Soroush Saman are not likely to be unique.

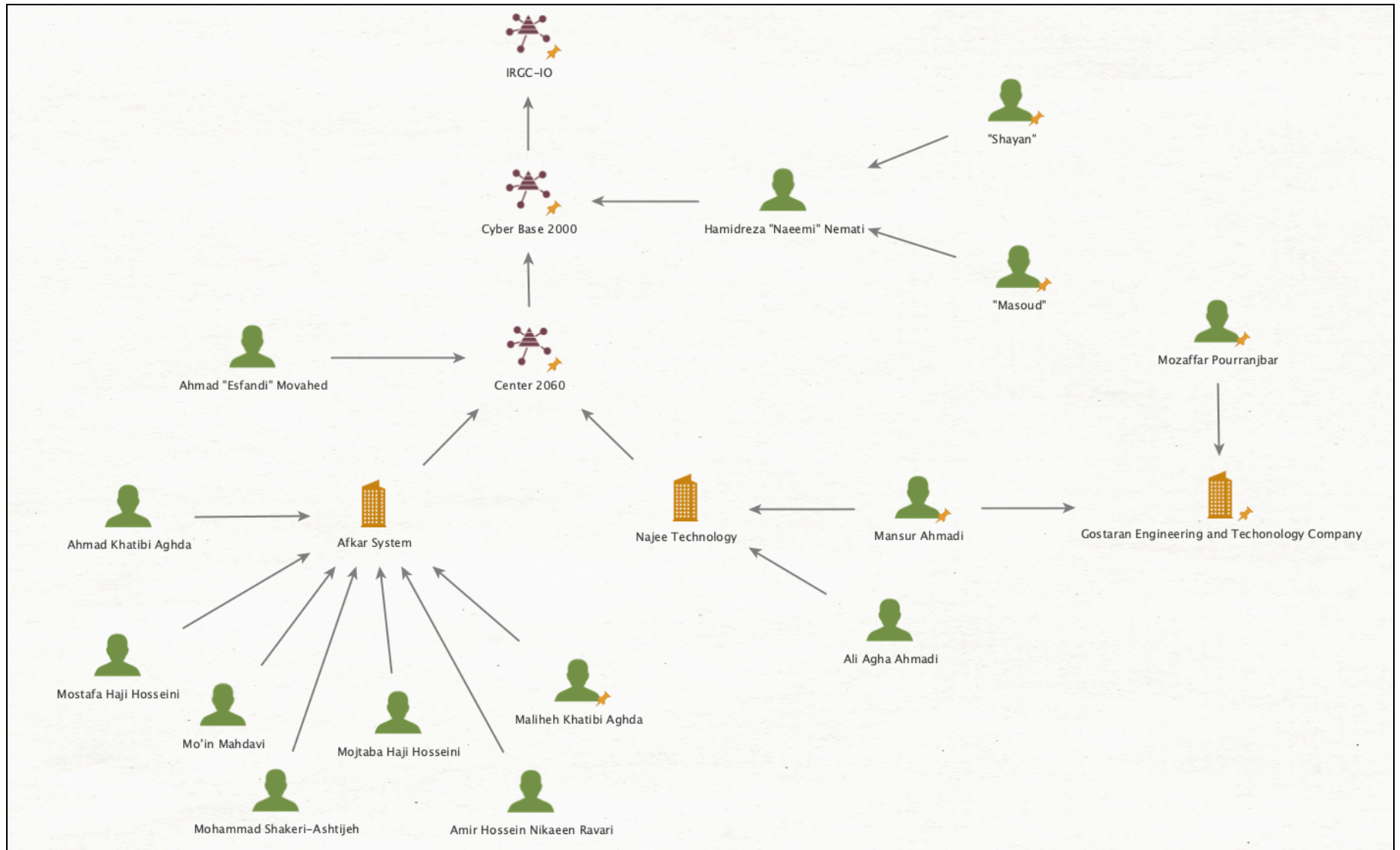
We did not observe an overlap between personnel (board members) of the IRGC-IO and those associated with either the IRGC-EWCD or the IRGC-QF. This is possibly suggestive of a partitioning of vested interests, and as such, specific individuals can be viewed as having a sphere of influence over specific contracting organizations.

As more information on the Iranian cyber program is disclosed by anti-government groups, we assess it is likely that Iranian government responses will redouble efforts to complicate the verification of information. As such, names of individuals, companies, and cyber projects may be further obfuscated and detached from the core of the IRGC's military and intelligence groups to better their operational security postures. Such shifts in security posture will also likely affect informant networks inside Iran, which will be targeted by the likes of the IRGC-IPO, IRGC-IO, and MOIS.

Appendix A — IRGC-EWCD Affiliations



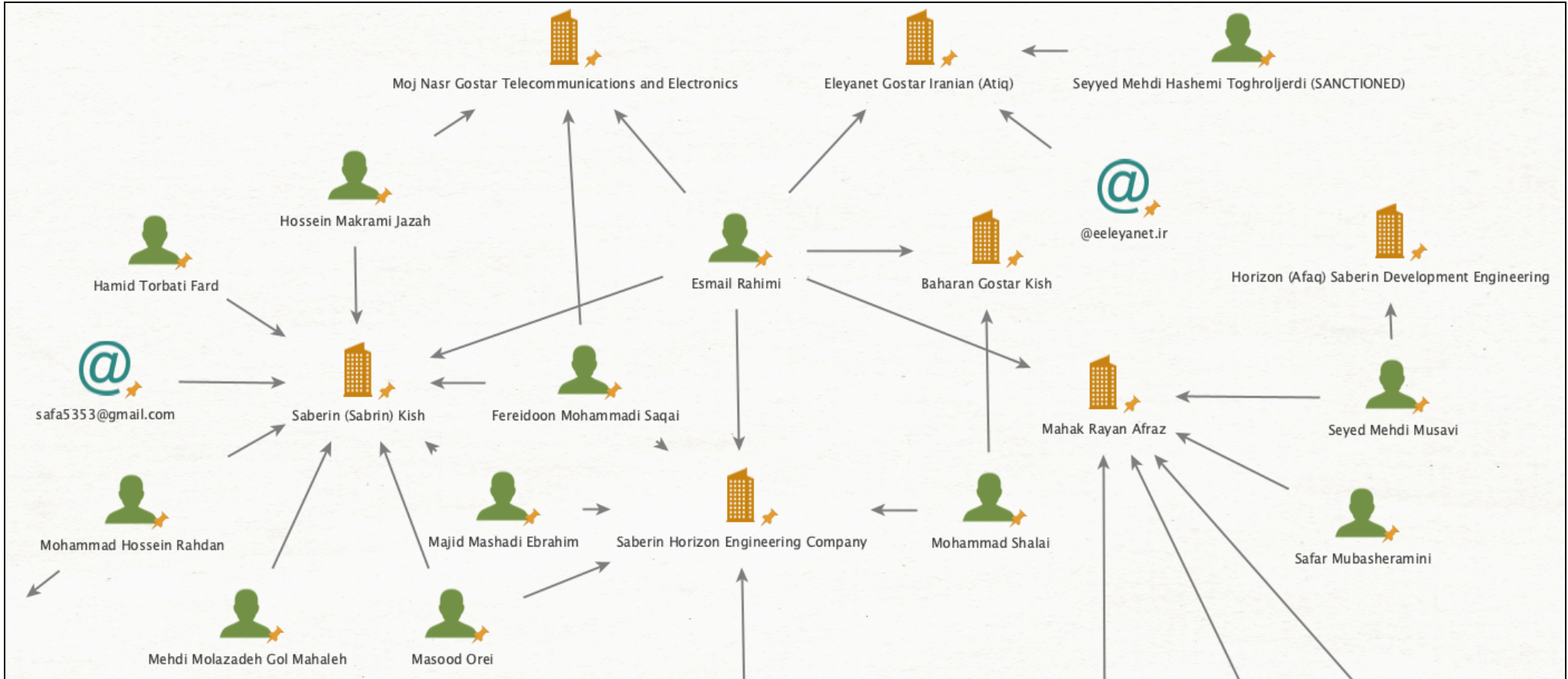
Appendix B — IRGC-IO Affiliations



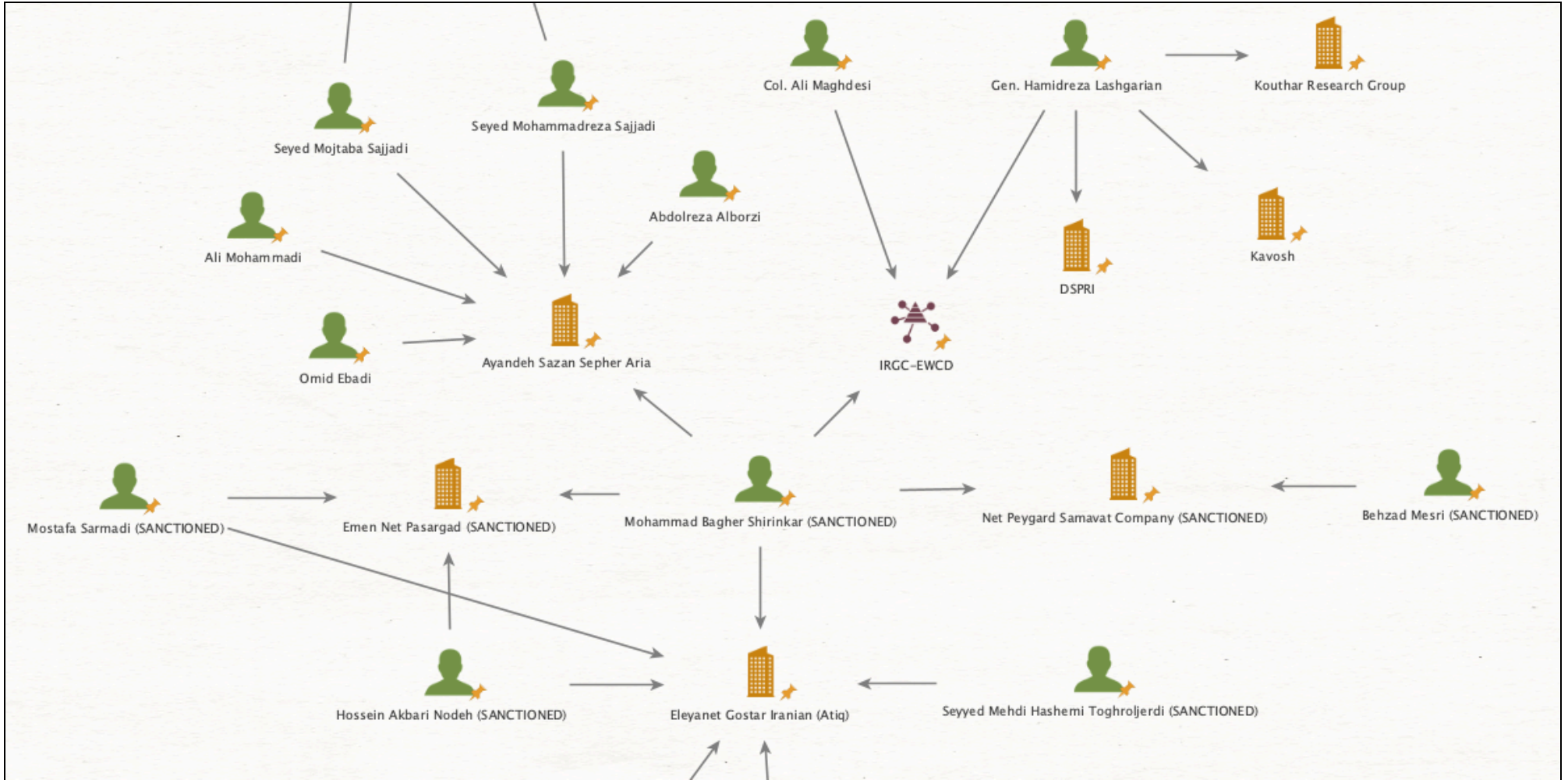
Appendix C — IRGC-QF Affiliations



Appendix D — Esmail Rahimi (اسمعیل رحیمی)



Appendix E — Mohammad Bagher Shirinkar (aka Mojtaba Tehrani / محمد باقر شیرینکار)



About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

[Learn more at recordedfuture.com](https://recordedfuture.com)