blogs.microsoft.com /on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/

Iran accelerates cyber ops against Israel from chaotic start

⋮ 2/7/2024

Since Hamas attacked Israel in October 2023, Iranian government-aligned actors have launched a series of cyberattacks and influence operations (IO) intended to help the Hamas cause and weaken Israel and its political allies and business partners. Many of Iran's immediate operations after October 7 were hasty and chaotic – indicating it had little or no coordination with Hamas – but it nevertheless has achieved growing success. Four findings stick out:

- A 42% increase in traffic, in the first week of the war, to news sites run by or affiliated to the Iranian state. Even three weeks later, this traffic was still 28% above pre-war levels.
- Despite early Iranian claims, many "attacks" in the early days of the war were either "leaking" old material, using pre-existing access to networks or were false.
- Iran's activity quickly grew from nine Microsoft-tracked groups active in Israel during the first week of the war to 14, two weeks into the war. Cyber-enabled influence operations went from roughly one operation every other month in 2021 to 11 in October 2023 alone.
- As the war progressed, Iranian actors expanded their geographic scope to include attacks on Albania, Bahrain and the USA. They also increased their collaboration, enabling greater specialization and effectiveness.

In some ways, Iran's work in support of Hamas seems to be as much about the appearance of having influence on the global stage as it is about concrete impact. As we look forward to the 2024 U.S.

presidential election, Iranian activities could build on what happened in 2020 when they impersonated American extremists and incited violence against U.S. government officials.

These insights are taken from the latest biannual report on Iran from the Microsoft Threat Analysis Center (MTAC) Iran surges cyber-enabled influence operations in support of Hamas.

From a reactive start to all hands on deck

Contrary to some claims of Iranian state media, Iranian cyber and IO actors were reactive in the initial phase of the Israel-Hamas war. MTAC observed Iranian state media issuing misleading details of claimed attacks and Iranian groups re-using dated material from historical operations and exaggerating the overall scope and impact of claimed cyberattacks. Three months on, the preponderance of data suggests Iranian cyber actors were reactive, quickly surging their cyber and influence operations after the Hamas attacks to counter Israel.

Since the outbreak of the Israel-Hamas war on October 7, Iran has increased its influence operations and hacking efforts against Israel, creating an “all hands on deck” threat environment. These attacks were reactive and opportunistic in the early days of the war but, by late October, nearly all of its influence and major cyber actors were targeting Israel. Cyberattacks became increasingly targeted and destructive and IO campaigns grew increasingly sophisticated and inauthentic, deploying networks of social media “sockpuppet” accounts.

Iran interrupted TV services with fake news reports using an AI-generated anchor

In early December 2023, Iran interrupted streaming television services and replaced them with a fake news video featuring an apparently AI-generated news anchor. This marked the first Iranian influence operation Microsoft has detected where AI played a key component in its messaging and is one example of the fast and significant expansion in the scope of Iranian operations since the start of the Israel-Hamas conflict. The disruption reached audiences in the UAE, UK, and Canada.

Disruption of streaming TV programming using an AI-generated broadcaster

Iranian state-affiliated media reach most successful in English-speaking nations closely allied with the U.S.

Microsoft's AI for Good Lab's Iranian Propaganda Index (IPI) monitors the proportion of traffic visiting Iranian state and state-affiliated news outlets and amplifiers compared to overall traffic on the internet. In the first week of the conflict, we observed a 42% increase. That surge was particularly pronounced in the United States and its English-speaking allies (UK, Canada, Australia, New Zealand), which indicates Iran's ability to reach Western audiences with its reporting on Middle East conflicts. While this success was strongest in the early days of the war, the reach of these Iranian sources one month into the war remained 28% above pre-war levels globally.

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

Iran's cyber-enabled operations in the Israel-Hamas war have moved through three phases since October 7.

Phase 1: Reactive and misleading

The first phase saw misleading claims from Iranian state media. One example was IRGC-affiliated Tasnim News Agency claiming that a group called “Cyber Avengers” had conducted cyberattacks against an Israeli power plant “at the same time” as the Hamas attacks. Cyber Avengers itself (also likely run by the IRGC) claimed to have attacked an Israeli electric company the evening before the Hamas attacks. However, its evidence was only some weeks-old press reporting of power outages “in recent years” and a screenshot of an undated disruption to the company’s website.

Elsewhere, another cyber persona “Malek Team,” assessed by MTAC to be run by Iran’s Ministry of Intelligence and Security (MOIS) leaked personal data from an Israeli university on October 8. There was no relevance to the unfolding conflict in Gaza other than some hashtags used on X (formerly Twitter) to support Hamas. This indicates the target was opportunistic and likely based on pre-existing access.

Phase 2: All hands on deck

By mid to late October, the second phase was emerging. This saw the number of Microsoft-tracked groups active in Israel rise from nine in the first days to 14 by day 15. Sometimes, multiple Iranian groups were targeting the same organization or military base in Israel with cyber or influence activity. This suggests coordination, common objectives set in Tehran, or both.

Furthermore, the use of cyber-enabled influence operations against Israel significantly accelerated. Iran showed its preference for such attacks in 2022 when it increased the pace of such operations from roughly every other month to multiple operations a month. Iran’s 10 cyber-enabled operations against

Israel in October marks a new high point. This was nearly double the previous high point of six operations per month in November 2022, though these previous attacks spanned operations targeting four countries.

One example happened on October 18 when the IRGC's Shahid Kaveh Group 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.

Phase 3: Expanding geographic scope

In late November 2023, Iranian groups began expanding their cyber-enabled influence beyond Israel, targeting countries Iran perceives are supporting Israel. This aligned with the Iran-backed Houthis starting their attacks on international shipping.

On November 20, the MOIS-aligned cyber persona "Homeland Justice" warned of forthcoming cyberattacks on Albania. They later claimed credit for attacks on a range of Albanian organizations and institutions on Christmas day.

On November 21, the 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, including taking one offline at a water authority in Pennsylvania on November 25. PLCs are industrial computers adapted for the control of manufacturing processes, such as assembly lines, machines, and robotic devices.

Defaced PLC at Pennsylvania water authority with Cyber Avengers logo on November 25. The Cyber Avengers posted the same message the next day on their Telegram channel as a caption to a video of Netanyahu, speaking at an American Israel Public Affairs Committee (AIPAC) conference, indicating an intent to target U.S. equipment made in Israel.

Iran's influence objectives in the Israel-Hamas war

Iran's efforts to undermine Israel and its supporters across the internet and social media, causing general confusion and a loss of trust are driven by four underlying objectives.

1. Destabilization through polarization

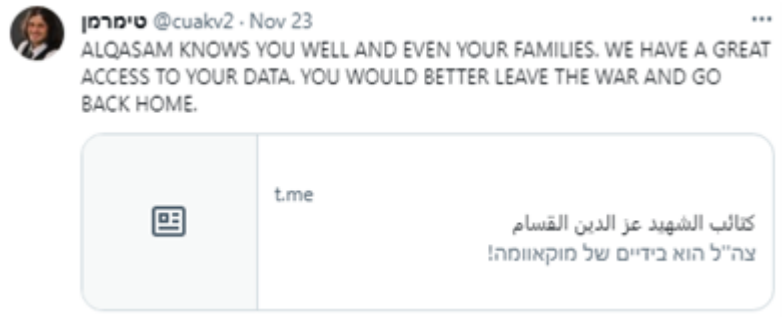
Iran aims to exacerbate domestic political and social rifts in its targets, often focusing on the Israeli government's approach to the 240 hostages taken by Hamas into Gaza and masquerading as peace-seeking activist groups criticizing the Israeli government. Israeli Prime Minister Netanyahu is the primary target of such messaging, often calling for his removal.

2. Retaliation

Many of Iran's messaging and targets are explicitly retaliatory. The persona Cyber Avengers claimed it had targeted Israeli electricity, water, and fuel infrastructure in retaliation for Israel stating it would cut off electricity, water and fuel to Gaza and elsewhere referenced "an eye for an eye."

3. Intimidation

Iran's operations also aim to undermine Israeli security and intimidate Israel's citizens and international supporters and threaten the families of IDF soldiers. Sockpuppet accounts spread messaging on X that the "IDF does not have any power to protect its own soldiers." Other messaging, as in the example below, appears aimed at attempting to convince IDF soldiers to give up.



4. Undermining international support for Israel

Iranian Influence actors often include messaging that seeks to weaken international support for Israel by highlighting the damage caused by Israel's attacks on Gaza.

Trends in Iranian influence operations

Impersonation is not new, but Iranian threat actors are now not just masquerading as their enemies but also their friends. Recent operations from Iranian groups have used the name and logo of Hamas's military wing, the al-Qassam Brigades, to spread false messaging and threaten IDF personnel. It is unclear whether Iran is acting with Hamas's consent.

Iran has managed to repeatedly recruit unwitting Israelis to engage in on-the-ground activities promoting its false operations. In one recent operation, "Tears of War," Iranian operatives convinced Israelis to hang branded Tears of War banners using AI-generated images in Israeli neighborhoods, based on Israeli press reporting.

A Tears of War banner with an image of Netanyahu that is likely AI-generated. The banner's text reads "Impeachment now." His collar translates to "#without Bibi we will win." The QR code has been intentionally blurred for publication.

Iran's use of bulk text message and email campaigns has grown in order to enhance the psychological effects of their cyber-enabled influence operations. Messages appearing on people's phones or in their inboxes have more impact than sockpuppet accounts on social media. Iran uses 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.

Trends in cyber operations

Weeks into the Israel-Hamas war, during what we view as phase 2, we began seeing examples of collaboration among Iran-affiliated groups, enhancing what the actors could achieve. This included collaboration between an MOIS group Pink Sandstorm and Hezbollah cyber units. 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.

Iranian focus on Israel has intensified. While Israel and the U.S. have always been Tehran's main targets, the outbreak of the Israel-Hamas war saw 43% of Iranian nation state cyber activity focused on Israel, more than the next 14 targeted countries combined.

Looking forward

We assess that the progression shown so far in the three phases of war will continue. Amid the rising potential of a widening war, we expect Iranian influence operations and cyberattacks will continue to be more targeted, more collaborative and more destructive as the Israel-Hamas conflict drags on. Iran will continue to test redlines, as they have done with an attack on an Israeli hospital and U.S. water systems in late November.

The increased collaboration we have observed between different Iranian threat actors will pose greater threats in 2024 for election defenders who can no longer take solace in only 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.

Tags: cyber influence, cyberattacks, cyberwar, Hamas, Iran, Israel