Microsoft

Iran surges cyber-enabled influence operations in support of Hamas

01001001 01110010 01100001
01101110 00100000 01110011
01110101 01110010 01100111
01100101 01110011 00100000
01100011 01111001 01100010
01100101 01110010 00101101
01100101 01101110 01100001
01100010 01101100 01100101
01100100 00100000 01101001
01101110 01100110 01101100
01110101 01100101 01101110
01100011 01100101 00100000
01101111 01110000 01100101
01110010 01100001 01110100
01101001 01101111 01101110
01110011 00100000 01101001
01101110 00100000 01110011
01110101 01110000 01110000
01101111 01110010 01110100
00100000 01101111 01100110
00100000 01001000 01100001
01101101 01100001 01110011

February 7, 2024

Microsoft Threat Intelligence

Table of Contents

Introduction

As the Israel-Hamas war broke out on October 7, 2023, Iran immediately surged support to Hamas with its now well-honed technique of combining targeted hacks with influence operations amplified on social media, what we refer to as cyber-enabled influence operations.[1] Iran's operations were initially reactionary and opportunistic. By late October, nearly all of Iran's influence and major cyber actors focused on Israel in an increasingly targeted, coordinated, and destructive manner, making for a seemingly boundless "all-hands-on-deck" campaign against Israel. Unlike some of Iran's past cyberattacks, all of its destructive cyberattacks against Israel in this war—real or fabricated—were complemented with online influence operations.

Influence operations grew increasingly sophisticated and inauthentic, deploying networks of social media "sockpuppets" as the war progressed. Throughout the war these influence operations have sought to intimidate Israelis while criticizing the Israeli government's handling of hostages and military operations to polarize and ultimately destabilize Israel.

Eventually, Iran turned its cyberattacks and influence operations against Israel's political allies and economic partners to undermine support to Israel's military operations.

We expect the threat posed by Iran's cyber and influence operations will grow as the conflict persists, particularly amid the rising potential for a widening war. Increased brazenness of Iranian and Iran-affiliated actors coupled with burgeoning collaboration among them portends a growing threat ahead of the US elections in November.

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.

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.

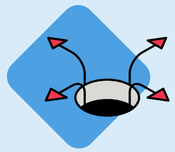
Sockpuppet
A false online persona employing fictitious or stolen identities for the purpose of deception.

Multiple Phases of the War

Iran's cyber and influence operations have progressed through multiple phases since the Hamas terrorist attack on October 7. One element of their operations has remained constant throughout: the combination of opportunistic cyber targeting with influence operations that often mislead the precision or scope of impact.

This report focuses on Iranian influence and cyber-enabled influence operations from October 7 until the end of 2023, while covering trends and operations dating back to the spring of 2023.

Phases of Iran's cyber-enabled influence operations in the Israel-Hamas war



Phase 1:
Reactive & Misleading

Cyber
- Leverage pre-existing access.

Influence
- Re-use old material for "leaks."
- Minimal use of sockpuppets.
- No detected use of bulk SMS or email.
- Some impersonation.

Phase 2:
All-Hands-on-Deck

Cyber
- Increase in number of groups targeting Israel.
- Shift to destructive and sometimes coordinated attacks.
- Begin incorporating messaging into attacks.

Influence
- Use sockpuppets, many hastily repurposed.
- Use bulk SMS and email.
- Extend success from impersonation to additional Israeli activists and Palestinian militant groups.

Phase 3:
Expanded Geographic Scope

Cyber
- Incorporate more messaging into cyberattacks.
- Hone targeting.

Influence
- Create greater cover for sockpuppets.
- Focus on undermining Israeli willingness to continue war and undercutting international support.

Phase 1:
Reactive & Misleading

Iranian groups were reactive during the initial phase of the Israel-Hamas war. Iranian state media issued misleading details of claimed cyberattacks and Iranian groups re-used dated material from historical operations, re-purposed access they had before the war, and exaggerated the overall scope and impact of claimed cyberattacks.

Nearly four months into the war, Microsoft has still not seen clear evidence from our data indicating Iranian groups had coordinated their cyber or influence operations with Hamas's plans to attack Israel on October 7. Rather, the preponderance of our data and findings suggests that Iranian cyber actors were reactive, quickly surging their cyber and influence operations after the Hamas attacks to counter Israel.

Misleading details on claimed attacks through state media:

The day the war broke out, Tasnim News Agency, an Iranian outlet affiliated with the Islamic Revolutionary Guard Corps (IRGC), falsely claimed that a group called "Cyber Avengers" conducted cyberattacks against an Israeli power plant "at the same time" as Hamas's attacks.[2] Cyber Avengers, an IRGC-run cyber persona, actually claimed to have conducted a cyberattack against an Israeli electric company the evening prior to Hamas's incursion.[3] Their evidence: weeks-old press reporting of power outages "in recent years" and a screenshot of an undated disruption of service to the company's website.[4]

Re-using old material:

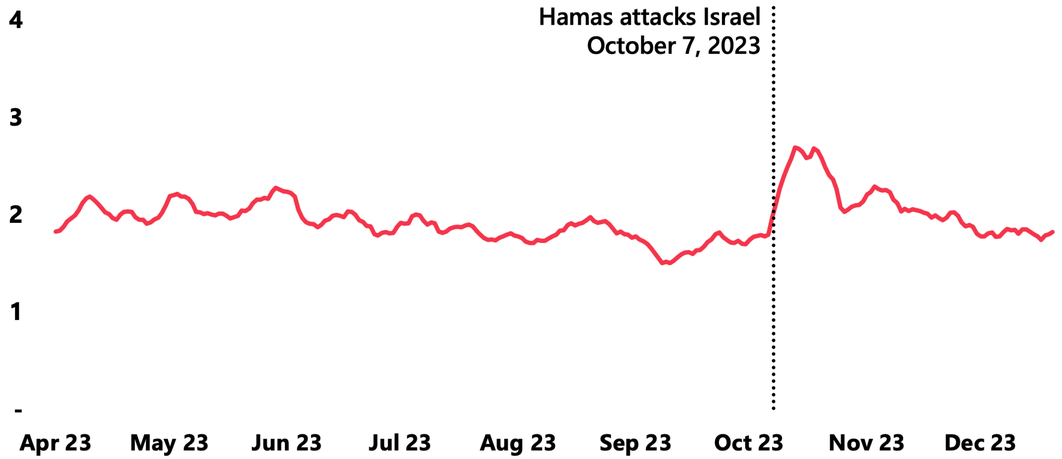
After Hamas's attacks on Israel, Cyber Avengers claimed to conduct a string of cyberattacks against Israel, the earliest of which our investigations revealed to be false. On October 8, they claimed to leak documents of an Israeli powerplant, though the documents had been previously published in June 2022 by another IRGC-run cyber persona "Moses Staff."[5]

Re-purposing access:

Another cyber persona "Malek Team," which we assess is run by Iran's Ministry of Intelligence and Security (MOIS), leaked personal data from an Israeli university on October 8 without any clear link in targeting to the burgeoning conflict there, suggesting the target was opportunistic and perhaps chosen based on pre-existing access prior to the outbreak of war. Rather than drawing links between the leaked data and support for Hamas's operations, Malek Team initially used hashtags on X (formerly Twitter) to support Hamas and only days later shifted messaging to align with the type of messaging denigrating Israeli Prime Minister Benjamin Netanyahu seen in other Iranian influence operations.

Figure 1 Microsoft Threat Intelligence

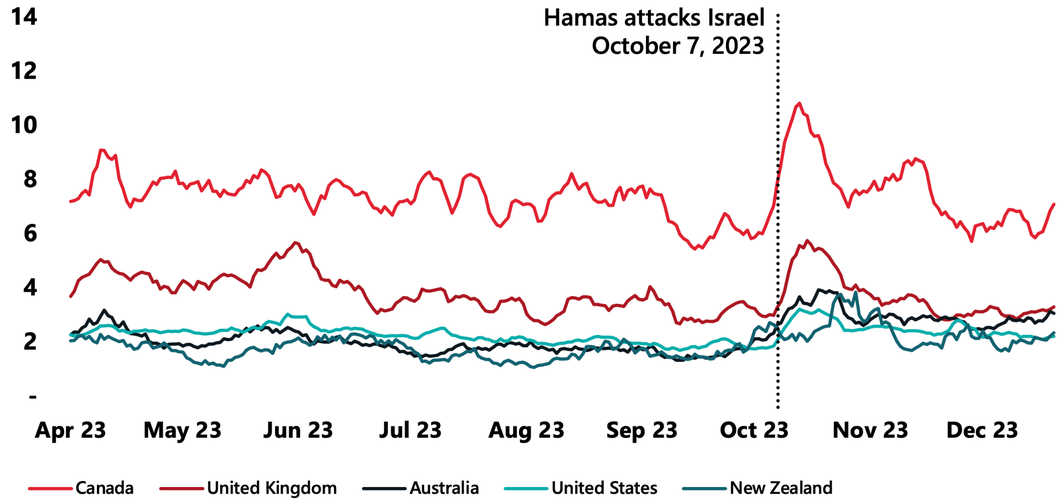
Iranian propaganda consumption worldwide



The index value on the y-axis measures the proportion of traffic visiting the mentioned Iranian sources to overall internet traffic using a seven-day moving average.

Figure 2 Microsoft Threat Intelligence

Iranian propaganda consumption by country



Iran's influence operations were most effective in the early days of the war

The reach of Iranian state-affiliated media surged after the outbreak of the Israel-Hamas War. In the first week of the conflict, we observed a 42% increase in Microsoft AI for Good Lab's Iranian Propaganda Index, which monitors the consumption of news from Iranian state and state-affiliated news outlets (see Figure 1). The index measures the proportion of traffic visiting these sites to overall traffic on the internet. That surge was particularly pronounced in English-speaking countries closely allied with the United States (Figure 2), highlighting Iran's ability to reach Western audiences with its reporting on Middle East conflicts. A month into the war, the reach of these Iranian sources remained 28-29% above pre-war levels globally.

Iran's influence without cyberattacks display agility

Iran's influence operations appeared more agile and effective in the earliest days of the war compared to its combined cyber-influence operations later in the conflict. Within days of Hamas's attack on Israel, a likely Iranian state actor that we track as Storm-1364, launched an influence operation using an online persona called "Tears of War," which impersonated Israeli activists to spread anti-Netanyahu messaging to Israeli audiences across multiple social media and messaging platforms. The speed at which Storm-1364 launched this campaign after the October 7 attacks highlights this group's agility and points to advantages of influence-only campaigns, which may be faster to form because they do not need to wait on cyber activity of a cyber-enabled influence operation.

Phase 2:
All-Hands-on-Deck

From mid- to late-October, a growing number of Iranian groups shifted their focus to Israel, and Iran's cyber-enabled influence operations moved from being largely reactive, fabricated, or both, to including destructive cyberattacks and developing targets of interest for operations. These attacks included data deletion, ransomware, and apparently adjusting an internet of things (IoT) device.[6] We also saw evidence of increased coordination among Iranian groups.

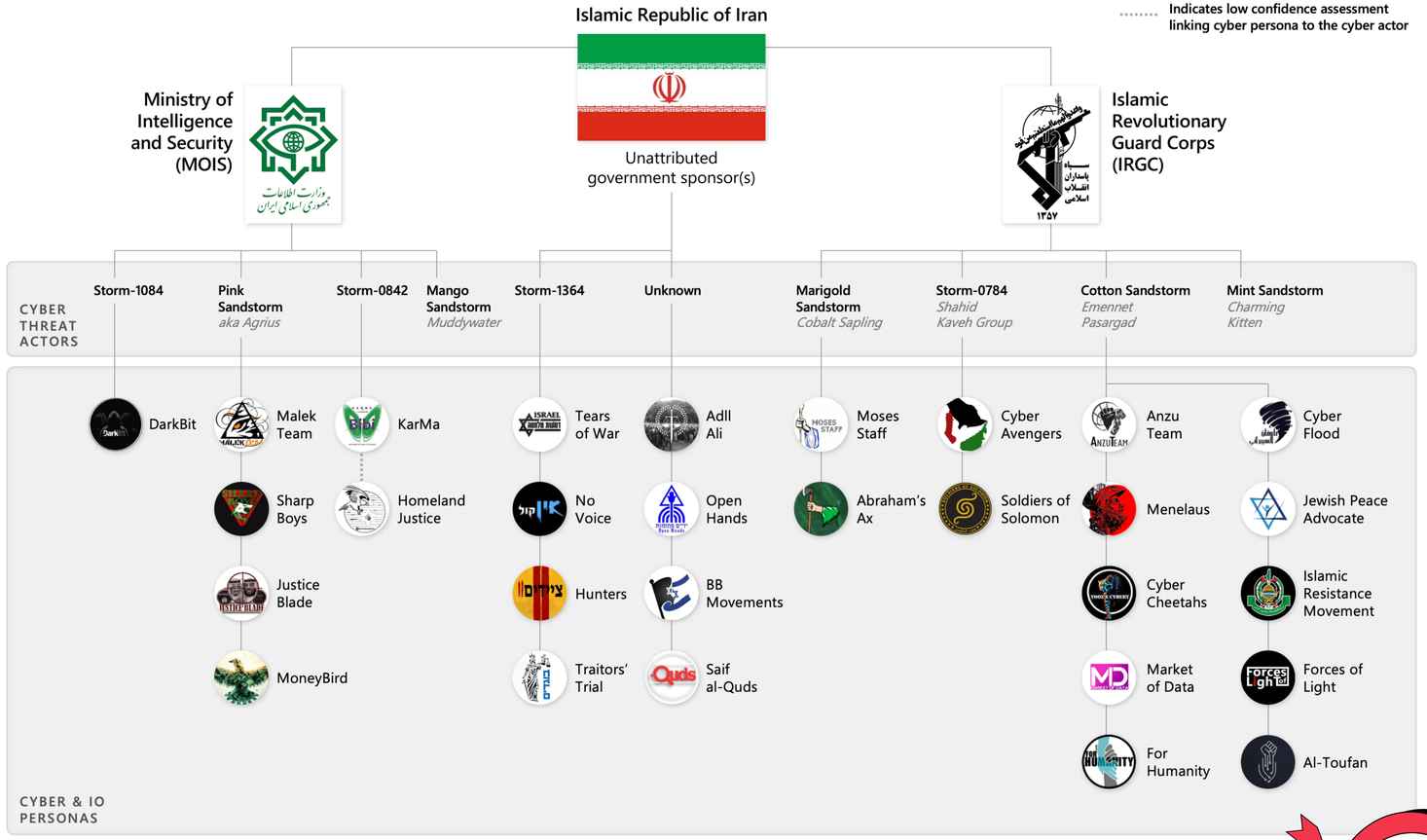
In the first week of the war, Microsoft Threat Intelligence tracked nine Iranian groups active in targeting Israel; that number grew to 14 groups by day 15. In some cases, we observed multiple IRGC or MOIS groups targeting the same organization or military base with cyber or influence activity, suggesting coordination, common objectives set in Tehran, or both.

Cyber-enabled influence operations also surged. We observed four hastily implemented cyber-enabled influence operations aimed at Israel in the first week of the war. By the end of October, the number of such operations more than doubled, marking a significant acceleration in these operations with by far the fastest tempo to date (see Figure 4).

Figure 3

Microsoft Threat Intelligence

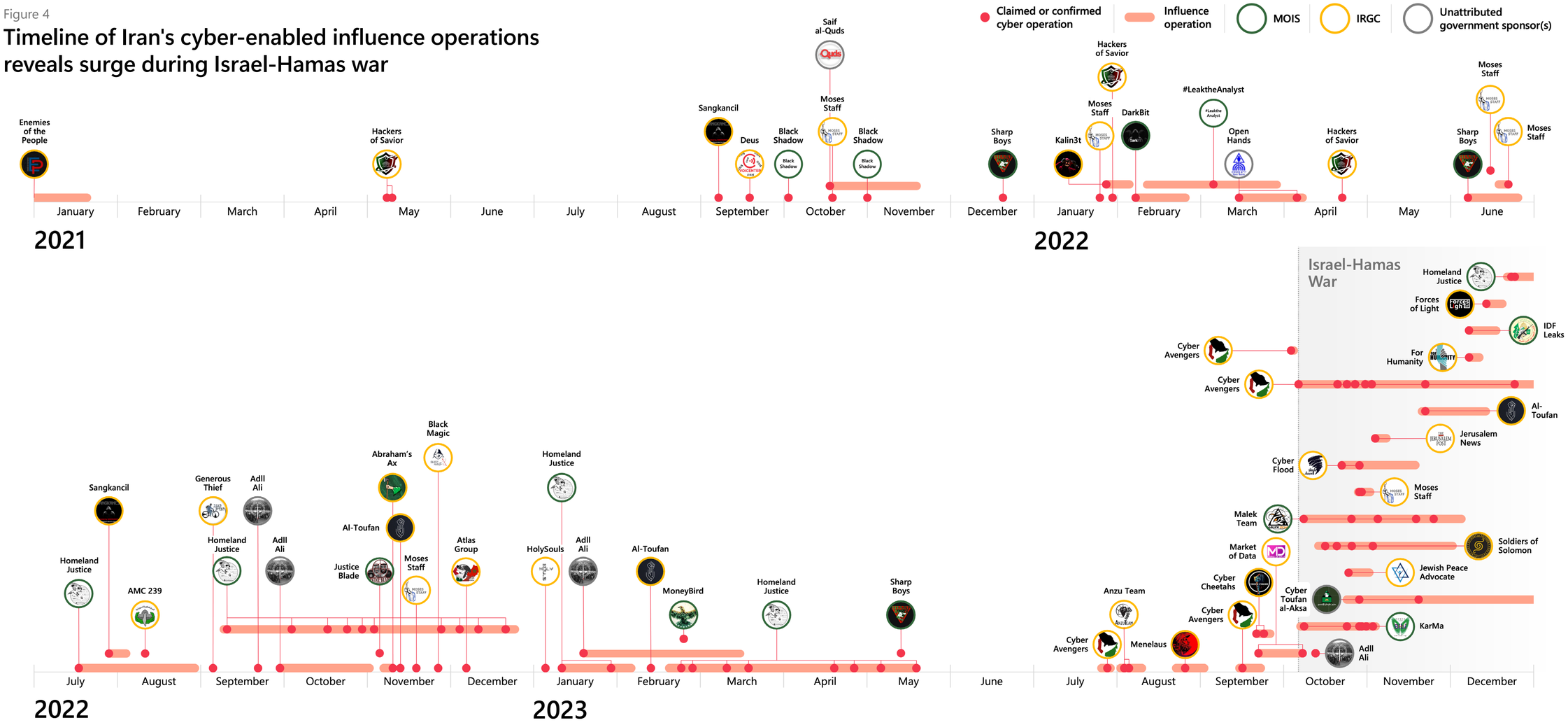
Iran at the crossroads of cyber and influence



This chart shows a sampling of assessed Iran state-run personas that we track at Microsoft Threat Intelligence. The IRGC's Cotton Sandstorm remains Iran's most prolific influence operator, regularly standing up new cyber-enabled influence operations. We have tracked double the number of personas operated by Cotton Sandstorm than represented here.

Figure 4

Timeline of Iran's cyber-enabled influence operations reveals surge during Israel-Hamas war



Microsoft Threat Analysis Center's (MTAC) research on Iran's cyber-enabled influence operations from 2020 until the end of 2023 shows a steady increase in the pace of operations over time with a surge following the outbreak of the Israel-Hamas war. This timeline excludes influence operations without a cyber component as well as several groups conducting cyber-enabled influence operations that we suspect are run by the Iranian government, but currently lack sufficient information to make a determination on their affiliation.

Microsoft Threat Intelligence

On October 18, the IRGC's Shahid Kaveh Group, which Microsoft tracks as Storm-0784, used customized ransomware to conduct cyberattacks against security cameras in Israel. It then used one of its cyber personas, "Soldiers of Solomon," to falsely claim it had ransomed security cameras and data at Nevatim Air Force Base. Examination of the security footage Soldiers of Solomon leaked reveals it was from a town north of Tel Aviv with a Nevatim street, not the airbase of the same name. In fact, analysis of the victims' locations reveal that none were near the military base (see Figure 5). While Iranian groups had begun destructive attacks, their operations remained largely opportunistic and continued to leverage influence activity to exaggerate the precision or effect of the attacks.

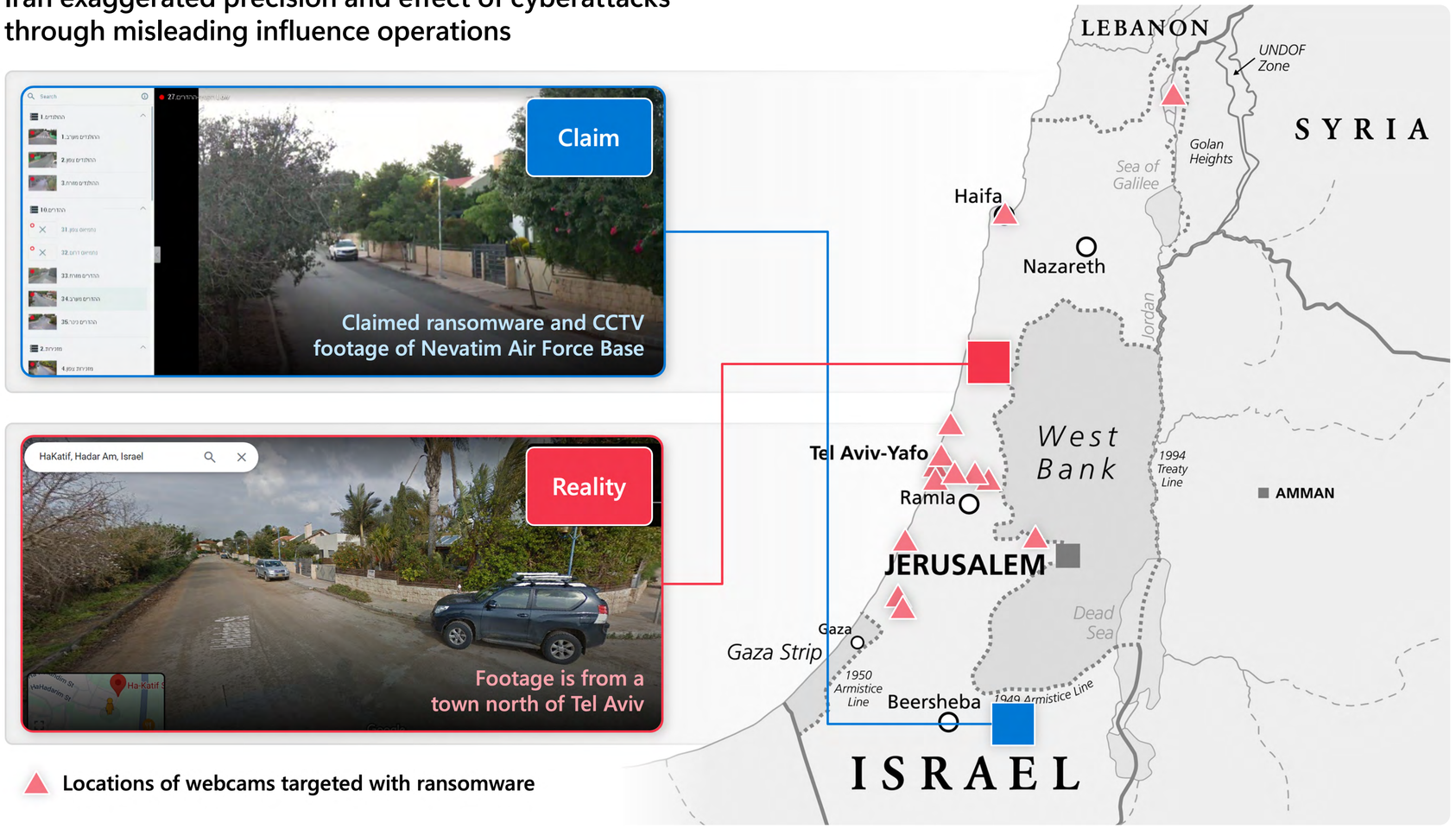
On October 21, another cyber persona run by the IRGC group Cotton Sandstorm (commonly known as Emennet Pasargad) shared a video of the attackers defacing digital displays at synagogues with messages that referred to Israel's operations in Gaza as "genocide."[7] This marked a method of embedding messaging directly into cyberattacks against a relatively soft target.

During this phase, Iran's influence activity used more extensive and sophisticated forms of inauthentic amplification. In the first two weeks

Figure 5

Microsoft Threat Intelligence

Iran exaggerated precision and effect of cyberattacks through misleading influence operations



of the war, we detected minimal advanced forms of inauthentic amplification—again suggesting operations were reactive. By the third week of the war, Iran's most prolific influence actor, Cotton Sandstorm, entered the scene launching three cyber-enabled influence operations on October 21. As we often see from the group, they used a network of social media sockpuppets to amplify the operations, though many appeared to be hastily repurposed without authentic covers disguising them as Israelis. On multiple occasions Cotton Sandstorm sent text messages or emails in bulk to amplify or boast about their operations, leveraging compromised accounts to enhance authenticity.[8]

Phase 3: Expanding Geographic Scope

Beginning in late November, Iranian groups expanded their cyber-enabled influence beyond Israel, to include countries that Iran perceives are aiding Israel, very likely to undermine international political, military, or economic support for Israel's military operations. This expansion in targeting aligned with the start of attacks on international shipping linked to Israel by the Houthis, an Iran-backed Shi'ite militant group in Yemen (see Figure 8).[9]

- On November 20, the Iran-run cyber persona "Homeland Justice," warned of major forthcoming attacks on Albania before amplifying destructive cyberattacks by MOIS groups in late December against Albania's Parliament, national airline, and telecommunication providers.[10]
- On November 21, Cotton Sandstorm-run cyber persona "Al-Toufan" targeted Bahraini government and financial organizations for normalizing ties with Israel.
- By November 22, IRGC-affiliated groups began targeting Israeli-made programmable logic controllers (PLCs) in the United States, and possibly Ireland, including taking one offline at a water authority in Pennsylvania on November 25 (Figure 6).[11] PLCs are industrial computers adapted for the control of manufacturing processes, such as assembly lines, machines, and robotic devices.
- In early December, a persona that MTAC assesses is Iran-sponsored, "Cyber Toufan Al-Aksa," claimed to leak data from a pair of American companies for financially backing Israel and providing equipment for its military.[12] They previously claimed data deletion attacks against the companies on November 16.[13] Due to a lack of strong forensic evidence linking the group to Iran, it is possible the persona is run by an Iranian partner outside the country with Iranian involvement.

Figure 6: Defaced PLC at Pennsylvania water authority with Cyber Avengers logo on November 25.

Iran's cyber-enabled influence operations also continued to grow in sophistication in this latest phase. They better disguised their sockpuppets by renaming some and changing their profile photos to appear more authentically Israeli. Meanwhile they made use of new techniques we've not seen from Iranian actors, including using AI as a key component to its messaging. We assess Cotton Sandstorm disrupted streaming television services in the UAE and elsewhere in December under the guise of a persona called "For Humanity." For Humanity published videos on Telegram showing the group hacking into three online streaming services and disrupting several news channels with a fake news broadcast featuring an apparently AI-generated anchor that claimed to show images of Palestinians injured and killed from Israeli military operations (Figure 7).[14] News outlets and viewers in the UAE, Canada, and the UK reported disruptions in streaming television programming, including BBC, that matched For Humanity's claims.[15]

Figure 7: Disruption of streaming TV programming using an AI-generated broadcaster.

Figure 8

Iran and affiliates expand targeting to Israeli supporters and business partners

Nov 6
Khamenei says Israel can't exist without US support

Nov 19
IRGC-run group alludes to attacks on Bahrain

Nov 22
IRGC begins targeting US PLCs

Dec 1
Cyber Toufan al-Aksa leaks data from US companies with ties to Israel

Nov 14
Houthi leader warns of attacking Israeli ships

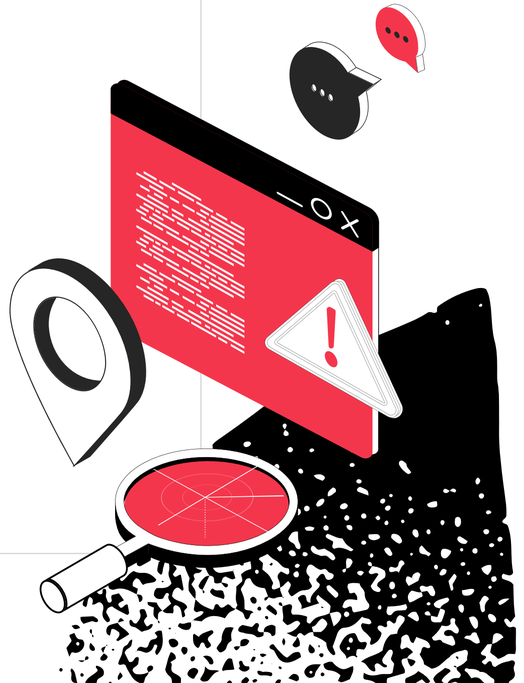
Nov 16
Cyber Toufan al-Aksa targets companies conducting business with Israel

Nov 19
Houthis seize Israeli-linked ship

Nov 20
MOIS-run persona warns of future attack against Albania

Nov 25
IRGC defaces PLC at US water authority

Within days of each other, several Iranian state and Iran-sponsored actors began targeting those that they claimed or perceived support the Israeli government. These cyberattacks occurred at the same time the Houthis began targeting international shipping. This all occurred after Iran's Supreme Leader Ali Khamenei commented that Israel "will be incapable of continuing" without US support and called on Muslim governments to block the export of oil to Israel.[16]



Iran's Influence Objectives in the Israel-Hamas War

Iran's operations worked toward four broad objectives: destabilization, retaliation, intimidation, and undermining international support for Israel. All four of these objectives also seek to undermine Israel and its supporters' information environments to create general confusion and lack of trust.

Destabilization through polarization

Iran's targeting of Israel during the Israel-Hamas war has increasingly focused on stoking domestic conflict over the Israeli government's approach to the war. Multiple Iranian influence operations have masqueraded as Israeli activist groups to plant inflammatory messaging that criticizes the government's approach to those kidnapped and taken hostage on October 7.[17] Netanyahu has been a primary target of such messaging, and calls for his removal were a common theme in Iran's influence operations.[18]

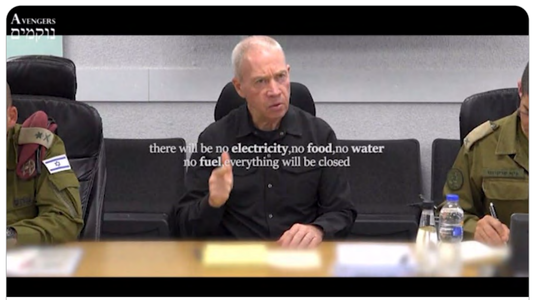


Figure 9: Cyber Avengers re-posted the video of Israel's Defense Minister announcing Israel would blockade Gaza.

Retaliation

Much of Iran's messaging and choice of targets emphasizes its operations' retaliatory nature. For example, the duly named persona Cyber Avengers released a video showing Israel's Defense Minister stating that Israel would cut off electricity, food, water, and fuel to Gaza City (see Figure 9), followed by a series of claimed Cyber Avengers attacks targeting Israeli electricity, water and fuel infrastructure.[19] Their previous claims of attacks on Israel's national water systems days earlier included the message "An eye for an eye" and the IRGC-affiliated Tasnim News Agency reported that the group said the attacks on water systems were retaliation for the siege on Gaza.[20] An MOIS-linked group we track as Pink Sandstorm (a.k.a. Agrius) conducted a hack and leak against an Israeli hospital in late November that appeared to be retaliation for Israel's days-long siege of al-Shifa Hospital in Gaza two weeks earlier.[21]

Intimidation

Iran's operations also serve to undermine Israeli security and intimidate the citizens of Israel and its supporters by delivering threatening messaging and convincing target audiences that their state's infrastructure and government systems are insecure. Some of Iran's intimidation appears aimed at undermining Israel willingness to continue the war, like messaging attempting to convince IDF soldiers that they should "leave the war and go back home" (Figure 10).[22] One Iranian cyber persona, which may be masquerading as Hamas, claimed to send threatening text messages to the families of Israeli soldiers, adding "The IDF [Israel Defense Forces] soldiers should be aware that till our families are not secure, then their families won't be either."[23] Sockpuppets amplifying the Hamas persona spread messaging on X that the IDF "does not have any power to protect its own soldiers" and pointed viewers to a series of messages allegedly sent from IDF soldiers asking Hamas to spare their families.[24]

Figure 10: A Cotton Sandstorm-run sockpuppet posting threatening messages in response to Israelis' posts on X. The message is accompanied by a link to a Cotton Sandstorm-run Telegram channel that contains a series of emails allegedly sent from IDF soldiers asking Hamas to spare their families.

Undermining international support for Israel

Iran's influence operations targeting international audiences often included messaging that seeks to weaken international support for Israel by highlighting the damage caused by Israel's attacks on Gaza. A persona masquerading as a pro-Palestinian group referred to Israel's actions in Gaza as "genocide."[25] In December, Cotton Sandstorm ran multiple influence operations—under the names "For Palestinians" and "For Humanity"—that called on the international community to condemn Israel's attacks on Gaza.[26]

Influence Trends

To achieve its objectives in the information space, Iran has relied heavily on four influence tactics, techniques, and procedures (TTPs) over the past nine months. These include use of impersonation and enhanced abilities to activate target audiences, paired with increasing use of text message campaigns and the use of IRGC-tied media to amplify influence operations.

Impersonating Israel activist groups and Iranian partners

Iranian groups have built on a longstanding technique of impersonation by developing more specific and convincing personas that masquerade both as Iran's friends and its enemies. Many of Iran's past operations and personas have purported to be activists in favor of the Palestinian cause.[27] Recent operations from a persona we assess is run by Cotton Sandstorm have gone further, using the name and logo of Hamas's military wing, the al-Qassam Brigades, to spread false messaging about the hostages held in Gaza and send Israelis threatening messages. Another Telegram channel that has threatened IDF personnel and leaked their personal data, which we assess was run by an MOIS group, also used the al-Qassam Brigades logo. It is unclear whether Iran is acting with Hamas's consent.

Similarly, Iran has created increasingly convincing impersonations of fictitious Israeli activist organizations on the right and left of the Israeli political spectrum. Through these fake activists, Iran seeks to infiltrate Israeli communities to gain their trust and sow discord.

Activating Israelis to action

In April and November, Iran demonstrated repeated success in recruiting unwitting Israelis to engage in on-the-ground activities promoting its false operations. In one recent operation, "Tears of War," Iranian operatives reportedly succeeded in convincing Israelis to hang branded Tears of War banners in Israeli neighborhoods featuring a seemingly AI-generated image of Netanyahu and calling for his removal from office (see Figure 11).[28]

Amplifying through text and email with increased frequency and sophistication

While Iranian influence operations continue to rely heavily on coordinated inauthentic social media amplification to reach target audiences, Iran has increasingly leveraged bulk text messaging and emails to enhance the psychological effects of their cyber-enabled influence operations. Amplification on social media using sockpuppets doesn't have the same impact as a message showing up in one's inbox, let alone one's phone. Cotton Sandstorm built on past successes using this technique beginning in 2022,[29] sending text messages, emails, or both in bulk in at least six operations since August. Their increased use of this technique suggests the group has honed the capability and views it as effective. Cotton Sandstorm's "Cyber Flood" operation in late October included up to three sets of bulk text messages and emails to Israelis amplifying claimed cyberattacks or distributing false warnings of Hamas attacks on Israel's nuclear facility near Dimona.[30] In at least one case, they leveraged a compromised account to enhance the authenticity of their emails.

Figure 11: A Tears of War banner hung in Israel with an image of Netanyahu that is likely AI-generated, judging from a Microsoft-developed model for detecting AI-generated images and an open-source detection tool. The banner's text reads "impeachment now." His collar translates to "#without_Bibi_we will win," a reference to Netanyahu's nickname "Bibi."

Leveraging state media

Iran has used overt and covert IRGC-linked media outlets to amplify alleged cyber operations and at times exaggerate their effects. In September, after Cyber Avengers claimed cyberattacks against Israel's railway system, IRGC-linked media almost immediately amplified and exaggerated their claims. IRGC-linked Tasnim News Agency incorrectly cited Israeli news coverage of a different event as proof that the cyberattack had occurred.[31] This reporting was further amplified by other Iranian and Iran-aligned outlets in a way that further obscured the lack of evidence supporting the cyberattack claims.[32]

Nascent AI adoption for influence operations

MTAC observed Iranian actors using AI-generated images and videos since the outbreak of the Israel-Hamas war. Cotton Sandstorm and Storm-1364, as well as Hezbollah and Hamas-affiliated news outlets, have leveraged AI to enhance intimidation and develop images denigrating Netanyahu and Israeli leadership.

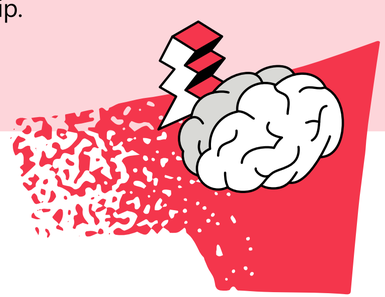


Figure 12

Microsoft Threat Intelligence

Cotton Sandstorm's influence operations (Aug–Dec 2023)

Cyber Persona	Anzu Team	Menelaus	Cyber Cheetahs	Market of Data	Jewish Peace Advocate	Islamic Resistance Movement	Cyber Flood	Hamas Hostage	Al-Toufan	For Humanity
Latest operations	Aug	Aug-Sep	Sep	Sep-Oct	Oct	Oct	Oct	Nov	Dec	Dec
Cyber Method										
Data theft		✓	✓	✓			✓		✓	
Defacement	✓	✓			✓					✓
DDoS	✓									
Email hijacking								✓		
Influence Method										
Data leak		✓	✓	✓		✓	✓		✓	
Sockpuppets			✓*	✓	✓	✓	✓	✓	✓	✓
Impersonation of victims								✓		
Impersonation of allies						✓		✓		
Text / Email messages	✓		✓	✓			✓	✓		
Fabricated news							✓	✓		✓

*MTAC assesses with low confidence that Cotton Sandstorm ran these sockpuppets.

Cyber Trends

1 Burgeoning collaboration

Weeks into the Israel-Hamas war, we began seeing examples of collaboration among Iran-affiliated groups, enhancing what the actors could achieve. Collaboration lowers the barrier to entry, allowing each group to contribute existing capabilities and removes the need for a single group to develop a full spectrum of tooling or tradecraft.

We assess that a pair of MOIS-linked groups, Storm-0861 and Storm-0842, collaborated on a destructive cyberattack in Israel in late October and again in Albania in late December. In both cases, Storm-0861 likely provided access to the network prior to Storm-0842 executing wiper malware. Similarly, Storm-0842 executed wiper malware at Albanian government entities in July 2022 after Storm-0861 gained access.

In October, another MOIS-linked group, Storm-1084, may also have had access to an organization in Israel where Storm-0842 deployed the "BiBi" wiper, named after the malware's re-naming of wiped files with the string "BiBi." It is not clear what role Storm-1084 played, if any in the destructive attack. Storm-1084 conducted destructive cyberattacks against another Israeli organization in early 2023 enabled by another MOIS-linked group Mango Sandstorm (a.k.a. MuddyWater).[33]

Since the outbreak of war, Microsoft Threat Intelligence has also detected collaboration between an MOIS-linked group, Pink Sandstorm, and Hezbollah cyber units. Microsoft has observed infrastructure overlaps and shared tooling. Iranian collaboration with Hezbollah on cyber operations, although not unprecedented, poses a concerning development, that the war might draw these groups across nation lines even closer together operationally.[34] As Iran's cyberattacks in this war have all been combined with influence operations, there is the additional likelihood that Iran improves its influence operations and their reach by leveraging native Arabic speakers to enhance the authenticity of its inauthentic personas.

2 Hyper focus on Israel

Iranian cyber actors' focus on Israel intensified. Iran has had a longstanding focus on Israel, which Tehran views as its main adversary alongside the United States. Accordingly, based on Microsoft Threat Intelligence data, in the past few years, Israeli and US enterprises have almost always been Iran's most common targets. Leading up to the war, Iranian actors focused most on Israel followed by UAE and United States. Following the breakout of the war, that focus on Israel spiked. Forty three percent of Iranian nation state cyber activity tracked at Microsoft targeted Israel, more than the next 14 targeted countries combined.

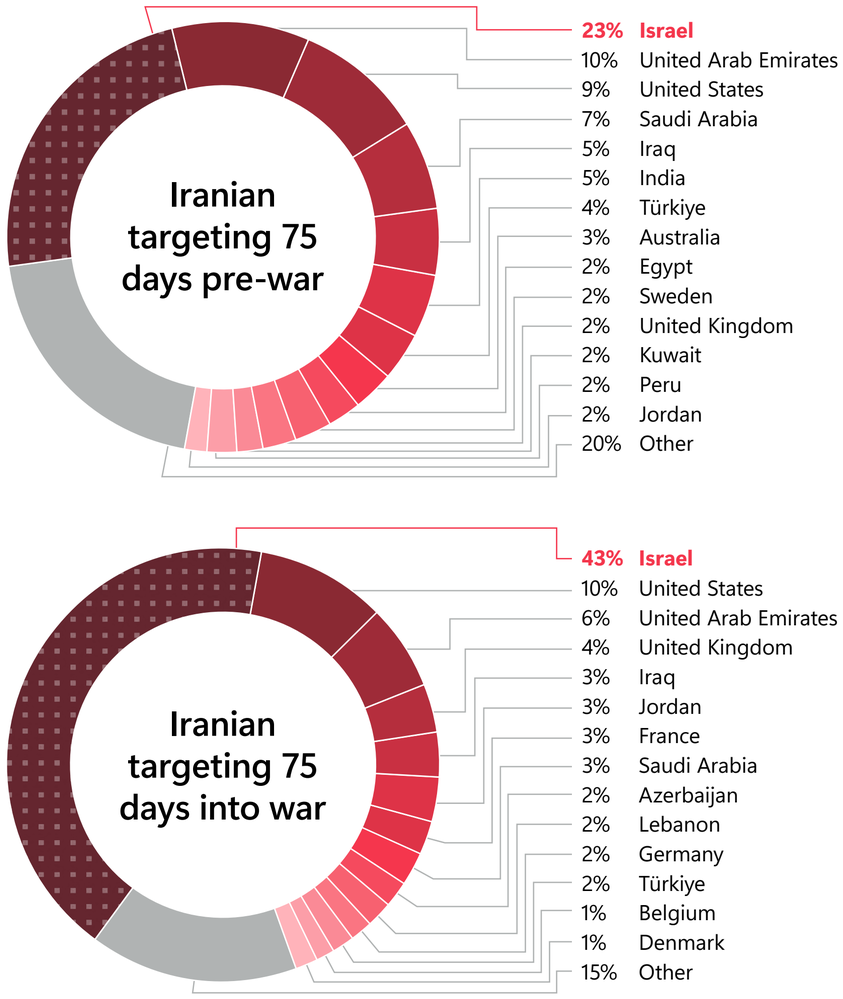


Figure 13: These figures track Microsoft observations of Iranian nation state cyber actors in the 75 days leading up to the war (top) and 75 days since the outbreak of war (bottom) on October 7, 2023. This includes activity from the full spectrum of the 14 phases of MITRE Att&ck® Framework relevant to targeting.

Looking Ahead

We expect the threat from Iran's cyber and influence operations will grow as the Israel-Hamas conflict persists, particularly amid the rising potential for escalation along additional fronts. While Iranian groups rushed to conduct, or simply fabricate, operations in the early days of the war, Iranian groups have slowed their recent operations allowing them more time to gain desired access or develop more elaborate influence operations. What the phases of war outlined in this report make clear, is that Iranian cyber and influence operations have slowly progressed, becoming more targeted, collaborative, and destructive.

Iranian actors have also grown increasingly bold in their targeting, most notably in a cyber strike against a hospital and testing Washington's red lines seemingly unconcerned about repercussions. The IRGC's attacks on US water control systems while opportunistic were seemingly a clever ploy to test Washington by claiming legitimacy in attacking equipment made in Israel.

Ahead of US elections in November 2024, the increased collaboration among Iranian and Iran-affiliated groups portends a greater challenge to those engaging in election defense. Defenders can no longer take solace in tracking a few groups. Rather, a growing number of access agents, influence groups, and cyber actors makes for a more complex and intertwined threat environment.

1. blogs.microsoft.com/on-the-issues/2023/02/03/dtac-charlie-hebdo-hack-iran-neptunium/; query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW13xRJ
2. t[.]me/Tasnimnews/270431; x.com/tasnimnews_fa/status/1710641145363972499?s=46&t=0osMy_biPlvXHjqKR75VzA
3. t[.]me/CyberAveng3rs/95; t[.]me/CyberAveng3rs/96; t[.]me/CyberAveng3rs/94
4. jpost.com/israel-news/article-759410; t[.]me/CyberAveng3rs/108
5. x.com/StaffofMoses1/status/1537062366168457218?s=20
6. t[.]me/Jewish_Peace/4
7. t[.]me/Jewish_Peace/4; t[.]me/Jewish_Peace/11
8. facebook.com/HerzliyaMyCity/posts/pfbid02BZVCHQPsUqgp6Xap4KqFdATCEjRAKbcYWkApLgRq8f9VYRNhn47QtqEcq4KzRZLyl?comment_id=1279245325976603
9. cfr.org/backgrounder/yemen-crisis
10. apnews.com/article/albania-cyberattack-parliament-iran-cc1a03b58bd753bbe935ad74f1abc0f7
11. cisa.gov/news-events/cybersecurity-advisories/aa23-335a
12. t[.]me/CyberToufan/49; t[.]me/CyberToufan/57
13. t[.]me/CyberToufan/13
14. khaleejtimes.com/uae/uae-cyberattack-disrupts-tv-services-rattles-some-residents-with-graphic-content-from-gaza; theemiratestimes.com/uae-a-cyberattack-imitates/; tiktok.com/@elias.j.2006/video/7311031767031500037; youtube.com/watch?v=otqvuDwwviM
15. web.archive.org/web/20231214162547/khaleejtimes.com/uae/uae-cyberattack-disrupts-tv-services-rattles-some-residents-with-graphic-content-from-gaza; youtube.com/watch?v=otqvuDwwviM; tiktok.com/@elias.j.2006/video/7311031767031500037
16. x.com/khamenei_ir/status/1721469381253726615?s=20
17. twitter.com/heartbreak91671/status/172041248281507065 4; t[.]me/demaothamelkhama/1363
18. t[.]me/Jewish_Peace/5; t[.]me/bbmovements/1919
19. t[.]me/CyberAveng3rs/181
20. t[.]me/CyberAveng3rs/166
21. reuters.com/graphics/ISRAEL-PALESTINIANS/MAPS/movajdladpa/#after-days-long-siege-israeli-forces-enter-al-shifa-hospital
22. twitter.com/cuakv2/status/1727659660990365927
23. t[.]me/kataeb_Al_Qassam/16
24. twitter.com/dennis09733448/status/1727662612874211332
25. t[.]me/cyber_flood/39
26. t[.]me/For_Humanity2023/11
27. microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/05/Iran-turning-to-cyber-enabled-influence-operations-for-greater-effect-05022023.pdf, pg 5.
28. twitter.com/fakereporter/status/1727787045177733568; t[.]me/demaothamelkhama/1082
29. sport5.co.il/articles.aspx?FolderID=10796&docID=422369; ashdodi.com/hackers-are-threatening-an-ashdod-resident-not-to-fly-to-the-emirates/
30. ynet.co.il/digital/technews/article/hvjiwssfa
31. tasnimnews[.]com/fa/news/1402/06/25/2956908
32. mehrnews[.]com/x333VJ; english.almayadeen[.]net/news/technology/israels-railroad-network-targeted-by-cyberattack:-israeli-me
33. microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/
34. microsoft.com/en-us/security/blog/2022/06/02/exposing-polonium-activity-and-infrastructure-targeting-israeli-organizations/