HackerWatch Roundup

The Hacktivists Challenging the Islamic Republic's Legitimacy

Filterwatch

January-June 2023

Executive Summary

The spree of hack-and-leak attacks continued in the first half of 2023. The Iranian government has become a prime target of hacktivist activists. Various hacking personas have defaced official websites, infiltrated domestic networks, and spilled top secret documents into the public domain. While the identity and affiliation of many of these groups remain unclear, they seem to share a common incentive: weaponizing the internet against one of the rising cyber powers of the world in revenge for suppression of Iranian people. Leaked documents expose the dark side of the regime – corruption, repression, and illegal affairs that the Islamic Republic resorts to for survival.

The scale of intrusion and leak would present a major national security dilemma for any country and prompt investigations to identify the vulnerabilities. But, so far, the Iranian government has only dismissed these attacks and leaked files as fake. Speculations about the affiliation of these groups continue. At best, they are dissident hackers showing sympathy with protesters. Or these hack-and-leaks are part of a larger intelligence contest by Iran's adversaries seizing the momentum to spill some of Iran's best kept secrets. As protests in Iran go underground due to increasing repression, vengeful hack-and-leaks will likely continue to surge.

Introduction

Over the past several years in Iran, many hacking groups have emerged with various aims, political motives, and ambitions. Attribution of these groups seems nearly impossible. Some operations seek to expose Iranian government secrets or support opposition groups while others target Iran's adversaries like Israel and the United States. Since 2020, attacks on both sides have become more frequent and publicly visible to the point of an overt, tit-for-tat rivalry in the cyber domain.

In the aftermath of the Woman, Life, Freedom protests that sparked last September, a growing number of groups have taken aim at the Iranian regime. They have exposed top secret documents on Iran's nuclear program, interrupted livecast of the state-run television, defaced official websites, among other moves. Each group has developed a unique persona and motto while trying to expand their range of targets every single time. These activities are often greeted by dissidents and dismissed by the government. Leaked files depict a convoluted infrastructure for bypassing economic sanctions, the regime's internal power struggle with the IRGC's extensive reach and growing political ambitions, and an intertwined machinery of surveillance and repression.

This Hackerwatch report covers hacktivist operations against the Islamic Republic between January and June 2023. The focus is due to an increase in the number of groups involved as well as the scope and nature of leaked documents. Together, these activities depict an evolving hacking landscape that's undermining the legitimacy of the Islamic Republic more than ever.

Anonymous

Hacktivist collective Anonymous continued its activities in 2023. On January 16, Anonymous leaked over 20,000 emails from Iran's largest petrochemical company. These emails include confidential correspondences, contacts, commercial documents, among others, dated August 2020 through October 2022. Together, the emails shed new light on the extent to which the Islamic Republic bypasses U.S. economic sanctions through private companies such as the Persian Gulf Petrochemical Industry Commercial Company (PGPICC). According to leaked files, Iran uses an extensive network of third party shell companies to export oil and other petrochemical goods to a number of countries. China is the most common destination, followed by India, Iraq, Turkey, and the UAE, among others.[1] The export to China alone amounted to 9.4 billion US dollars in slightly over two years.

Anonymous continued its hacking spree in the following two months. On February 2, Anonymous announced it had defaced the official website of the Headquarters for Moral Guidance, a state-funded political establishment on a mission to boost moral and religious values in Iran. In the aftermath of Mahsa Amini's death in the morality police custody, this headquarter became the target of public contempt for its mission to impose religious beliefs on Iranian youth. On February 19, Anonymous allegedly defaced the website of Kerman province administration. On March 26, Anonymous leaked a map of alleged IRGC bases, including armory and ammunition stations, along the western border of Iran (Figure 1).

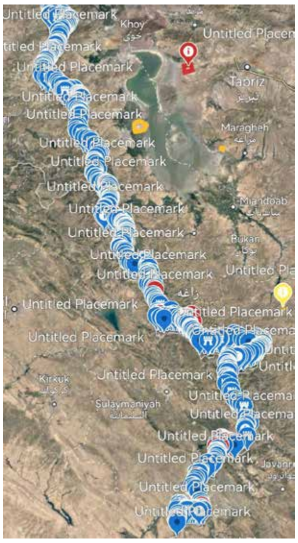


Figure 1. Anonymous's alleged map of IRGC military bases along the western border of Iran.

Black Reward

On January 20, Black Reward, which had made a fiery debut[2] last October, made a comeback

[1] WikiIran has archived tranches of leaked files over the past months. Their searchable dataset of PGPICC emails indicates that Europe is another destination for Iranian petrochemical cargo (appeared 65 times in the dataset without specifying the country or countries it was delivered to). The same goes to the Commonwealth of Independent States (CIS) (29 times) and Africa (2 times) without naming a particular country. Other destinations include Afghanistan, Pakistan, Russia, Singapore, Brazil, Oman, Taiwan, and more.

[2] Between October and December 2022, Black Reward single-handedly released more documents than any other hacktivist personas since the Woman, Life, Freedom protests began. Its revelations included documents from IRGC-affiliated Fars News, Iran's Atomic Energy Development Agency, the National Oil and Gas Company, and Press TV, the international arm of the state broadcaster.

with new troves of documents from an IRGC-affiliated university. Imam Sadiq University was originally founded (under a different name) by a number of Harvard and MIT educated Iranian scholars before the 1979 revolution. The mission was to educate high-skilled managers and bureaucrats that would serve both public and private sectors. After the revolution, the university was seized by pro-regime figures and turned into a pipeline for training managers that were politically and ideologically aligned with the regime.

The hack-and-leak operation against Imam Sadiq University was significant in a number of ways. First, leaked documents indicated the university's plan for revenue generating activities that are, at best, questionable. A particular focus is on mining cryptocurrency – a murky policy issue in Iran that has had electricity providers impose limitations on mining due to high power consumption of crypto farms. Imam Sadiq University has managed to obtain a crypto-mining license from a local authority on matters of industry, mining, and trade in Khorasan Razavi province. The university stationed the mining farm at a semi-dormant local garment factory (کارخانه پوشاک جامعه)[3] to save on energy – and to obfuscate its activities. However, the crypto farm was suspended by the local electricity provider due to unpaid bills. The crypto farm managed to resume its activities with a court order, but billing disputes remained with the power company, according to leaked documents.

Second, these revelations also demonstrate the extent to which pro-regime establishments are invested in compulsory hijab, not only as an ideological matter but also for monetization purposes. One leaked document revealed that the university was considering a partnership with local businesses in Mashhad, a religious tourism destination for Shi'te pilgrimage. The goal would be to produce black clads (Chador in Persian, a religious outfit for women that covers head to toe) for sales in Mashhad. The university's leadership supposedly considered this as a profitable business model given the popularity of black clads among the religious population of Mashhad and tourists that need a clad to enter the eighth Imam's shrine.

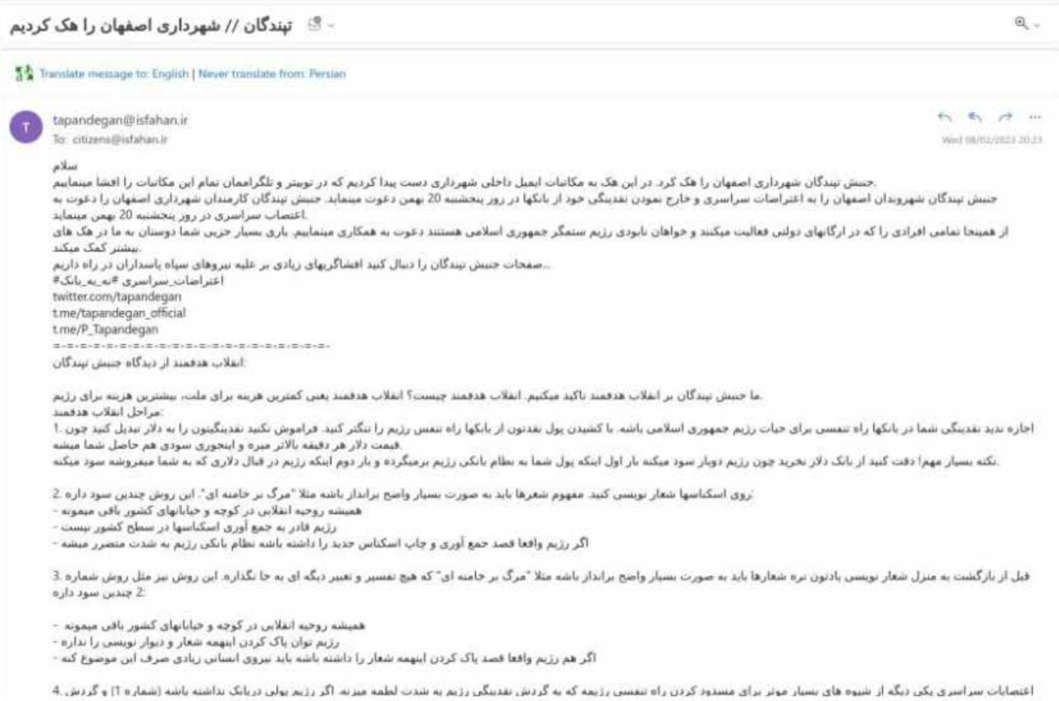
Third, leaked files also suggest extensive mismanagement of finances and lack of transparency in documentation and record keeping at the highest level of the university's board of trustees. One particular document details the findings of auditors about the university's finances. Recommendations include several lines about the lack of

[3] Leaked documents also show that this garment factory is part of the Imam Sadiq University conglomerate.

documentation of the university's real estate and other properties, a matter that allegedly has not been dealt with for years and could have significant tax evasion implications.

Imam Sadiq University was not the only target of Black Reward. On February 18, the group dumped new files from semi-official Fars News Agency, a key media affiliate of the IRGC. Black Reward had previously hacked Fars News in November 2022 and leaked confidential bulletins that outlined the regime's approach to suppressing the Woman, Life, Freedom protests. The latest file dump was allegedly the second batch of documents obtained around the same time. Leaked documents consisted of draft reports that Fars journalists had prepared, audio files of interviews (published or otherwise), bulletins (open source intelligence reports) that Fars had produced for IRGC leaders between 2019 and 2022.

The bulletins covered a range of topics, from social media analytics reports to the state of economy. Among them is a 247-word document[4], ostensibly prepared for the Supreme Council of Cyberspace, the main authority for monitoring cyberspace. The report dated February 4, 2021 presents an overview of the most popular Persian-speaking posts on Instagram (supposedly in the preceding week). Categories of posts include celebrities' daily life, music (produced by domestic and diaspora artists), domestic and



تپندگان // شهرداری اصفهان را هک کردیم

Translate message to: English | Never translate from: Persian

tapandegan@isfahan.ir
To: citizens@isfahan.ir
Wed 08/02/2023 20:23

سلام
جنبش تپندگان شهرداری اصفهان را هک کرد. در این هک به مکاتبات ایمیل داخلی شهرداری دست پیدا کردیم که در توییتر و تلگراممان تمام این مکاتبات را افشا مینماییم.
جنبش تپندگان شهروندان اصفهان را به اعتراضات سراسری و خارج نمودن نقدینگی خود از بانکها در روز پنجشنبه 20 بهمن دعوت مینماید. جنبش تپندگان کارمندان شهرداری اصفهان را دعوت به اعتصاب سراسری در روز پنجشنبه 20 بهمن مینماید.
از همینجا تمامی افرادی را که در ارگانهای دولتی فعالیت میکنند و خواهان نابودی رژیم ستمگر جمهوری اسلامی هستند دعوت به همکاری مینماییم. یاری بسیار جزیی شما دوستان به ما در هک های بیشتر کمک میکند.
صفحات جنبش تپندگان را دنبال کنید افشاگریهای زیادی بر علیه نیروهای سپاه پاسداران در راه داریم...
#اعتراضات_سراسری #نه_به_بانک
twitter.com/tapandegan
t.me/tapandegan_official
t.me/P_Tapandegan
=-
انقلاب هدفمند از دیدگاه جنبش تپندگان:

ما جنبش تپندگان بر انقلاب هدفمند تاکید میکنیم. انقلاب هدفمند چیست؟ انقلاب هدفمند یعنی کمترین هزینه برای ملت، بیشترین هزینه برای رژیم.
مراحل انقلاب هدفمند:
1. اجازه ندید نقدینگی شما در بانکها راه تنفسی برای حیات رژیم جمهوری اسلامی باشه. با کشیدن پول نقدتون از بانکها راه تنفس رژیم را تنگتر کنید. فراموش نکنید نقدینگیتون را به دلار تبدیل کنید چون قیمت دلار هر دقیقه بالاتر میره و اینجوری سودی هم حاصل شما میشه.
نکته بسیار مهم: دقت کنید از بانک دلار نخرید چون رژیم دوبار سود میکنه بار اول اینکه پول شما به نظام بانکی رژیم برمیگرده و بار دوم اینکه رژیم در قبال دلاری که به شما میفروشه سود میکنه.

2. روی اسکناسها شعار نویسی کنید. مفهوم شعرها باید به صورت بسیار واضح براندار باشه مثلا "مرگ بر خامنه ای". این روش چندین سود داره:
- همیشه روحیه انقلابی در کوچه و خیابانهای کشور باقی میمونه
- رژیم قادر به جمع آوری اسکناسها در سطح کشور نیست
- اگر رژیم واقعا قصد جمع آوری و چاپ اسکناس جدید را داشته باشه نظام بانکی رژیم به شدت متضرر میشه

3. قبل از بازگشت به منزل شعار نویسی یادتون نره شعارها باید به صورت بسیار واضح براندار باشه مثلا "مرگ بر خامنه ای" که هیچ تفسیر و تعبیر دیگه ای به جا نگذاره. این روش نیز مثل روش شماره 2 چندین سود داره:

- همیشه روحیه انقلابی در کوچه و خیابانهای کشور باقی میمونه
- رژیم توان پاک کردن اینهمه شعار و دیوار نویسی را نداره
- اگر هم رژیم واقعا قصد پاک کردن اینهمه شعار را داشته باشه باید نیروی انسانی زیادی صرف این موضوع کنه

4. اعتصابات سراسری یکی دیگه از شیوه های بسیار موثر برای مسدود کردن راه تنفسی رژیمه که به گردش نقدینگی رژیم به شدت لطمه میزنه. اگر رژیم پولی در بانک نداشته باشه (شماره 1) و گردش

Figure 2. Sample email sent by Tapandegan to Isfahani residents

[4] Document 991104 titled "شورای عالی فضای مجازی."

international news, celebrity posts related to human rights and good governance[5], among other topics.

This document is significant as, first, it shows the extent to which Fars News feeds information to the Supreme Council of Cyberspace, exerting indirect influence on the council's decision making and priorities. Second, the report hints at the role of Fars News in Iran's expansive surveillance apparatus. By monitoring social media and compiling detailed reports, they take the pulse of society in real life and package this information to decision-making bodies – playing informant, at best, and, at worst, being an official piece of digital surveillance processes.

Tapandegan

On February 8, another hacktivist persona Tapandegan returned with a new hack, this time targeting the Isfahan Municipality. Following the incident, Tapandegan sent text messages en masse to the residents of Isfahan, asking them to withdraw their savings and other assets from local banks to induce a monetary vacuum and bring the regime to the cusp of its collapse. The group sent similar emails to residents of Isfahan, staff of the municipality, and local and diaspora journalists.

In October 2022, Tapandegan infiltrated the online portal of Iran's Al-Zahra University, an all-female higher education institution historically known for its obsessive religious rules around hijab and admission requirements.

Wonder

On the same day as Tapandegan's attack, February 8, a new hacktivist persona made a debut appearance. Wonder took down the portal of Iran judiciary, claiming it was responding to multiple recent unjust execution sentences.

Edalate Ali

On February 9, Edalate Ali, a hacking collective that had previously

[5] Examples include Masih Alinejad's posts about the prison sentence for an indie filmmaker as well as women being banned from entering soccer stadiums. Another refers to a standup comedy show host speaking out about air pollution in Tehran, inviting residents to hold the authorities accountable.

leaked video footage of the notorious Evin prison, released a confidential report from the judiciary that quickly became controversial. The report describes in detail how two IRGC members – one also affiliated with the IRGC's intelligence arm – had sexually assaulted two young detainee women. According to the leaked report, said women were arrested at a gas station after two IRGC members inspected their phones and found 'anti-regime' and protest content. The officers then sexually assaulted their detainees on the way to an IRGC headquarter – an 'independent' detention center, according to the judiciary's report.

Following the incident, the two women tried to file a criminal complaint at a police station but were turned away with interference from the intelligence ministry. However, their statements invoked an investigation by the office of Prosecutor General that was filed under top secret. Not only did the investigation find IRGC officers guilty but also it elaborated on the findings of an inspection of the main defendant's home. Among the items found were drugs, weapons, as well as police and clerical costumes that the officer supposedly used for camouflage on IRGC missions.

The leaked report is significant in a number of ways. It explicitly documents the criminal conduct of IRGC officers against Iranian women and, by extension, dissidents. During the Woman, Life, Freedom protests, many accused the IRGC of suppressing the protestors, particularly women, by shooting at their genitals and sexually assaulting them. Detainees's accounts also repeatedly raised concerns about torture, blackmailing, and mistreatments in detention centers. This leaked report, produced by the judiciary's highest ranking officials, confirms these accusations. However, the report falls short of taking action against such wrong doings. It recommends the matter be handled with extreme caution to not raise public scrutiny. Instead, it advises that the officers be dismissed and their [IRGC] affiliations not be named in further reports.

Two days after this document leak, on February 11, Edalat Ali briefly took over Telewebion, a streaming service for the state-owned broadcaster (IRIB). The livecast of president Raisi's speech on the 44th anniversary of the Islamic Republic was interrupted, which lasted for about a minute with a logo of Edalate Ali appearing on the screen. A voice shouted "Death to the Islamic Republic."

On March 15, Edalate Ali exposed a judiciary letter regarding a lawsuit that involves relatives of the Supreme Leader, Ali Khamenei. The document suggests expansive financial corruption at their commercial company, including mishandling of financial records to evade audit.

Unknown

On the Persian New Year, an unknown hacktivist group hacked IRIB's Channel 2 during live celebrations. The livecase was converted to a show by a fictitious news channel show "DBC" a play on the "BBC."[6] The new year celebration was replaced with facetious, politically charged commentary and news programs. One segment even mimicked a PKK leader claiming that he did not have any secessionist views – a sarcastic reaction to recent debates among dissidents accusing ethnic minority activists of secessionist plans to disintegrate Iran.

Farhikhtegan newspaper confirmed the incident. However, no group claimed responsibility and no further statement was released by Iranian authorities or dissident groups.

LabDookhtegan

LabDookhtegan, one of the oldest, most prolific, allegedly Iranian hacktivist groups expanded on some of its previous leaks between March and June 2023. On March 23, the group disclosed additional documents about surveillance technologies, including for wiretapping and eavesdropping, that DSPRI, an IRGC-affiliated company, provides to the IRGC and its Quds Force. Additional information about DSPRI was posted to LabDookhtegan's Telegram channel on June 22.[7] On May 1, LabDookhtegan exposed two hackers of the IliaNet Gostar, a hacking group affiliated with the cyber division of the IRGC. Ilianet Gostar (aka Shahid Shushtri, Iman-net Pasargad, and Emenet Pasargad) became subject to U.S. sanctions in February 2022 for posing as Yemen Cyber Army in 2018. On May 18, LabDookhtan posted an assault video allegedly against Ali Mahdavian, one of IliaNet Gostar hackers, whom the US State Department has issued a $10-million reward for information for his attempt to interfere in the 2020 presidential election posing as ProudBoys, an American extremist group. On June 18, the group exposed two front companies of the IRGC that are allegedly

[6] BBC Persian is a popular news channel among Iranians.

[7] As part of these revelations, collaborations between top Iranian universities, such as Tehran University, and Unit 300 of the Quds Force also came to light.

manufacturers of Shahed-136 drones, which Iran exports to Russia for the war in Ukraine.[8]

Ghyam Sarnegouni

On May 7, GhyamSarnegouni[9] (Persian for Revolt to Overthrow (RTO)) claimed to have hacked the Iranian Ministry of Foreign Affairs (MoFA) servers and defaced 210 domains and websites. Defaced websites displayed pictures of Mujahedeen-e-Khalq (MEK) leaders. A news article about the hack also appeared on the MEK website. In the hours and days that followed, RTO posted troves of documents from the infiltrated MoFA servers covering various topics between early 2020 and April 2023. These included images of Basij[10] membership of high-ranking officials, such as the current foreign minister Hossein Amir-Abdollahian, and passport information of officials such as secretary general of Iran's Supreme Council of National Security.

Leaked documents also indicate some of Iran's highest priorities in foreign policy. The first is an obsession with the MEK and its presence in Albania. Iran's MoFa has repeatedly corresponded with the Albanian government and members of parliament to voice discontent with their accommodation of the "terrorist" MEK. Another priority was the detention of Assadollah Assadi, an Iranian diplomat that was arrested in Belgium in 2021 for a foiled bomb plot at the MEK's annual rally in France and sentenced to 20 years in prison. The Iranian government has been heavily lobbying for his release, which resulted in a prisoner swap with Belgium in May 2023.

On May 29, GhyamSarnegouni returned with a fresh leak. The group claimed on Telegram that "The entire highly protected internal network of the executioner president's office in Tehran was captured and out of reach." Over the next three hours, the group posted new files, images, and videos every few minutes – all categorized and clearly packaged for quick circulation. Around the same time, the MEK website reported "Iranian dissidents take over high-security servers of regime presidency," attributing the attack to GhyamSarnegouni.

[8] These entities include: Chekad Sanat Faraz Asia Company and Sadid Sazeh Zafaraz Sharif Company.

[9] GhyamSarnegouni emerged on Telegram on Jan. 26, 2022. From early days, its messaging has echoed the MEK, suggesting an affiliation of some kind. The group previously hacked different government entities, including the Tehran municipality CCTV cameras as well personal information of over 3000 staff members of Iran's judiciary as a form of protest.

[10] Basij is a paramilitary organization under the IRGC.

The group claimed it gained control of 120 servers connected to the presidential body's internal network and central databases and more than 1,300 computers on the network, access to classified internal communications to the presidency and the government, including classified, top secret, and secret documents, floor plans of the president's office, and IP addresses for facilities associated with the president as well as other top government leaders and institutions, including the interior and intelligence ministries and the Basij.

Leaked documents shed light on the regime's priorities on a range of critical issues, including the mechanisms of information control. For example, in a letter dated January 10, 2023,[11] General Salami, top commander of IRGC's Thar-Allah Headquarters that is in charge of security for the Tehran area, confirms that the internet must go down on the day of the college entry exam (کنکور in Persian). The move, purportedly suggested by the minister of higher education, was to protect the integrity of the exam by preventing cheating and distribution of questions ahead of time. However, it reaffirms a deeply rooted belief that the regime's silver bullet to any socio-political tension can be to unplug the internet, be it during political unrest or to preserve a major exam's integrity.

The second significant document is a top secret letter authored by the commander of IRGC's cyber affairs to President Raisi on March 30, 2023. The letter proposes sweeping changes to the makeup of the Supreme Council of Cyberspace with IRGC-endorsed individuals. The letter also advocates for an enhanced role for military forces, in particular the IRGC, in protecting Iran's gateways in cyberspace. The document goes as far as diminishing the authority of the executive branch (in particular the ministry of Information and Communications Technology (MoICT)). Instead, IRGC Cyber Commander recommends that military and intelligence bodies are better equipped to protect Internet exchange points (aka Iran's gateways to the global internet). In other words, the IRGC seeks to become the prime authority of cyberspace in Iran. This is despite a failed legal battle to codify the military's oversight of the Internet also known as the Internet Protection Bill.

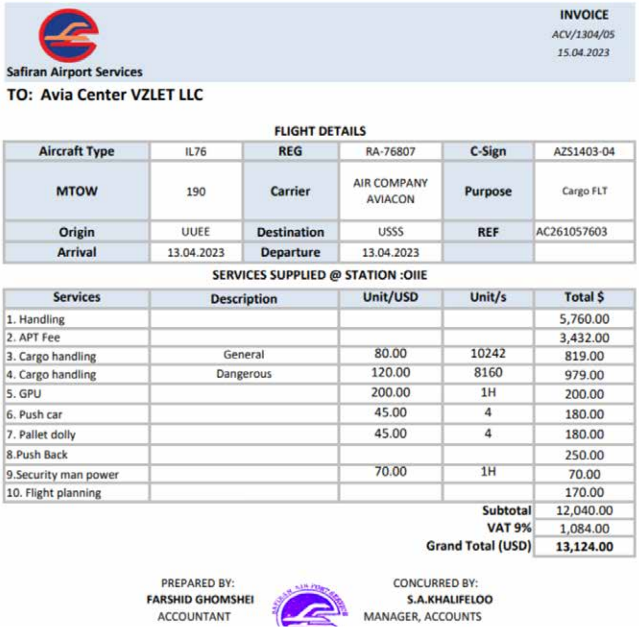
Leaked documents indicate the regime's sensitivity to ongoing protests at university campuses and shows the extent to which the IRGC is involved in suppressing these movements. Multiple

[11] Document titled "Salame-07" published by Ghyam Sarnegouni on May 29, 2023.

documents detail discussions at IRGC intelligence units about dealing with student and professor protesters. In a letter dated October 3, 2021 president Raisi asks the executive branch to use such hashtags as "#integrated_Iran" in their social media communications to promote a message of unity and anti-secessionist sentiments. This is a rare and obvious example of dictating state-endorsed narratives to pro-regime accounts on social media. Yet the regime has only dismissed the leak as inauthentic without providing further proof.

On June 20, less than a month after the attack on the presidential institution, the Albanian police raided MEK's camp near Manze, a small town 30 kilometers west of Tirana, Albania's capital. The police seized 150 computer devices allegedly linked to prohibited political activities, and several MEK members and police officers were injured. Albania has reportedly opened investigations into suspected political activities by MEK members. According to the agreement between the Albanian government and the MEK to shelter Mujahedeen members in 2013, the MEK is not supposed to engage in any political activity and must abide by the country's laws. If proven, the alleged activities that prompted the raid would be in violation of the agreement.
The United States government, which was the force behind MEK relocation from Iraq to Albania a decade ago, voiced support for the Albanian government to defend its sovereign right.

MEK members in Albania have proudly told local journalists how they have hacked or penetrated communication systems of the



Safiran Airport Services

INVOICE
ACV/1304/05
15.04.2023

TO: Avia Center VZLET LLC

FLIGHT DETAILS

Aircraft Type	IL76	REG	RA-76807	C-Sign	AZS1403-04
MTOW	190	Carrier	AIR COMPANY AVIACON	Purpose	Cargo FLT
Origin	UUEE	Destination	USSS	REF	AC261057603
Arrival	13.04.2023	Departure	13.04.2023		

SERVICES SUPPLIED @ STATION :OIIE

Services	Description	Unit/USD	Unit/s	Total $
1. Handling				5,760.00
2. APT Fee				3,432.00
3. Cargo handling	General	80.00	10242	819.00
4. Cargo handling	Dangerous	120.00	8160	979.00
5. GPU		200.00	1H	200.00
6. Push car		45.00	4	180.00
7. Pallet dolly		45.00	4	180.00
8.Push Back				250.00
9.Security man power		70.00	1H	70.00
10. Flight planning				170.00
			Subtotal	12,040.00
			VAT 9%	1,084.00
			Grand Total (USD)	13,124.00

PREPARED BY:
FARSHID GHOMSHEI
ACCOUNTANT

SAFIRAN AIR PORT SERVICES

CONCURRED BY:
S.A.KHALIFELOO
MANAGER, ACCOUNTS

Figure 3. A leaked invoice by Hooshyaran Vatan from April 2023 references handling of a "dangerous" cargo by a Russian air carrier.

Tehran government and Iranian institutions. It is unclear whether the activities in question refer to GhyamSarnegouni's hacking activities. The timing and circumstance of the raid are, at best, curious. It happened only a month after Iran suffered sweeping attacks on government networks from GhyamSarnegouni, an alleged MEK-affiliate hacking persona. According to leaked documents by the group, Iran has been preoccupied with the presence of the MEK in Albania and has tried different ways to undermine their agreement with the local government.

Ties between Iran and Albania have been tense since Albania gave MEK members a safe haven a decade ago. Last July, Albania suffered a cyberattack that the government and Microsoft attributed the attack to Iran's ministry of intelligence. The attack, believed to be in retaliation for Albania sheltering the Iranian opposition in exile, led Albania to sever diplomatic ties with Iran. The United States also imposed new sanctions on Iranian individuals and entities for the attack.

Hooshyaran Vatan

On June 17, another hacktivist persona Hooshyaran Vatan released emails of a commercial travel agency Safiran Airport Services (SAS). According to their Telegram post, SAS "facilitates the transfer of weapons from the IRGC to Imperial Russia." SAS is allegedly affiliated with the IRGC, offers VIP travel services to (mostly Russian) businessmen or entities that have financial dealings with the IRGC, even facilitates military cargo delivery to Russia. In doing so, SAS uses shell companies in Oman and the UAE to launder payments and bypass U.S. and other international sanctions. It specifically asks clients to refrain from including the company's name in banking transactions, presumably to evade being flagged. Leaked documents also show payment disputes between Russian entities and SAS. Hooshyaran Vatan claims that the revenue from these services fund IRGC's suppression of Iranian ethnic minorities.

The group has a history of exposing state-affiliated (or state-owned) airlines' dealings with the IRGC and its elite, extraterritorial combat unit (the Quds Force), etc.

Conclusion

Hacktivist collectives continue to target the Iranian government in seeming solidarity with Iranian dissidents. However, recent events, including the raid on the MEK camp in Albania, suggest that some hacker groups may have other origins and affiliations. It remains to be seen what kind of evidence, if any, the Albanian government offers once investigations into possible MEK cyber activities conclude. The jury is still out on the origins of other groups such as Black Reward.

Analysis of recent troves of leaked files shows intertwined priorities of the Islamic Republic on a range of social, political, technology, and foreign policy issues, an expansive involvement of the IRGC in governance, and its ambitious plans for even further expansion. Leaked documents also portray a battle between dissidents and their [seemingly] hacker sympathizers, on one hand, and the Islamic Republic, on the other. In an uneven struggle for justice, the dissidents are getting a leg up from hacktivist groups that may also be pursuing their own political purposes. The result is a field that is becoming more crowded and expansive evidence of the regime's corruption and repression. Hacktivists (and their possible sponsors) are weaponizing Iran's own tactics head-on.