

Iran turning to cyber-enabled influence operations for greater effect

May 2, 2023

Microsoft Threat Intelligence

01010111 01101000 01101001
01101100 01100101 00100000
01110011 01100101 01100101
01101011 01101001 01101110
01100111 00100000 01101110
01100101 01110111 00100000
01100011 01111001 01100010
01100101 01110010 01100001
01110100 01110100 01100001
01100011 01101011 00100000
01100011 01100001 01110000
01100001 01100010 01101001
01101100 01101001 01110100
01101001 01100101 01110011

++
++



Table of contents

- 3 Introduction
 - 4 Iran increasing pace of cyber-enabled IO
 - 10 Leveraging cyber-enabled IO to pack a bigger retaliatory punch
 - 11 Trends in influence methods
 - 12 Trends in cyber threats
 - 13 Looking ahead
- 

Introduction

Iranian state actors have latched onto a new set of preferred techniques, combining cyber and influence operations (IO)—what we refer to as cyber-enabled influence operations—for greater geopolitical effect. Multiple Iranian state groups have turned to cyber-enabled IO more regularly since June 2022 to boost, exaggerate, or compensate for shortcomings in their network access or cyberattack capabilities. More fundamentally, they have combined offensive cyber operations with multi-pronged influence operations to fuel geopolitical change in alignment with the regime's objectives. This has included operations this year that have sought to bolster Palestinian resistance, foment Shi'ite unrest in Bahrain, and counter the normalization of Arab-Israeli ties.¹

The increased convergence of cyber and influence operations by Iranian groups follows on the heels of highly sophisticated cyberattacks against Iran since July 2021. Iran's inability to match the sophistication of some of the cyberattacks it has faced likely prompted the regime to find innovative methods to retaliate in a way that appeared proportional—to align with their national security preference of proportional and directed retaliation.²

As Iranian threat actors improve their capabilities, they are likely to continue to hone both their cyber and influence

techniques to match the highly sophisticated cyberattacks of their adversaries in an attempt at proportional retaliation. Continued improvements in Iranian threat actors' offensive cyber methods will enhance their ability to be more selective in targeting, including against higher-profile targets, while their new influence techniques will add to the amplification, realism, and ultimate effectiveness of their campaigns.

This report will focus on the likely reasons for Iran's increased use of cyber-enabled influence operations, the techniques being utilized, and the potential for future threats.

The report also provides a semi-annual update on improvements demonstrated by Iranian state-sponsored actors in both cyber operations and influence methods since late 2022.

Microsoft will publish semi-annual updates on these and other nation state actors to warn our customers and the global community of the threat posed by such operations, identifying specific sectors and regions at heightened risk.

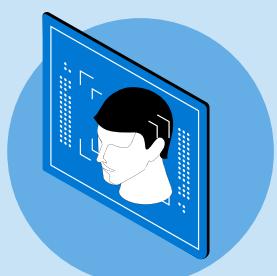


Key terms defined



Cyber-enabled influence operations

Operations which combine offensive computer network operations with messaging and amplification in a coordinated and manipulative fashion to shift perceptions, behaviors, or decisions by target audiences to further a group or a nation's interests and objectives.³



Cyber persona

A manufactured public-facing group or individual that takes responsibility for a cyber operation while providing plausible deniability for the underlying group or nation responsible.



Sockpuppet

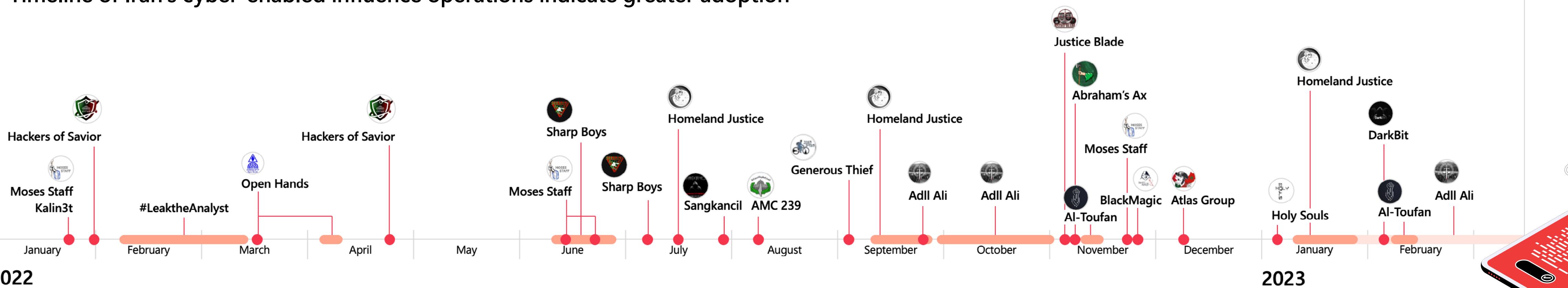
A false online persona employing a fictitious or stolen identity for the purpose of deception.

Iran increasing pace of cyber-enabled IO

Iran's integration of cyber and influence operations has accelerated since June 2022. Microsoft linked 24 unique cyber-enabled influence operations to the Iranian government in 2022—including 17 since mid-June—compared to seven in 2021 (see Figure 1).⁴ The rise in these operations, which may be partly attributable to improvements in our detection capabilities, has corresponded with a decline in ransomware or wiper attacks by groups linked to Iran's military, notably the Islamic Revolutionary Guard Corps (IRGC). As we previously reported, Microsoft detected a spike in such attacks from IRGC and Ministry of Intelligence and Security (MOIS) groups from 2020 to mid-2022.⁵ The IRGC's latest string of cyber-enabled IO in the last year has leveraged low-impact, low-sophistication cyberattacks, such as defacements, which are less time and resource intensive, while dedicating more effort to its multi-pronged amplification methods.

Figure 1

Timeline of Iran's cyber-enabled influence operations indicate greater adoption



In the past year, Iran's cyber-enabled influence operations have pushed narratives seeking to bolster Palestinian resistance, foment Shi'ite unrest in the Gulf, counter the normalization of Arab-Israeli diplomatic and economic relations, sow panic or fear among Israelis,⁶ and expose corrupt or embarrassing activity of Iranian adversaries.⁷ As we explore below, some operations pursued multiple influence narratives.

Bolstering Palestinian resistance

In mid-February, a probable Iranian group we track as Storm-1084 (DEV-1084) coupled destructive cyberattacks with messaging encouraging action in response to Israel's policies toward Palestinians. The group presented their attacks as ransomware and posted data for sale on the dark web using the cyber persona DarkBit, likely to enhance Iran's plausible deniability. The ransomware included a ransom note using the cyber persona with the same message DarkBit

posted on Telegram, calling Israel "an apartheid regime" that should "pay for occupation, war crimes against humanity, killing the people," including Palestinians. This type of messaging was previously commonplace among groups that we assess conducted cyber-enabled IO for the IRGC (see Figure 3).⁸

As detailed in a Microsoft Security blog on April 7, another Iranian state actor linked to Iran's MOIS likely gained remote

access to enable Storm-1084's attacks.⁹ The operations also impacted on-premises and cloud environments and likely entailed greater time, resources, and skills than most of the IRGC's other recent cyber-enabled influence operations. The operation used several techniques and tools—including some customized backdoors—to gain access, maintain persistence, escalate privileges, and execute the attacks.¹⁰

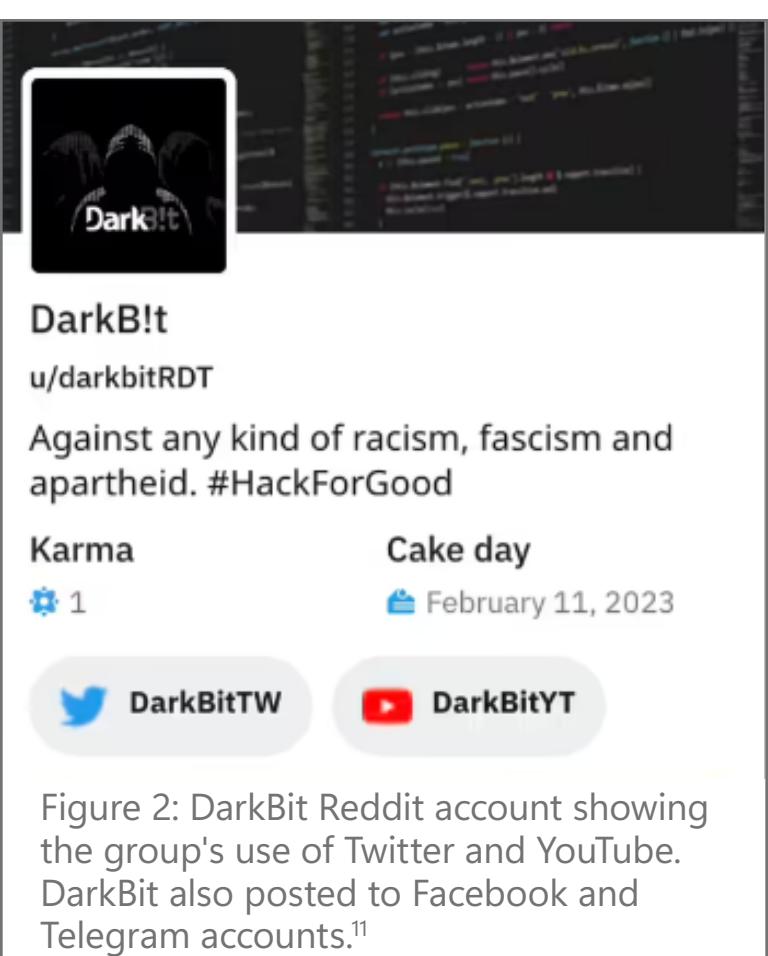
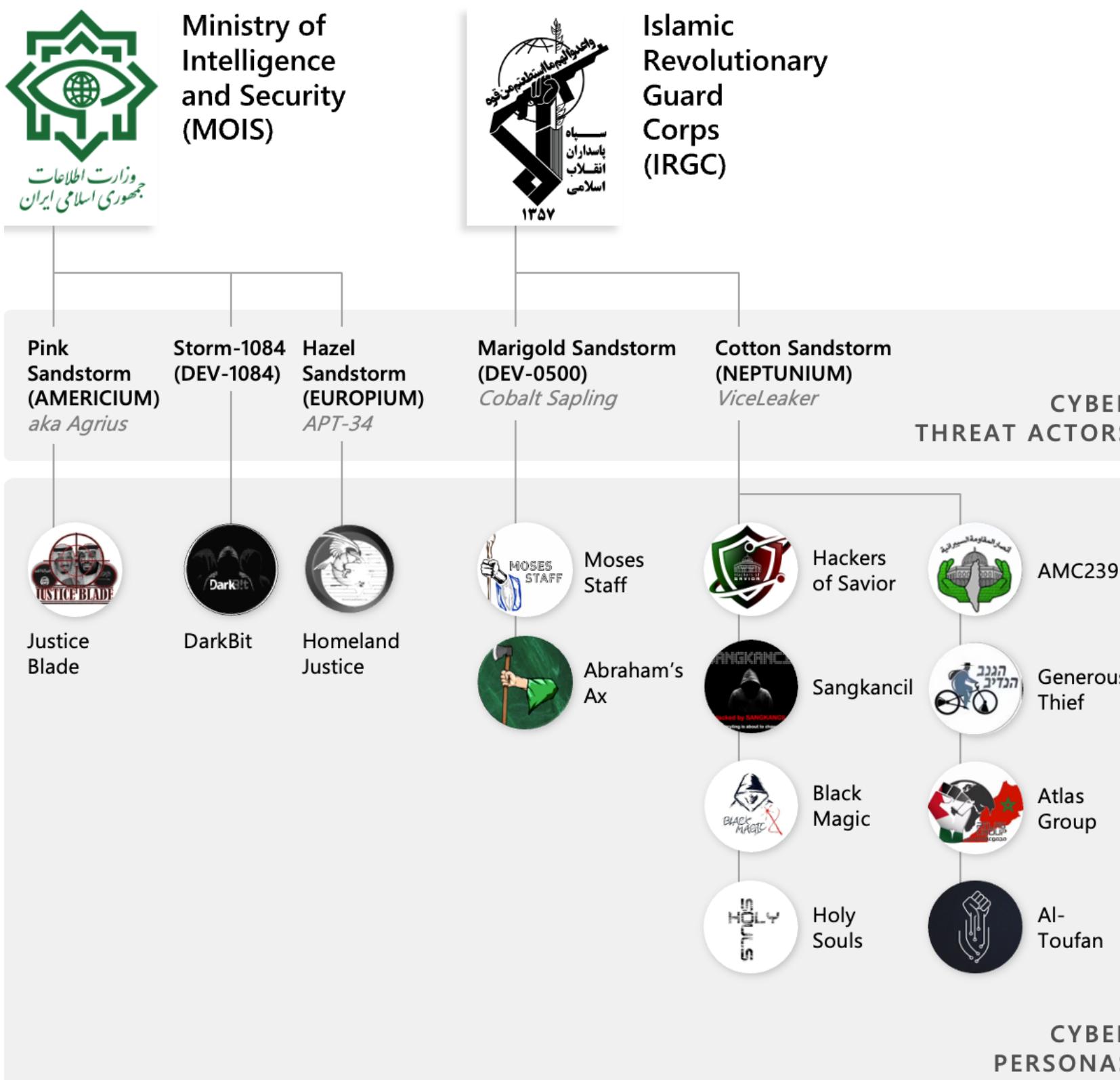


Figure 2: DarkBit Reddit account showing the group's use of Twitter and YouTube. DarkBit also posted to Facebook and Telegram accounts.¹¹

Figure 3

Iranian state actors at the crossroads of cyber and influence operations



MOIS and IRGC groups have adopted the use of cyber-enabled IO. This report uses Microsoft's new threat actor naming taxonomy. For details on the new taxonomy and a cross reference to Microsoft's old names (in parentheses in this report) see our blog and reference guide.¹²

Figure 4

Cotton Sandstorm's cyber-enabled influence operations

Cyber Persona	Hackers of Savior	AMC239	Sangkancil	Generous Thief	Black Magic	Atlas Group	Holy Souls	Al-Toufan
Most Recent Operation	Apr 2022	Jul 2022	Aug 2022	Sep 2022	Nov 2022	Dec 2022	Jan 2023	Feb 2023
Cyber Method								
Data theft	🏃	🏃	🏃	🏃	🏃	🏃	🏃	🏃
Defacement	💥	💥	💥		💥	💥	💥	💥
DDoS								💥
Ransomware					🔒			
Influence Method								
Data leak			📁	📁	📁	📁	📁	
Sockpuppets	👤	👤	👤	👤	👤	👤	👤	👤
Impersonation of victims			🎭	🎭	🎭	🎭	🎭	🎭
Sharing into social media groups/pages	📋	📋	📋	📋	📋	📋	📋	📋
SMS/ Email					✉️		✉️	

Microsoft assesses that most of Iran's cyber-enabled influence operations are being run by Emennet Pasargad—which we track as Cotton Sandstorm—an Iranian state actor sanctioned by the US Treasury Department for their attempts to undermine the integrity of the 2020 US Presidential Elections.¹³ We assess that Cotton Sandstorm has run or been involved in all eight of these fictitious cyber group personas since 2022. As this chart demonstrates, Cotton Sandstorm's influence tactics, techniques, and procedures (TTPs) have expanded and improved since mid-2022. We assess the groups are linked to Cotton Sandstorm based on extensive overlaps in influence TTPs. We have higher confidence in some of the groups' links to Cotton Sandstorm based on information released by the US government,¹⁴ victim overlaps, or forensic links between Cotton Sandstorm and the influence operations. Information shared by industry partners at Meta also boosted our confidence levels in attributing some of these cyber personas to Cotton Sandstorm. See: The Digital Threat Analysis Center's Attribution Model for Influence Operations for a fuller treatment of how we determine confidence levels.¹⁵

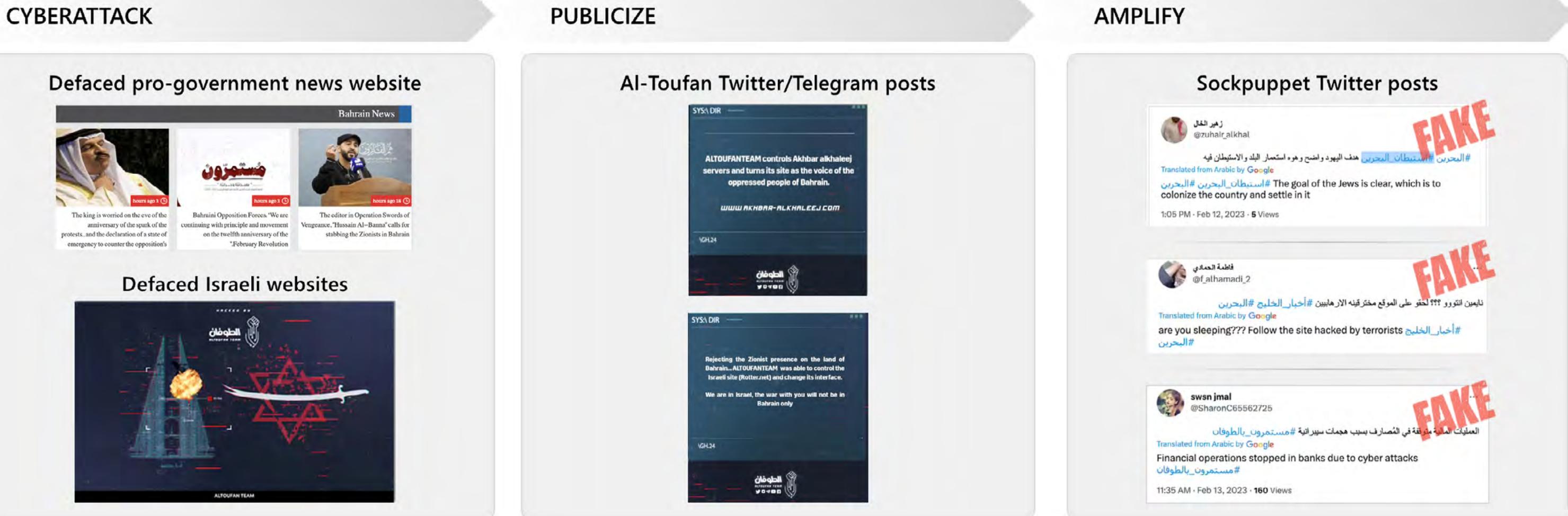


Fomenting Shi'ite unrest in Bahrain

In mid-February, cyber persona Al-Toufan ("the flood" in Arabic) claimed to deface several Bahraini and Israeli websites in conjunction with the 12th anniversary of the outbreak of nationwide anti-government protests in Bahrain. Al-Toufan, which we assess is run by Cotton Sandstorm, targeted Bahraini news and government websites to foment unrest among the politically underrepresented Shi'ite majority in Bahrain by encouraging protests and highlighting poverty and inflation. In its initial defacement of a pro-government news website on February 11, Cotton Sandstorm replaced legitimate content with articles critical of the regime and promoting protests.¹⁶ Arabic-language inauthentic social media accounts, or sockpuppets, later amplified Al-Toufan's claimed defacements.

Figure 5

Cotton Sandstorm's cyber-enabled IO playbook



Both of Cotton Sandstorm's operations in Bahrain followed a predictable playbook for cyber-enabled influence operations that they have replicated elsewhere. Following a low-sophistication **cyberattack** (e.g., a defacement), a fictitious cyber persona **publicizes** and exaggerates the attacks on social media, before seemingly unassociated sockpuppets **amplify** the news in the language of the target audience. As was the case in Al-Toufan's operation against Bahrain's elections, the group's initial amplification sometimes entails the impersonation of accounts of a targeted organization, or a senior official at that organization, to add credibility to the cyberattack.

In November, Cotton Sandstorm conducted its first cyber-enabled influence operation under the guise of Al-Toufan against Bahrain's parliamentary elections using a similar playbook (see Figure 5). The operation also sought to foment unrest among Bahraini Shi'ites, in part by delegitimizing the elections. One day ahead of the November 12 vote, Al-Toufan claimed to disrupt Bahrain's

parliament website (nuwab.bh) in support of boycotting the elections and in response to Bahraini authorities' "persecution," presumably a reference to Manama's political dissolution of Shi'ite groups.¹⁷ Although the cyberattacks only temporarily disrupted nuwab.bh and a news site, Cotton Sandstorm had hundreds of Twitter and Instagram sockpuppets ready to amplify

and exaggerate the impact of the attacks. In fact, some of the sockpuppets impersonated Bahrain's parliamentary and municipal elections organization and its executive director, claiming the election might be postponed. Dozens of sockpuppets then amplified the fake news of an election delay.

Countering normalization of Arab-Israeli ties

We assess that Cotton Sandstorm conducted another campaign using the cyber persona Atlas Group to counter the normalization of Arab-Israeli relations. On December 10, Atlas Group claimed to deface an Israeli sports website with a message stating that Israelis were not welcome at the World Cup in Qatar, or in any Muslim countries. Similar to operations in Bahrain, Cotton Sandstorm leveraged dozens of sockpuppets to amplify the news and intensify anti-Israeli sentiment, drawing on a simple URL manipulation exploiting an open redirect in the URL on a Sport5 webpage. This influence operation took place during the World Cup quarterfinals, one month after Israel and Qatar agreed to establish direct flights for the games.¹⁸



Figure 6: Image that Atlas Group publicized on its social media pages and in text messages posing as Sport5.

Sowing panic in Israel

On Black Friday in late November, another cyber persona likely run by Cotton Sandstorm called BlackMagic claimed to deface dozens of Israeli websites, leaked shipping and personal data from logistics companies, and posted a video of a cyber operator altering destinations in the product distribution logs of an Israeli shipping company. The lack of corroborating evidence that the group affected actual shipments suggests the operation was another example of Cotton Sandstorm using an influence operation to exaggerate the effects of its cyberattacks. This is similar to its false claims of having cast ballots in the 2020 US Presidential Elections.¹⁹ The operation sought to disrupt retail shipping, or at least provide the appearance of such disruption, likely to spark panic among Israelis.



Figure 7: BlackMagic Telegram post of Israeli retail and logistics companies it claimed to impact.

We assess Cotton Sandstorm was behind the BlackMagic persona based on forensic links and the use of several similar amplification TTPs. A BlackMagic-labeled ransomware and a Cotton Sandstorm-linked tunneling tool used in the operation were hosted on an IP that we assess was linked to Cotton Sandstorm.²⁰ Similar to other Cotton Sandstorm influence operations, sockpuppets associated with the BlackMagic campaign impersonated Israelis on Twitter and Facebook (in some cases re-using the same fake accounts from other campaigns), published messages seeking to undermine trust in Israeli institutions, and posted messages to inauthentic community groups targeting Israelis. They also used Twitter accounts masquerading as breached Israeli businesses.

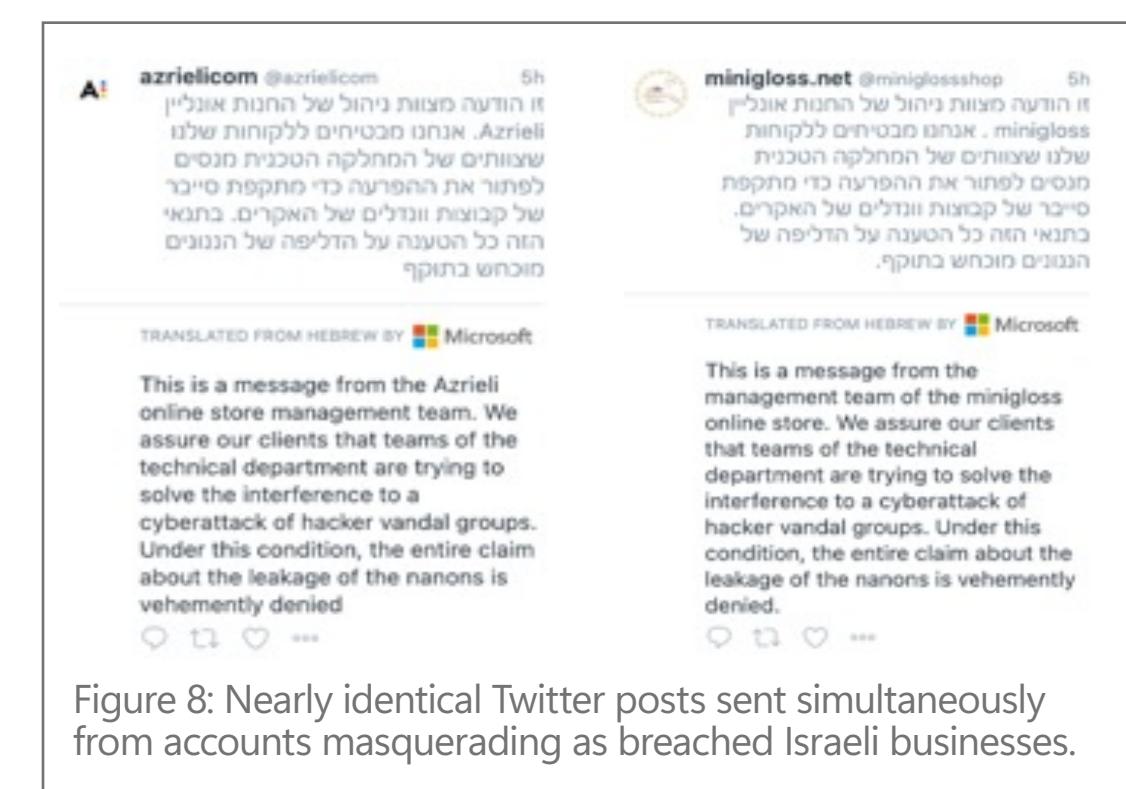


Figure 8: Nearly identical Twitter posts sent simultaneously from accounts masquerading as breached Israeli businesses.

Another Iran-linked cyber persona, Moses Staff, released closed-circuit television (CCTV) footage of one of the November 23 Jerusalem bus station bombings, likely to sow fear among Israelis. The group's access to and release of the sensitive footage on the same day as the attacks suggests involvement in the planning of the attack on civilians, even though the Iranians may not have been responsible for the bombing itself.²¹ Microsoft assesses that Moses Staff is operated by an Iranian state actor other than Cotton Sandstorm, which we track as Marigold Sandstorm. In contrast to Cotton Sandstorm, we have not detected Moses Staff amplifying cyberattacks on social media using sockpuppets. We have also not detected an overlap in victims between Moses Staff and Cotton Sandstorm.



"Exposing" their adversaries

Iran has adopted cyber-enabled IO to undercut the momentum of nationwide protests by leaking information that aims to embarrass prominent regime opposition figures or to expose their "corrupt" relationships. Shortly after the outbreak of anti-government protests in Iran in late September, a new cyber persona, Adll Ali, which we assess is acting on Iran's behalf, began leaking information to slander several prominent Iranian opposition figures. Their targets included the eldest son of Iran's former Shah (the leader of Iran's former

monarchy) and Masih Alinejad, a vocal Iranian-American women's rights activist.²² Adll Ali's first posts exploited documents they claimed to have acquired from a cyber operation against a Kurdish separatist group, the Komala Party. Adll Ali sought to shift blame onto the Komala Party for orchestrating protests in Iran and possibly the events that led to the arrest of Mahsa Amini, who died at the hands of Iranian morality police in September 2022, sparking nationwide protests.²³

Iranian state actors have executed an ongoing and nearly year-long set of cyberattacks and influence operations against the Albanian government questioning Tirana's harboring of the Mujahideen-e Khalq (MEK), an Iranian dissident group that seeks to overthrow the Islamic Republic. As Microsoft disclosed in September, we assess multiple Iranian actors linked to the MOIS were responsible for the initial data deletion attack and follow-on influence operations against Tirana over the summer.²⁴ Iran has sought to boost its influence narrative

by exposing the alleged corruption of Albania's political leaders and nefarious links between the MEK and Tirana. In January, the cyber persona taking responsibility for the attacks, Homeland Justice, leaked personal details of banking customers, claiming they revealed Albanian officials had laundered money from the MEK.

Hacktivists stoking anti-regime protests

Since October, several anti-regime hacktivist groups have conducted cyberattacks and hack-and-leak operations against Iran to foment nationwide protests. Several anti-regime cyber groups (e.g., Lab Dookhtegan, Edaalate Ali) shifted their focus to the protests while other new groups cropped up (Bakhtak, Black Reward, ZZA Hackers) specifically focused on the protests. All the groups regularly used slogans from the nationwide protests, such as #Mahsa_Amini and #زن_زندگی_آزادی (Woman, Life, Freedom). Cyber groups claiming to be hacktivists, such as Black

Reward, Lab Dookhtegan, ZZA Hackers, and Edaalate Ali have leaked Iranian government email databases, defaced government-linked websites, hacked and interrupted Iranian state TV broadcasts, and have more generally tried to embarrass the Iranian government. Other more prolific but less sophisticated anti-regime cyber activity, including Distributed Denial-of-Service (DDoS) attacks and hack-and-leaks of government data, have centered around "Anonymous" branded groups and hacktivist collectives with indeterminate backing.

Anti-regime cyber personas



Black Reward:
Leaked internal communications of state-linked media



"Anonymous":
Targeted regime-linked websites



Bakhtak:
Leaked data of IRGC officials and regime corruption



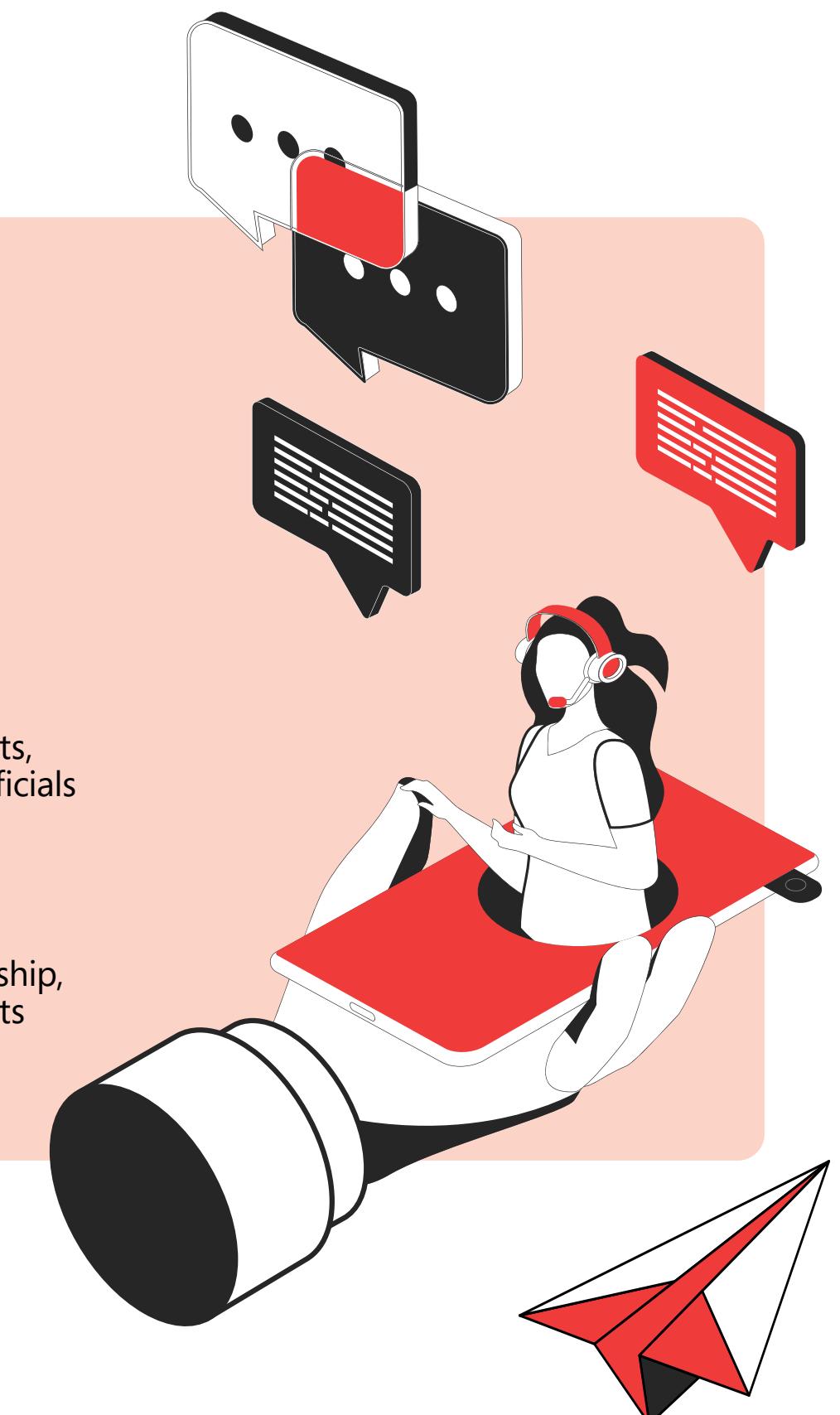
Edaalate Ali:
Amplified calls for protests, leaked data of regime officials



Lab Dookhtegan:
Exposed Iranian cyber actors



ZZA Hackers:
Exposed regime's censorship, protest surveillance efforts



Leveraging cyber-enabled IO to pack a bigger retaliatory punch

Iran's cyber-enabled influence operations have sought to retaliate for cyberattacks or cyber-enabled IO against Iran on multiple occasions. In September, Homeland Justice leaked CCTV feeds from border crossings and Albania police, whose systems were reportedly impacted by a cyberattack.²⁵ We assess the attack on the police-controlled information system was retaliation for the Albanian police's raid on the Iranian Embassy in Tirana the day prior.²⁶ The published CCTV feeds likely sought to mimic an anti-Iran group, Edaalate Ali, which released CCTV footage showing the disruption of surveillance video at Iran's notorious Evin prison with a defacement message in 2021 (see Figure 9). As the images below depict, Iran's cyber operation did not send as clear a message in the attack itself, requiring close examination of the CCTV feeds to notice border agents' operations were impacted.

In some cases, Iran's cyber-enabled influence operations likely sought retaliation for highly sophisticated cyberattacks that Iran could not rival. Cotton Sandstorm's targeting of Israel's transportation sector in the BlackMagic campaign mirrored the sector targeted in Iran repeatedly in 2021 by an anti-Iran group called Predatory Sparrow. The BlackMagic operation's influence objective also mimicked what several senior Iranian leaders viewed as the aim of Predatory Sparrow's cyberattacks against Iran's fueling stations—to cause anger and disorder.²⁷ In contrast to the cyberattack in Iran that impacted fueling stations nationwide, BlackMagic leveraged low-sophistication defacements, network access, and a likely doctored video to make the impact of their operation appear comparable (see Figure 10).

In February 2022, Cotton Sandstorm attempted to conduct a cyberattack against an Israeli logistics facility, which operates terminals at major Israeli seaports.²⁸ The cyberattack likely sought to retaliate for a cyberattack in May 2020 against a major Iranian port, which some US and foreign government officials pinned on Israel.²⁹ Unlike the cyberattack on Iran's port, which brought sea and land traffic to a halt, Iran's cyberattack was likely caught prior to full execution, judging from the limited impact beyond the Israeli company having to temporarily shut down some of its computers.³⁰ In spite of a lack of meaningful impact on operations, Cotton Sandstorm resorted to an influence operation under the guise of Hackers of Savior, publicizing access to CCTV footage at the facility in an attempt to prompt fear among Israelis.



Figure 9: Edaalate Ali leaked CCTV footage showing defaced monitoring equipment at Iran's notorious Evin prison from 2021. Text reads, "Evin prison is a shameful stain on [President] Raisi's black turban and white beard. Widespread protests until the freedom of political prisoners."



Figure 10: Homeland Justice leaked video in September 2022 of CCTV footage of border control station with long lines where agents are using their phones while computers appear down.³¹

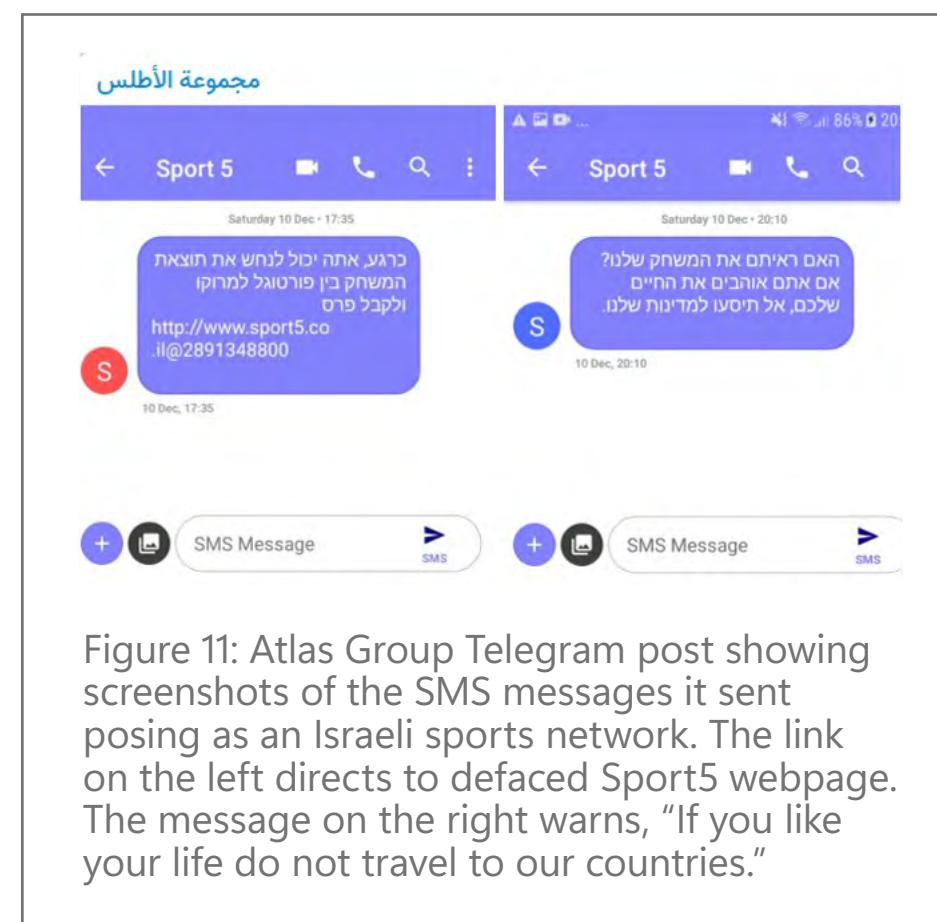
Trends in influence methods

Iranian state actors have honed their influence techniques through an increased use of cyber-enabled IO. They have added two new amplification methods to their toolkit.

1

SMS messaging to contact a target audience

Microsoft observed multiple Iranian actors attempting to use bulk SMS messaging in three cases in the second half of 2022, likely to enhance the amplification and psychological effects of their cyber-influence operations. We assess that Cotton Sandstorm was partially successful in at least one case in December. According to the FBI, as of early 2021, Cotton Sandstorm had demonstrated an interest in leveraging bulk SMS services to broadly disseminate its messaging.³²



In December, Cotton Sandstorm sent SMS messages, ostensibly from the Sport5 network they targeted warning Israelis not to travel to Muslim countries. One such message included a link to an altered Sport5 webpage. The SMS messages likely served to exaggerate the effects of the cyberattack and to sow panic among Israelis.³³ Sport5 confirmed that SMS messages posing as them were sent to thousands of people. This included at least some Israelis who had planned travel to Arab Gulf countries, according to separate Israeli press reports.³⁴

2

Impersonating victims to add credibility

Late last year, Cotton Sandstorm began impersonating purported victim organizations, or leading figures in those organizations, to add credibility to the effects of the cyberattack or compromise. In November, the BlackMagic operation included the impersonation of several Israeli retailers whom the cyber persona claimed to hack. Al-Toufan's operation impersonated an official from Bahrain's election organization. Likewise, in January, an operation amplified by the Holy Souls persona used inauthentic Twitter accounts spoofing the editor-in-chief of French satirical magazine Charlie Hebdo.³⁶ As is often the case with sockpuppets created by Cotton Sandstorm, the inauthentic accounts were created in the weeks leading up to the publicized cyberattack or data leak.



Trends in cyber threats

While lagging behind their Russian and Chinese counterparts in sophistication, Iranian nation state actors have added some new tools and techniques to their arsenal. This continued advancement in sophistication will enhance their ability to acquire access to specific targets of interest and maintain persistence while avoiding detection, a challenge they likely faced in some of their cyber-enabled influence operations since 2022.

1

Rapid adoption of N-day vulnerabilities

Iranian state actors have increased the speed with which they are operationalizing newly reported exploits to compromise organizations. On January 19, the same day the proof-of-concept (POC) code was publicly released, a group we track as Mint Sandstorm (PHOSPHORUS) began exploiting a remote code execution vulnerability in Zoho ManageEngine (CVE-2022-47966), a suite of products used to manage enterprise IT.³⁷ In February, Mint Sandstorm incorporated an exploit for a newly disclosed vulnerability only five days after a POC code was publicly reported (CVE-2022-47986).³⁸ This was a pre-authentication remote code execution vulnerability in an IBM file transfer application.

Microsoft has observed Iranian state actors continuing to rely on older vulnerabilities as well, including Log4Shell, to compromise vulnerable devices. As this activity is typically opportunistic and indiscriminate, Microsoft recommends that organizations regularly patch vulnerabilities with publicly available POCs, regardless of how long the POC has been available.

2

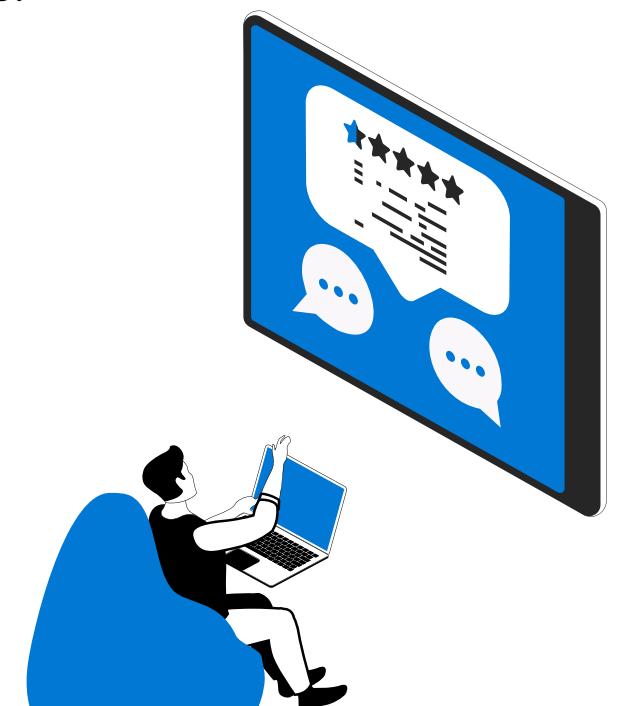
Use of victim websites for C2

Beginning in late 2022, an Iranian actor we assess is linked to Iran's MOIS, Storm-0133 (DEV-0133), used custom malware to establish communication between an already compromised Israeli website and multiple other in-country victim networks. The MOIS group used the legitimate yet compromised Israeli website for command and control (C2), demonstrating an improvement in operational security, as the technique complicates defenders' efforts, which often leverage geolocation data to identify anomalous network activity. Storm-0133's campaign exclusively targeted Israeli organizations, affecting local government agencies and companies serving the defense, lodging, and healthcare sectors.

3

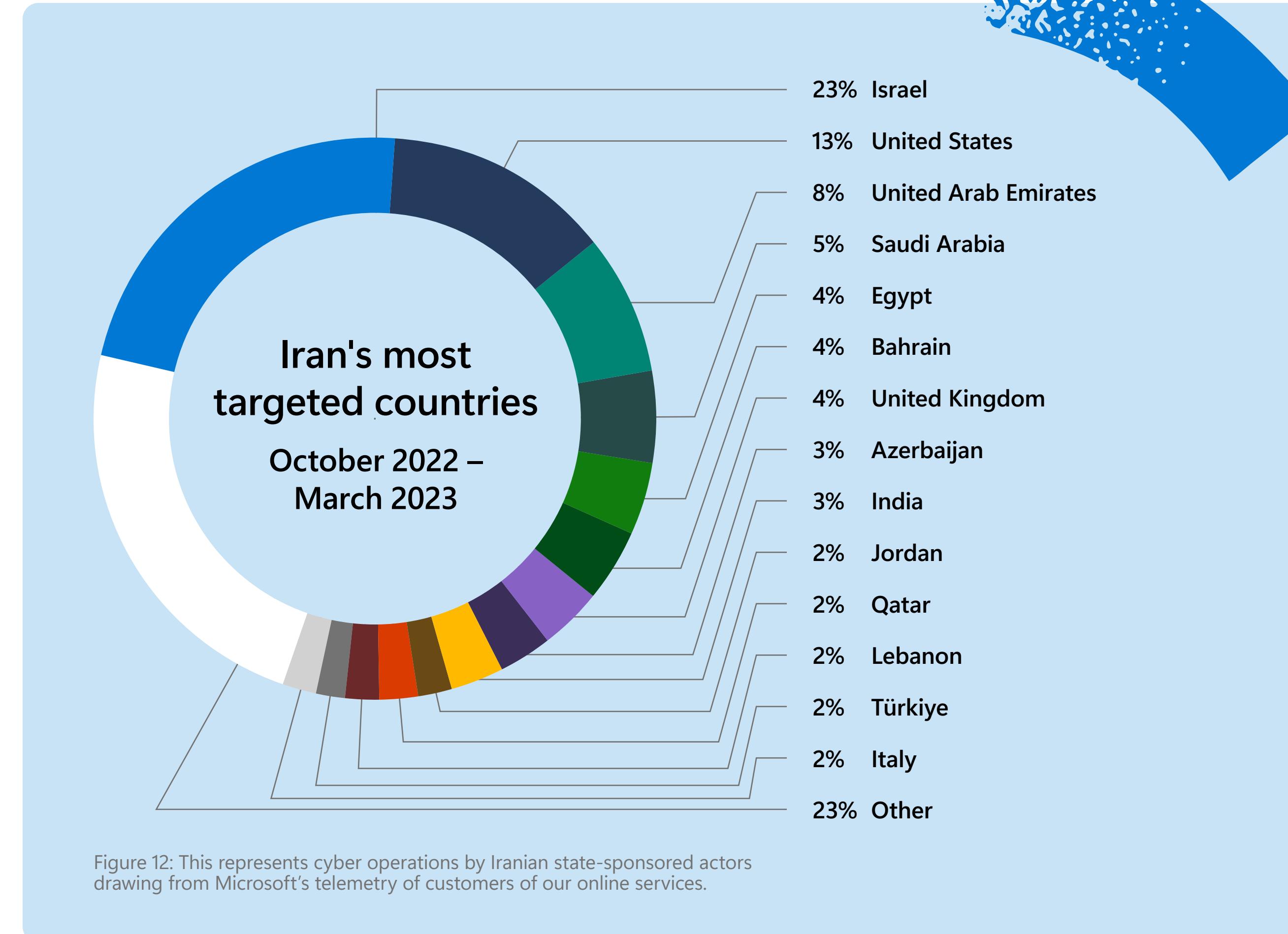
Steady use of custom tooling

IRGC and MOIS groups used custom tooling against targets of interest in early 2023. The shift away from publicly available tools and simple scripts towards the development and use of bespoke implants suggests that at least a subset of operators are capable of increasingly sophisticated tradecraft. The malware that Storm-0133 used against Israeli organizations was a custom malware that we refer to as Mango malware. Mint Sandstorm's exploitation of CVE-2022-47986 also involved a custom PowerShell script designed with built-in obfuscation to scrape information from victims. Mint Sandstorm developed another pair of custom tools that Microsoft has detected in use since 2022: Drokbk and Soldier (a more sophisticated variant of Drokbk). These implants are backdoors that operators use to persist in target environments and deploy additional tools. These tools use GitHub to host a domain rotator, tradecraft that allows operators to dynamically update their C2 and potentially evade static block lists implemented by defenders.



Looking ahead

Iranian cyberattacks and influence operations are likely to remain focused on retaliating against foreign cyberattacks and perceived incitement of protests inside Iran. Israel, followed by the United States, is likely at highest risk for future such operations, particularly in the near term given Iran's rapprochement with Saudi Arabia and diplomatic blitz of other Arab Gulf nations in March.³⁹ Israeli and US organizations have consistently been the most common targets of Iranian cyber operations in the past year, with a further increase in Israeli targeting in the past six months, judging from Microsoft data (see Figure 12). In October, Supreme Leader Khamenei and Iran's intelligence agencies blamed Israel and the United States for inciting protests in Iran, while other key regime figures have blamed Israel and the United States for major cyberattacks against Iran.⁴⁰

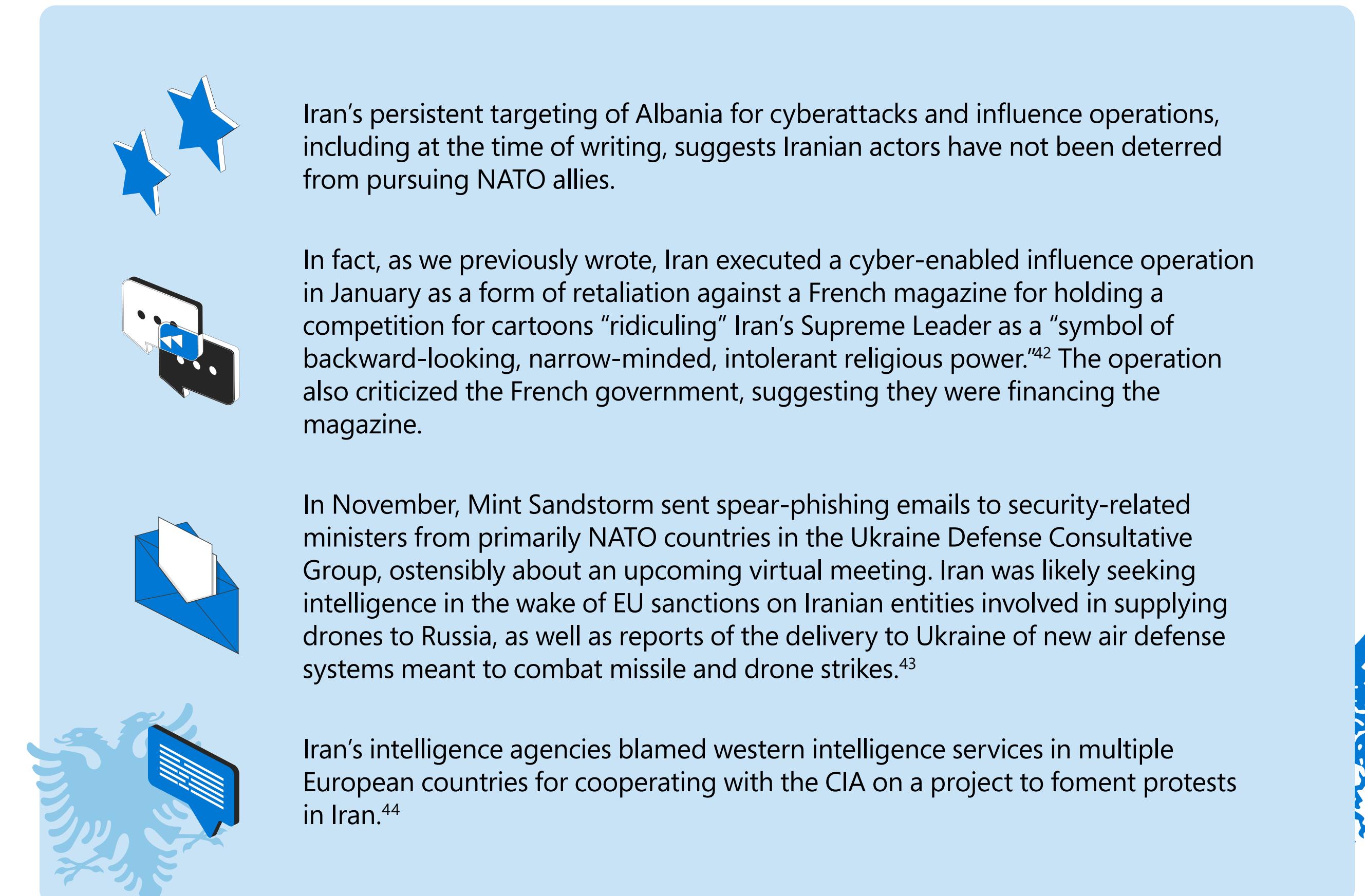


In its operations against the Albanian government, Iran signaled that the attacks were also aimed at Israel or would be in the future. Homeland Justice's logo, which they used in both the ransom note and regularly on their public posts, was an eagle preying on the logo of the Predatory Sparrow group inside a Star of David (see Figure 13). Predatory Sparrow conducted highly sophisticated cyberattacks against Iran that delayed trains in July 2021, impacted gas fueling pumps across the country in October 2021, and caused a fire at an Iranian steel factory by adjusting controls at the facility in June 2022.⁴¹



Figure 13: Homeland Justice banner and ransomware image of an eagle preying on the Predatory Sparrow symbol inside a Star of David.

NATO member nations and European countries may also be at a heightened risk of future Iranian cyber and influence operations. The increased aggressiveness of Iranian actors since 2021, including Iran's first cyberattack directly against a NATO government (Albania) in July 2022, indicate a less bounded operating environment and portend a greater future threat for less conventional Iranian targets, such as other NATO members.



Iran's persistent targeting of Albania for cyberattacks and influence operations, including at the time of writing, suggests Iranian actors have not been deterred from pursuing NATO allies.

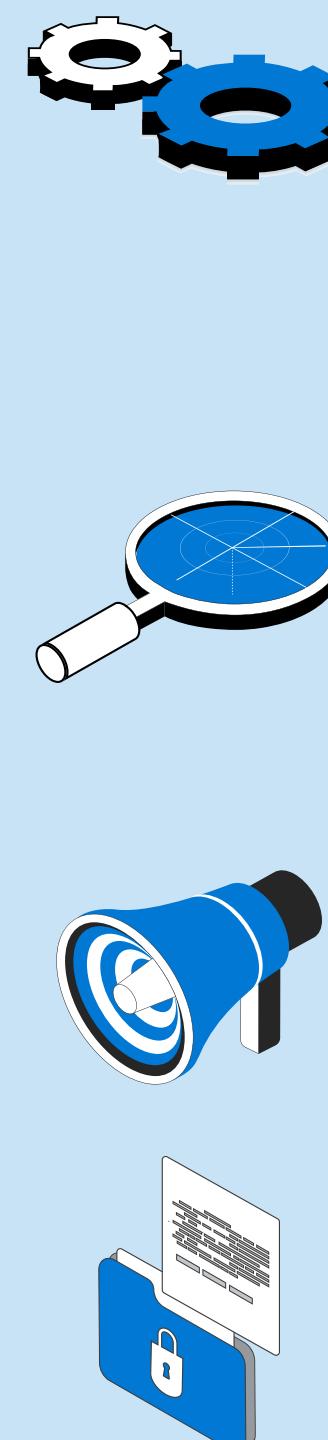
In fact, as we previously wrote, Iran executed a cyber-enabled influence operation in January as a form of retaliation against a French magazine for holding a competition for cartoons "ridiculing" Iran's Supreme Leader as a "symbol of backward-looking, narrow-minded, intolerant religious power."⁴² The operation also criticized the French government, suggesting they were financing the magazine.

In November, Mint Sandstorm sent spear-phishing emails to security-related ministers from primarily NATO countries in the Ukraine Defense Consultative Group, ostensibly about an upcoming virtual meeting. Iran was likely seeking intelligence in the wake of EU sanctions on Iranian entities involved in supplying drones to Russia, as well as reports of the delivery to Ukraine of new air defense systems meant to combat missile and drone strikes.⁴³

Iran's intelligence agencies blamed western intelligence services in multiple European countries for cooperating with the CIA on a project to foment protests in Iran.⁴⁴

Iran's efforts at conducting higher impact cyberattacks against operational technology

Iran is likely to continue leveraging its newfound penchant for cyber-enabled IO to keep pace with external pressure, in part to overcome shortcomings in its cyber threat capabilities relative to the attacks it has faced. At the same time, Iranian cyber actors are likely seeking greater cyberattack capabilities to achieve the regime's desire for proportional retaliation. In fact, there remain occasional outliers that demonstrate efforts along these lines.



In early April 2023, an Iran-linked group was most likely behind a cyberattack that disabled the water controllers of at least ten Israeli farms, replacing the image on programmable logic controllers (PLCs) with the message "Down with Israel." The image was identical to one used in a probable Iranian cyberattack against Israel Post in January 2022, days after an Iranian state broadcast was disrupted with the message "Down with Khamenei."

Prior to the most recent attack on Israel's water system, Microsoft Threat Intelligence detected an Iranian actor conducting reconnaissance of an Israeli water company in mid-2022 and scanning the web interfaces of Israel-based industrial control systems in December 2022. We do not know if that actor was involved in this latest attack.

In June, Moses Staff amplified a cyberattack that set off emergency rocket sirens in Israel using software that adjusts Audio over Internet Protocol (AoIP) networks.⁴⁵ We assess an Iran-affiliated actor was also responsible for the cyberattack on the alarm system, but we do not have indications linking the group with Moses Staff.

Classified documents leaked by a British news outlet in July 2021 indicate that in 2020 an IRGC unit was conducting research into vulnerabilities in PLCs and methods of remotely adjusting the controls of fuel pumps at petrol stations and ballast water on cargo ships, which could disrupt a ship's operations.⁴⁶



Figure 14: Image on disabled water controllers on Israeli farms, April 2023.

1. "Hackers Target Israeli TV/Radio Infrastructure," 6 May 2021, al-sarira.com/2021/05/06/hackers-target-israeli-tv-radio-infrastructure/; "Listen: Hackers broke into 100 FM broadcasts" (machine translation from Hebrew), 6 May 2021, ice.co.il/media/news/article/819193; web.archive.org/web/20210616224505/https://www.hackersofsvior.com/event-item.html
2. "Iran says retaliation will be proportionate and 'against legitimate targets,'" 7 January 2020, cbsnews.com/news/iran-news-zarif-cbs-news-retaliation-qassem-soleimani-killing-proportionate-legitimate-targets-today-2020-01-07/; "Iran warns of 'immediate counter-response' if US attacks its bases after strikes on Syria," 25 March 2023, news.sky.com/story/amp/iran-warns-of-immediate-counter-response-if-us-attacks-its-bases-after-strikes-on-syria-12842303; "Second US base hit in Syria following retaliatory strikes," 24 March 2023, thehill.com/policy/defense/3916342-second-us-base-hit-in-syria-following-retaliatory-strikes/; "U.S. Responds to Attack That Killed U.S. Contractor in Syria," 24 March 2023, defense.gov/News/News-Stories/Article/Article/3341127/us-responds-to-attack-that-killed-us-contractor-in-syria/
3. This definition draws on elements of definitions of influence operations used by RAND, Recorded Future, and scholars at NATO's Cooperative Cyber Defense Center of Excellence. "Foundations of Effective Influence Operations A Framework for Enhancing Army Capabilities," 2009, rand.org/pubs/monographs/MG654.html; "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations," ccdcoe.org/uploads/2018/10/Art-08-Influence-Cyber-Operations-The-Use-of-Cyberattacks-in-Support-of-Influence-Operations.pdf
4. web.archive.org/web/20210509224051/https://hackersofsvior.com/Event_item.html; web.archive.org/web/20210616224505/https://www.hackersofsvior.com/event-item.html; moses-staff[.]se; eotp-us[.]ca
5. "Microsoft Digital Defense Report," October 2022, microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022. "Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021," 16 November 2021, microsoft.com/en-us/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/
6. "Hackers Target Israeli TV/Radio Infrastructure," 6 May 2021, al-sarira.com/2021/05/06/hackers-target-israeli-tv-radio-infrastructure/; "Listen: Hackers broke into 100 FM broadcasts" (machine translation from Hebrew), 6 May 2021, ice.co.il/media/news/article/819193; web.archive.org/web/20210616224505/https://www.hackersofsvior.com/event-item.html
7. t[.]me/s/Saifal_Quds
8. "Israel's cyber directorate issues annual warning ahead of Iran's 'Jerusalem Day,'" 24 April 2022, timesofisrael.com/israel-cyber-directorate-issues-annual-warning-ahead-of-israins-jerusalem-day/
9. "MERCURY and DEV-1084: Destructive attack on hybrid environment," 7 April 2023, microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/
10. "MERCURY and DEV-1084: Destructive attack on hybrid environment," 7 April 2023, microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/
11. web.archive.org/web/20230212181234/https://www.facebook.com/profile.php?id=100090227412050; archive.is/9Ad5K; web.archive.org/web/20230213005442/https://www.youtube.com/@darkbitYT/about; web.archive.org/web/20230212213845/https://www.reddit.com/user/darkbitRDT/; web.archive.org/web/20230212181721/https://t.me/DarkBitChannel/7; iW6v2p3cruy7qfup3y14dgt4pfibfa3ai4zgnu5df2q4hus3lm7c7ad[.]onion;
12. "Microsoft shifts to a new threat actor naming taxonomy," 18 April 2023, microsoft.com/en-us/security/blog/2023/04/18/microsoft-shifts-to-a-new-threat-actor-naming-taxonomy/; "How Microsoft names threat actors," 18 April 2023, learn.microsoft.com/en-us/microsoft-365/security/intelligence/microsoft-threat-actor-naming?view=o365-worldwide
13. "Treasury Sanctions Iran Cyber Actors for Attempting to Influence the 2020 U.S. Presidential Election," 18 November 2021, home.treasury.gov/news/press-releases/jy0494; "Iranian Cyber Actors Responsible for Website Threatening U.S. Election Officials," 23 December 2020, fbi.gov/news/press-releases/iranian-cyber-actors-responsible-for-website-threatening-us-election-officials
14. "Iranian Cyber Group Emennet Pasargad Conducting Hack-and-Leak Operations Using False Flag Personas," FBI Private Industry Notification, 20 October 2022, ic3.gov/Media/News/2022/221020.pdf; "Context and Recommendations to Protect Against Malicious Activity by Iranian Cyber Group Emennet Pasargad," FBI Private Industry Notification, 26 January 2022, ic3.gov/Media/News/2022/220126.pdf
15. "DRAFT WHITE PAPER: An Attribution model for influence operations," 31 January 2023, blogs.microsoft.com/wp-content/uploads/prod/sites/5/2023/02/DTAC-Attribution-Framework.pdf
16. web.archive.org/web/20230213170158/https://www.akhbar-alkhaleej.com/
17. "Bahrain dissolves main Shia opposition Al-Wefaq party," 17 July 2016, aljazeera.com/news/2016/7/17/bahrain-dissolves-main-shia-opposition-al-wefaq-party; "Bahrain: Elections, But No Civic Space," 10 November 2022, amnesty.org/en/documents/mde11/6124/2022/en/
18. "Israel reaches agreement with Qatar to allow direct flights during World Cup," 10 November 2022, timesofisrael.com/israel-reaches-agreement-with-qatar-to-allow-direct-flights-during-world-cup/; "World Cup 2022: First ever Israel-Qatar flight lands in Doha," 20 November 2022, middleeasteye.net/news/qatar-world-cup-first-ever-israel-flight-doha#
19. "Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election," 18 November 2021, justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed
20. "Israel purchase Bahraini island," english.almayadeen.net/videos/israel-purchase-bahraini-island, "Bahrainis confident of toppling treasonous regime that sells islands to Israel," kayhan[.]ir/en/news/112404/bahrainis-confident-of-toppling-treasonous-regime-that-sells%20-islands-to-israel, "Israel 'buys island' in Bahrain; activists call it 'dangerous and worrying,'" 13 February 2023, parstoday[.]ir/en/news/west_asia-i195944; israel_buys_island_in_bahrain_activists_call_it_dangerous_and_worrying, virustotal.com/gui/file/8f855ed4c2f17487bac5d5079437acd728cc68d93b49ab2f5b6d6d2430da133/details
21. "Moses Staff Hackers Publish Footage of Jerusalem Explosion," 25 November 2023, hackread.com/moses-staff-hackers-jerusalem-footage/; kan.org.il/item/?itemId=138720
22. "Iranian Dissident Masih Alinejad Won't Be Silenced," 2 March 2023, time.com/6259111/masih-alinejad/
23. t[.]me/adll_ali
24. "Microsoft investigates Iranian attacks against the Albanian government," 8 September 2022, microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/
25. "Albanian PM says Iranian hackers hit country with another cyberattack," 11 September 2022, therecord.media/albanian-pm-says-iranian-hackers-hit-country-with-another-cyberattack; twitter.com/ediramaal/status/1568920720658268165
26. "Albanian police force open Iranian Embassy after expulsions," 8 September 2022, apnews.com/article/middle-east-iran-albania-tirana-5cd399beaa7381fd2c01ac6831fed208
27. "Iran Says Gas Stations Were Target Of Cyberattack To Foment Unrest," 28 October 2021, iranintl.com/en/20211028778677
28. "'Effect of cyber attack on Gold Bond will last for weeks,' warns expert," 1 February 2022, calcalistech.com/ctech/articles/0,7340,L-3928403,00.html
29. "Officials: Israel linked to a disruptive cyberattack on Iranian port facility," 18 May 2020, washingtonpost.com/national-security/officials-israel-linked-to-a-disruptive-cyberattack-on-iranian-port-facility/2020/05/18/9d1da866-9942-11ea-89fd-28fb313d1886_story.html
30. "'Effect of cyber attack on Gold Bond will last for weeks,' warns expert," 1 February 2022, calcalistech.com/ctech/articles/0,7340,L-3928403,00.html
31. "Videos: When The Security of the Terrorists of Durres(MEK) is More Important than The Security of Your Own People," 26 September 2022, justicehomeland[.]ru/videos-when-the-security-of-the-terrorists-of-durresmek-is-more-important-than-the-security-of-your-own-people/
32. "Context and Recommendations to Protect Against Malicious Activity by Iranian Cyber Group Emennet Pasargad," FBI Private Industry Notification, 26 January 2022, ic3.gov/Media/News/2022/220126.pdf
33. "Messaging impersonating the sports channel are sent" (machine translation from Hebrew), 10 December 2022, sport5.co.il/articles.aspx?FolderID=10796&docID=422369
34. "The Arab world celebrates Morocco's success in the World Cup – and in the meantime, the resident of Ashdod received threats in text messages." 10 December 2022, ashdodi.com/hackers-are-threatening-an-ashdod-resident-not-to-fly-to-the-emirates/
35. reddit.com/r/albania/comments/w2y6wx/a_ju_erdhi_edhe_ju_a_jam_i_vetmi/
36. twitter.com/gerardbiard_; twitter.com/thierrykarsent
37. nvd.nist.gov/vuln/detail/CVE-2022-47966
38. cve.mitre.org/cgi-bin/cvename.cgi?name=2022-47986
39. "China-Brokered Deal Between Iran, Saudi Arabia Marks a New Middle East," 11 March 2023, wsj.com/articles/china-brokered-deal-between-iran-saudi-arabia-marks-a-new-middle-east-d1leaf94e; "Saudi Arabia, Iran Restore Relations in Deal Brokered by China," 10 March 2023, wsj.com/articles/saudi-arabia-iran-restore-relations-in-deal-brokered-by-china-406393a1; "Senior Iranian Official Visits UAE on Heels of Saudi Deal," 16 March 2023, voanews.com/a/senior-iranian-official-visits-uae-on-heels-of-saudi-deal-/7008237.html; "Iranian MP's meet with Bahraini parliament speaker in Manama, 1st in years," 14 March, 2023, ifpnews[.]com/iranian-mps-bahraini-parliament-speaker-manama-1st-years/
40. "Iran Says Israel, U.S. Likely Behind Cyberattack on Gas Stations," 31 October 2021; bloomberg.com/news/articles/2021-10-31/iran-says-israel-u-s-likely-behind-cyberattack-on-gas-stations; "Iran's supreme leader breaks silence on protests, blames US," 3 October 2022, apnews.com/article/iran-israel-middle-east-dubai-united-arab-emirates-25c14800b5b145d850fe3181eb062664; "Tehran lashes out at Israel's support for Iranian protest movement," 2 November 2022, mei.edu/publications/tehran-lashes-out-israelis-support-iranian-protest-movement; "Joint statement by intelligence ministry, IRGC: CIA project to destroy Iran defeated," 28 October 2022, en.iran[.]ir/news/84926113/Joint-statement-by-intelligence-ministry-IRGC-CIA-project-to
41. "Cyberattack forces Iran steel company to halt production," 27 June 2022, apnews.com/article/technology-middle-east-iran-dubai-b0404963ae23e5008439a0b607952de1; "The Iran Steel Industry Cyber Attack Explained," 7 July 2022, blog.scadafence.com/the-iran-steel-industry-cyber-attack-explained; "Cyber-attack' hits Iran's transport ministry and railways," 11 July 2022, theguardian.com/world/2021/jul/11/cyber-attack-hits-irans-transport-ministry-and-railways
42. "#MULLAHSGETOUT : CHARLIE HEBDO'S INTERNATIONAL COMPETITION," charliehebdo.fr/mullahsgetout-international-competition/
43. "EU agrees on new sanctions over Iranian drones in Ukraine," 20 October 2022, aljazeera.com/news/2022/10/20/eu-agrees-new-sanctions-over-iranian-drones-in-ukraine; "Ukraine-bound NASAMS are in US hands now: Raytheon," 25 October 2022, defensenews.com/pentagon/2022/10/25/ukraine-bound-nasams-are-in-us-hands-now-raytheon/
44. "Joint statement by intelligence ministry, IRGC: CIA project to destroy Iran defeated," 28 October 2022, en.iran[.]ir/news/84926113/Joint-statement-by-intelligence-ministry-IRGC-CIA-project-to
45. "Iranian hackers take responsibility for cyber attacks on Israeli sirens," 22 June 2022, www.israelnationalnews.com/flashes/580076; "Cyberattack suspected behind false siren alerts in Jerusalem, Eilat," 20 June 2022, timesofisrael.com/cyberattack-suspected-behind-false-siren-alerts-in-jerusalem-eilat/
46. "Iran's Secret Cyber Files," July 2021, news.sky.com/story/irans-secret-cyber-files-on-how-cargo-ships-and-petrol-stations-could-be-attacked-12364871

