Research memo

FDD
Foundation for
Defense of Democracies

A Year of Meming Dangerously: Iranian Influence Operations Targeting Israel Since October 7

By Ari Ben Am

August 28, 2025

Introduction

An Israeli florist delivered a funeral bouquet in April 2024 to the parents of Liri Albag, a 19-year-old hostage in Gaza. Albag was very much alive, but the note with the bouquet said, "May her memory be a blessing, we all know that the country is more important." The customer who purchased the bouquet placed his order online and was never identified. The Israeli Security Agency (ISA), Israel's domestic intelligence arm, said it suspected the order was an Iranian ruse intended to cause anguish to the Albag family and sow division among the Israeli public.[1]

The incident illustrates how the regime in Tehran, despite its setbacks on the battlefield, has escalated its efforts to influence Israelis by exploiting the internet in different ways. Sometimes, initiatives that begin online spill offline, often intentionally, such as the delivery of a funeral bouquet to the Albags. This cruel example exemplifies how the Islamic Republic of Iran, limited in its military options for harming Israel and its population, employs influence operations of all kinds in an attempt to shape Israeli perception. A deeper understanding of how Iran conducts these operations points toward multiple lessons for the United States and its own ability to succeed in nontraditional domains of conflict.

Despite the massacre of October 7 — an overwhelming success from the perspective of Tehran and its proxies, including Hamas — the clerical regime's so-called "axis of resistance" has suffered pivotal setbacks in the war it started. With American assistance, Israel has destroyed much of Iran's nuclear and ballistic missile programs. A combination of covert operations and airstrikes eliminated Hezbollah's leadership and left it paralyzed. In the absence of support from Hezbollah, Syrian President Bashar al-Assad's regime collapsed. The Iran-backed Houthi rebels in Yemen endured both U.S. and Israeli airstrikes. Hamas suffered terrible manpower losses in Gaza, although it continues to fight. What began as a catastrophe for the Jewish state increasingly seems like a strategic defeat for its adversaries.

Nevertheless, Iranian activity online merits greater attention both because its tempo has increased since the start of the war and because Israel has not proven capable of responding decisively. This analysis examines three basic

[1] Liri Albag returned to Israel as a result of a January 2025 ceasefire with Hamas. "Shin Bet says Iran was behind funeral bouquet sent to taunt hostage's family," *The Times of Israel* (Israel), April 7, 2024. (https://www.timesofisrael.com/shin-bet-says-iran-was-behind-funeral-bouquet-sent-to-taunt-hostages-family); Israelis usually refer to the ISA as Shabak, a reference to its Hebrew acronym. Previously, they called it the Shin Bet.

categories of Iranian influence operations: cyber-enabled influence operations, online influence operations, and physical influence operations. In the first, Iran-aligned hackers attack or infiltrate a website, service, or network with the goal of extracting and leaking sensitive information, defacing the website, or employing ransomware. The second category entails inauthentic online behavior, in which hackers create fake personas or even fake news organizations, with the goal of disseminating information that seems credible to Israelis but has a demoralizing or divisive effect. Third are cases where the web serves as a communication tool to spur offline behavior, such as spraying graffiti, hanging up posters, organizing a protest, or, in the unusual case of the Albags, sending flowers.

Since October 7, the Tehran regime has stepped up its operations, increasing the range of its operational types and quality, not just their quantity. The regime's emphasis has been on the first category of operations, which entails infiltrating Israeli networks, domains, databases, industrial control systems, and other internet-connected or online infrastructure to damage them or collect, exfiltrate, and potentially delete data.[2] These operations require greater skill and effort than the others since they typically must overcome the target site's cyber defenses. Despite the lesser skill and effort required for the second category of operations, which mainly entails coordinated networks engaged in inauthentic online behavior, its tempo has remained roughly constant. The success of the third category of operations may be the most concerning, especially with Tehran's increasing ability to recruit Israelis via social media and messaging operations, then assign them offline tasks intended to lower morale or sow division either as a goal in and of themselves — or as part of espionage or covert operations.

The American public generally associates malign influence campaigns with attempts to shape election outcomes, but the case of Israel and Iran demonstrates their relevance to warfare and conflict below the threshold of war. The United States may be able to learn from this example what to expect in a wartime environment and potentially how to adjust its defenses — or even turn these tactics against those who employ them.

Cyber-Enabled Influence Operations: Iran's Hacktivist Fronts

According to Microsoft, Iranian threat actors carried out one cyber-enabled influence operation against Israel every two months on average prior to the war, whereas at least 11 occurred in October 2023 alone.[3] Those who conduct the operations often present themselves as independent "hacktivists,"[4] claims that mainly serve to mask their affiliation with the regime. Most have ties to Iran's Islamic Revolutionary Guard Corps (IRGC), but several are linked to the Ministry of Intelligence and Security (MOIS).[5] The IRGC and MOIS have created multiple new front groups targeting Israel. The fronts' methods did not change significantly after October 7 but shifted from targeting commercial and civilian entities to government, military, and industrial defense base targets.[6]

The fronts' operations have become more technically and operationally sophisticated following October 7, showing increasing coordination capabilities and investments in digital infrastructure. Still, they have not been able to penetrate high-value government and military targets. Several months prior to the massacre, Microsoft Threat

[2] "Iran surges cyber-enabled influence operations in support of Hamas," *Microsoft Threat Intelligence*, February 26, 2024. (https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas)

[3] Clint Watts, "Iran accelerates cyber ops against Israel from chaotic start," *Microsoft Threat Analysis Center*, February 6, 2024. (https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel)

[4] "Hacktivist" is a portmanteau of "hacker" and "activist." Numerous governments employ fronts that pose as hacktivists. "What is Hacktivism?" *Check Point*, accessed July 22, 2025. (https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-hacktivism)

[5] "Iran surges cyber-enabled influence operations in support of Hamas," *Microsoft Threat Intelligence*, February 26, 2024, page 7. (https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas)

[6] "Iranian backed group steps up phishing campaigns against Israel, U.S.," *Google Threat Analysis Group*, August 14, 2024. (https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us)

Intelligence reported that Iranian operators were turning to "cyber-enabled influence operations … to compensate for shortcomings in their network access or cyberattack capabilities."[7] In some instances, the threat actors falsely claim that their attacks succeeded. To support such claims, they sometimes release information they claim to have exfiltrated but is in fact publicly available data.[8] For instance, the hacktivist front Cyb3rAv3ngers repurposed previously leaked data to level false claims that they successfully compromised the Israel Electric Company.[9] Iranian state media outlets often participate in these efforts to exaggerate or invent the impact, with hacktivist fronts amplifying the message.[10] Still, Iranian threat actors have had some genuine success in hacking government, military, and private sector targets, albeit those of lesser value.

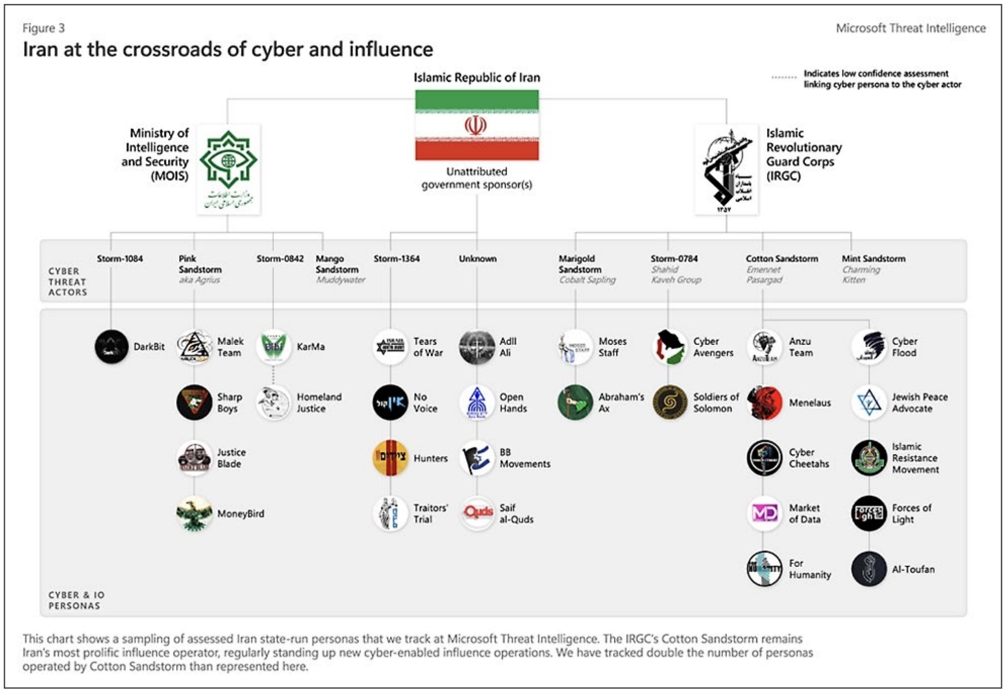


Figure 3

Iran at the crossroads of cyber and influence

Microsoft Threat Intelligence

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.

Microsoft Threat Intelligence overview of Iranian threat actor groups affiliated with the Iranian MOIS and IRGC. Source: Microsoft Threat Intelligence.

In November 2024, one Iran/Hezbollah-aligned group, Radwan Cyber Pal, compromised an Israeli Ministry of National Security server that Israeli citizens used to upload identification to receive firearm licenses.[11] In addition,

[7] "Iran turning to cyber-enabled influence operations for greater effect," *Microsoft Threat Intelligence*, May 2, 2023. (https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Iran-turning-to-cyber-enabled-influence-operations-for-greater-effect-05022023.pdf)

[8] Rafaela Goichman, "מצג שווא: האקרים איראנים טענו שפרצו למערכות בנק ישראל - אך פירסמו חומרים גלויים מהאתר [Misrepresentation: Iranian Hackers Claimed To Have Hacked Bank of Israel's Systems – But Published Open Materials From the Website]," *The Marker* (Israel), November 18, 2024. (https://www.themarker.com/captain-internet/2024-11-18/ty-article/.premium/00000193-3df0-dab9-a1db-7df5042a0000)

[9] David DiMolfetta, "Report: Iranian hackers are trying to create a psychological war in cyberspace," *NextGov/FCW*, June 24, 2025. (https://www.nextgov.com/cybersecurity/2025/06/report-iranian-hackers-are-trying-create-psychological-war-cyberspace/406267)

[10] Clint Watts, "Iran accelerates cyber ops against Israel from chaotic start," *Microsoft Threat Analysis Center*, February 6, 2024. (https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel); Clint Watts, "Rinse and repeat: Iran accelerates its cyber influence operations worldwide," *Microsoft Threat Analysis Center*, May 2, 2023. (https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat)

[11] David Hollingworth, "Exclusive: Anti-Israel hacker claims hack on Ministry of National Security, posts settler IDs online," *Cyber Daily* (Australia), November 11, 2024. (https://www.cyberdaily.au/security/11332-exclusive-anti-israel-hacker-claims-hack-on-ministry-of-national-security-posts-settler-ids-online)

a front named NetHunt3r compromised an Israeli Ministry of Defense server used for purchasing and acquisitions, exposing sensitive but not classified data.[12] A third front targeted the Israeli Ministry of Justice and published what it said were confidential documents it had extracted.[13] According to Microsoft, on October 18, 2023, an Iranian threat actor falsely claimed to have compromised cameras on an Israeli military base. In reality, the group merely posted images on Telegram taken from cameras on a residential street with the same name as the base.[14] The effort made headlines in and out of Israel.[15] Iranian threat actors posing as hacktivists have also impersonated anti-Zionist Israelis on at least one occasion to carry out hack-and-leak and wiper attacks (attacks that delete the data of the victim organization) utilizing the "BiBi" wiper malware, named after Prime Minister of Israel Benjamin Netanyahu's nickname, according to the cybersecurity firm Checkpoint.[16]

One of the most active front groups is Handala Hack, founded in December 2023, which has carried out more than 50 cyber operations against Israeli and Israel-related international targets.[17] Handala repeatedly claimed to have targeted the Israeli Iron Dome anti-missile systems and Israeli defense contractors, although it has provided no evidence of such actions.[18] The group also sent mass text messages with malicious links to Israelis and successfully accessed personal photographs and other information belonging to senior Israeli defense officials.[19] Iranian state media has amplified Handala's claims,[20] and Israeli and international media have given significant attention to their operations, even those that have been debunked or exaggerated.[21]

The ISA published information in December 2024 about more than 200 phishing attacks carried out by Iranian actors against Israeli political and military figures meant to compromise their personal devices for later doxxing and potential physical attacks.[22] Google's Threat Analysis Group exposed Iranian threat actor APT 42, affiliated with the IRGC's Intelligence Organization, as being behind most of these operations.[23]

[12] **12.** Ari Ben Am, "Memetic Warfare Weekly: Divan e-Tags e-Tabrizi," *Memetic Warfare*, April 5, 2024. (https://www.memeticwarfare.io/p/memetic-warfare-weekly-divan-e-tags)

[13] **13.** "Israel's Justice Ministry reviewing 'cyber incident' after hacktivists' claim breach," *Reuters*, April 5, 2024. (https://www.reuters.com/world/middle-east/israels-justice-ministry-reviewing-cyber-incident-after-hacktivists-claim-breach-2024-04-05)

[14] **14.** "Iran surges cyber-enabled influence operations in support of Hamas," *Microsoft Threat Intelligence*, February 26, 2024, page 8. (https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas)

[15] **15.** "Iran Promotes Cyber-Influence Operations in Support of Hamas", *Microsoft Threat Intelligence*, February 26, 2024. (https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas)

[16] **16.** "Bad Karma, No Justice: Void Manticore Destructive Activities in Israel," *Check Point Research*, May 20, 2024. (https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel)

[17] **17.** "Threat Overview of Handala Hack," *Ransomware.live*, accessed July 22, 2025. (https://www.ransomware.live/group/handala)

[18] **18.** Idan Dror and Hadar Eichler, "Handala Hack: What We Know About the Rising Threat Actor," *Check Point*, February 20, 2025. (https://cyberint.com/blog/threat-intelligence/handala-hack-what-we-know-about-the-rising-threat-actor)

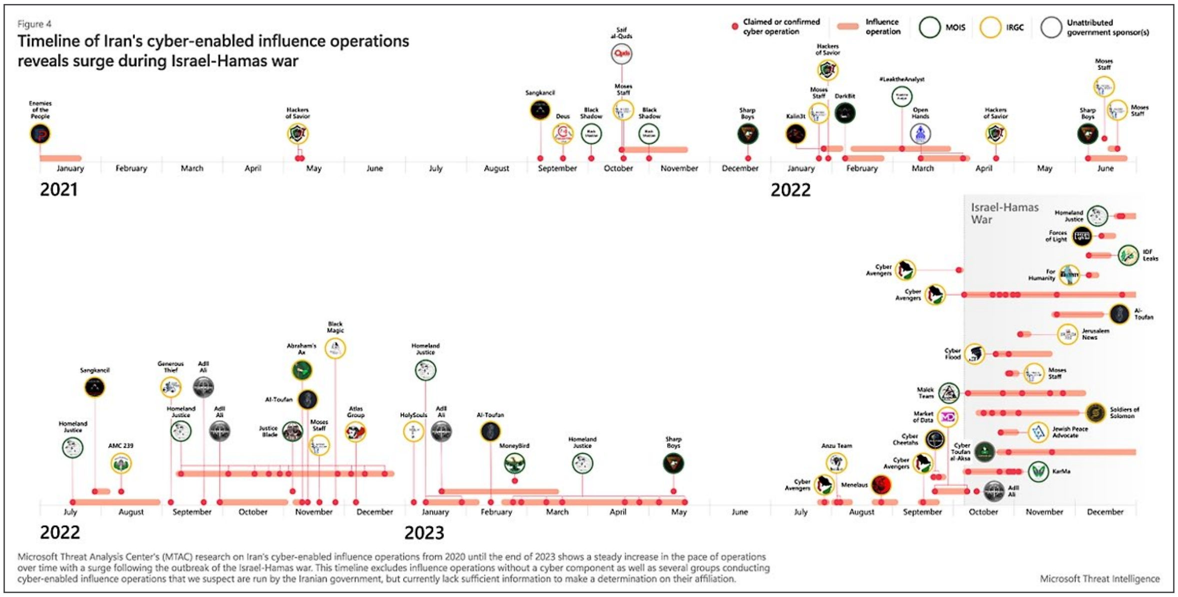
[19] **19.** Raphael Kahan, "Iranian hackers claim to breach nuclear research center system in Israel," *Ynet* (Israel), September 30, 2024. (https://www.ynetnews.com/article/bjkqmvda0)

[20] **20.** "Handala hack: How a shadowy hacker group infiltrated Israeli spy, military networks," *Press TV* (Iran), accessed December 11, 2024. (https://web.archive.org/web/20241211203050/https://www.presstv.ir/Detail/2024/11/26/737960/How-Handala-hackers-infiltrated-israeli-spy-military-apparatus)

[21] **21.** "Police say 'no breach' after Iranian hackers claim they stole gov't docs," *The Jerusalem Post* (Israel), February 10, 2025. (https://www.jpost.com/breaking-news/article-841499)

[22] **22.** Rafaela Goichman, "השב״כ: איראן ביצעה 002 ניסיונות תקיפה בסייבר של בכירים ישראלים במטרה להתנקש בהם [The ISA: Iran Conducted 200 Cyberattack Attempts Against Senior Israeli Officials With the Aim of Assassinating Them]," *The Marker* (Israel), December 2, 2024. (https://www.themarker.com/captain-internet/2024-12-02/ty-article/.premium/00000193-8820-dc84-a3d7-88ad14f10000)

[23] **23.** "Iranian backed group steps up phishing campaigns against Israel, U.S.," *Google Threat Analysis Group*, August 14, 2024. (https://blog.google/threat-analysis-group/iranian-backed-group-steps-up-phishing-campaigns-against-israel-us)



Timeline of Iranian hacktivist fronts and cyber-enabled influence operations targeting Israel, 2021-2023. Source: Microsoft Threat Intelligence.

One of the most successful doxxing efforts dubbed itself IDFLeaks and published collated case files on thousands of Israeli servicemembers.[24] Branded with Hamas logos, these files consisted of personal information taken from past data breaches as well as open-source information, such as social media profiles. Aside from the potential to instill fear, doxxing may enable additional cyber or physical harassment. Microsoft attributed IDFLeaks to the MOIS,[25] and an FDD investigation into the operation found multiple technical and behavioral indicators tying the operation to Iran.[26] (See Appendix for IDFLeaks threat indicators.)

Israeli critical infrastructure has long been a target of Iranian cyber operations, and this has continued during the war. IRGC-affiliated hacktivist front Cyb3rAv3ngers targeted Israeli water plants in October 2023 and since then has continued to target other critical infrastructure in Israel, the United States, and around the world. Cyb3rAv3ngers gained notoriety in the United States for targeting water utilities that utilized Israeli-manufactured programmable logic controllers (PLCs), a piece of equipment used for managing industrial systems, defacing screens with anti-Israel messaging.[27] The U.S. Department of the Treasury sanctioned six IRGC-affiliated cyber operators in February 2024, accusing them of operating the Cyb3rAv3ngers persona.[28]

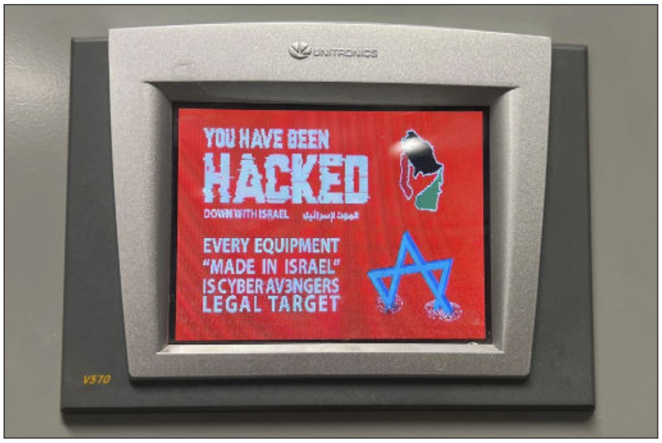
[24] **24.** Ari Ben Am and Max Lesser, "Iranian Cyber Operations Raise Fears of Attacks on Military Personnel," *The Cipher Brief*, October 3, 2024. (https://www.fdd.org/analysis/op_eds/2024/10/03/iranian-cyber-operations-raise-fears-of-attacks-on-military-personnel)

[25] **25.** "Iran surges cyber-enabled influence operations in support of Hamas," *Microsoft Threat Intelligence*, February 26, 2024. (https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas)

[26] **26.** Ari Ben Am and Max Lesser, "Iranian Cyber Operations Raise Fears of Attacks on Military Personnel," *The Cipher Brief*, October 3, 2024. (https://www.fdd.org/analysis/op_eds/2024/10/03/iranian-cyber-operations-raise-fears-of-attacks-on-military-personnel)

[27] **27.** U.S. Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, National Security Agency, Environmental Protection Agency, Israel National Cyber Directorate, and Canadian Centre for Cyber Security, "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities." December 18, 2024. (https://www.cisa.gov/sites/default/files/2024-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors.pdf); Konner McIntire, "Fact Check Team: Iranian cyberattack poses threat to Pennsylvania water utilities," *ABC 15 News*, January 5, 2024. (https://wpde.com/news/nation-world/iranian-cyberattack-poses-threat-to-pennsylvania-water-utilities-growing-us-concern-hackers-pumps-drinking-contamination-cybersecurity-audit-farm-bill-congress-data-breach)

[28] **28.** U.S. Department of the Treasury, Press Release, "Treasury Sanctions Actors Responsible for Malicious Cyber Activities on Critical Infrastructure," February 2, 2024. (https://home.treasury.gov/news/press-releases/jy2072)



Defacement of a Unitronics PLC in a U.S.-based water facility. (Source: Municipal Water Authority of Aliquippa via AP)

Aria Sepehr Ayandehsazan (ASA)

One Iranian threat actor stands out for increasingly potent capabilities. Emennet Pasargad, an IRGC-affiliated front company now operating as Aria Sepehr Ayandehsazan (ASA), is Iran's most prolific cyber-enabled influence operation threat actor. In 2022, Microsoft attributed the majority of Iran's cyber-enabled influence operations to ASA alone.[29] ASA has also carried out influence operations targeting U.S. elections.[30] The company also runs multiple hacktivist front groups.[31] ASA's operations were so pervasive that the FBI, Treasury, and the Israel National Cyber Directorate (INCD) published a joint advisory on ASA's activity in October 2024, detailing how ASA operates.[32]

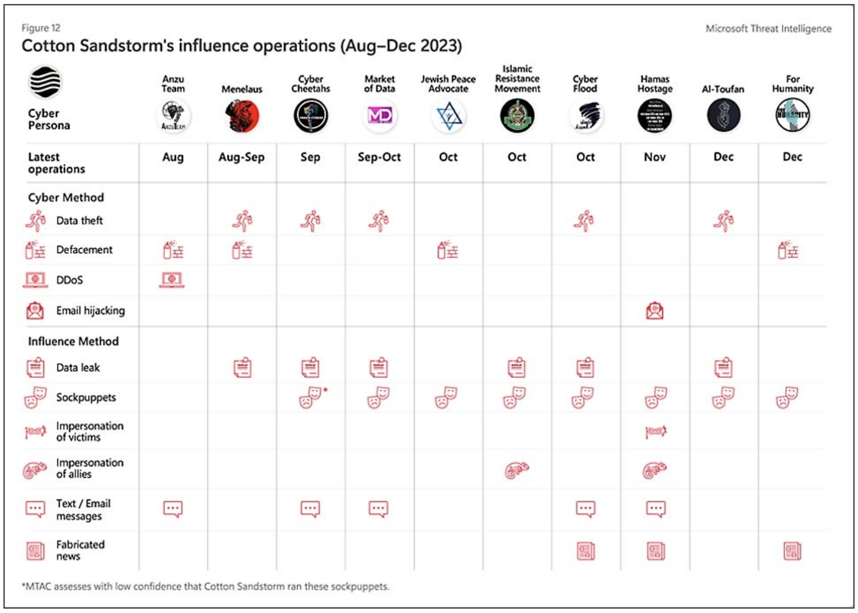


Figure 12

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.

Microsoft overview of ASA's operations, August-December 2023. Microsoft tracks ASA activity as "Cotton Sandstorm." Source: Microsoft Threat Intelligence.

[29] Clint Watts, "Rinse and repeat: Iran accelerates its cyber influence operations worldwide," *Microsoft Threat Analysis Center*, May 2, 2023. (https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat)

[30] Max Lesser and Ari Ben Am, "U.S. and Israel Expose Iran's Tenacious Malign Influence," *Foundation for Defense of Democracies*, November 8, 2024. (https://www.fdd.org/analysis/policy_briefs/2024/11/08/u-s-and-israel-expose-irans-tenacious-malign-influence); Max Lesser, Mason Krusch, and Ari Ben Am, "America Resilient in the Face of Aggressive Foreign Malign Influence Targeting the 2024 U.S. Elections," *Foundation for Defense of Democracies*, December 18, 2024. (https://www.fdd.org/analysis/2024/12/18/america-resilient-in-the-face-of-aggressive-foreign-malign-influence-targeting-the-2024-u-s-elections)

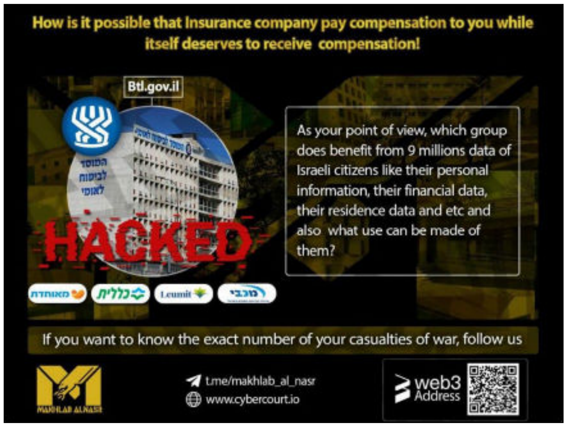
[31] "Iran surges cyber-enabled influence operations in support of Hamas," *Microsoft Threat Intelligence*, February 26, 2024, page 14. (https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas)

[32] U.S. Cybersecurity and Infrastructure Security Agency, Department of the Treasury, and Israel National Cyber Directorate, "New Tradecraft of Iranian Cyber Group Aria Sepehr Ayandehsazan aka Emennet Pasargad," October 30, 2024. (https://www.ic3.gov/CSA/2024/241030.pdf)

ASA has carried out at least four complex, high-profile operations targeting Israel following October 7.[33] It launched the first, CyberCourt, on April 4, 2024. CyberCourt's behaviors and network infrastructure align with previous Iranian activity despite its attempts to disguise its infrastructure. Last year, the U.S. government seized CyberCourt's primary domain, but it remains active on a new website.[34] Previously, to bypass other sanctions, ASA created two front companies, Server Speed and VPS Agent. ASA used these fronts to purchase server space from European providers, including Stark Industries, a Moldovan-based hosting service known for servicing Russian influence operations.[35] (See Appendix for CyberCourt threat indicators.)

The CyberCourt network presents itself as a "tribunal" that issues "verdicts against Zionist criminals."[36] The network claims to represent a broad swathe of hacktivist groups, including Iranian fronts such as Cyb3rAv3ngers and Cyber Toufan al-Aqsa, as well as non-Iranian groups, such as Anonymous Sudan. ASA also created new hacktivist fronts for the CyberCourt operation, including NetHunt3r, Anonymous South Africa, the Emirates Student Movement, and later Zeusistalking.[37] Once the CyberCourt issues a verdict, it calls upon these hacktivist member groups to exact justice.

In addition to issuing "indictments," the CyberCourt carried out two cyber operations of its own against the Israeli National Insurance Institute and the Israeli Ministry of Defense via the NetHunt3r and Makhlab al-Nasr fronts. The operations compromised web-facing portals. ASA then amplified the operations by posting exfiltrated files and data, including personal information of Israeli citizens, to hacking forums, Reddit, YouTube, and Telegram. Iranian state media also immediately amplified the attacks.[38]



How is it possible that Insurance company pay compensation to you while itself deserves to receive compensation!

As your point of view, which group does benefit from 9 millions data of Israeli citizens like their personal information, their financial data, their residence data and etc and also what use can be made of them?

If you want to know the exact number of your casualties of war, follow us

Screenshot from the Makhlab al-Nasr hacktivist front group amplifying a cyber operation targeting the Israeli National Insurance Institute. Source: Memetic Warfare.

Next, ASA targeted the Israeli delegation to the Paris Olympics in July 2024 with two distinct yet concurrent operations. First, ASA set up a new hacktivist group, Zeusistalking, and equipped it with the requisite Telegram channel, clear and Onion domains,[39] and X and Facebook accounts. As in other ASA operations, the Zeusistalking

[33] Ari Ben Am, "Unity of Hacktivist Fronts: Iranian Cyber-Enabled IO Targeting Israel," *CYBERWARCON*, November 22, 2024. (https://www.cyberwarcon.com/unity-of-hacktivist-fronts-iranian-cyber-enabled-io-targeting-israel)

[34] U.S. Cybersecurity and Infrastructure Security Agency, Department of the Treasury, and Israel National Cyber Directorate, "New Tradecraft of Iranian Cyber Group Aria Sepehr Ayandehsazan aka Emennet Pasargad," October 30, 2024. (https://www.ic3.gov/CSA/2024/241030.pdf)

[35] Ari Ben Am, "The Rise and Fall of a Mideastern Pasargad," *Memetic Warfare*, November 6, 2024. (https://www.memeticwarfare.io/p/the-rise-and-fall-of-a-mideastern); Max Lesser and Ari Ben Am, "U.S. and Israel Expose Iran's Tenacious Malign Influence," *Foundation for Defense of Democracies*, November 8, 2024. (https://www.fdd.org/analysis/policy_briefs/2024/11/08/u-s-and-israel-expose-irans-tenacious-malign-influence)

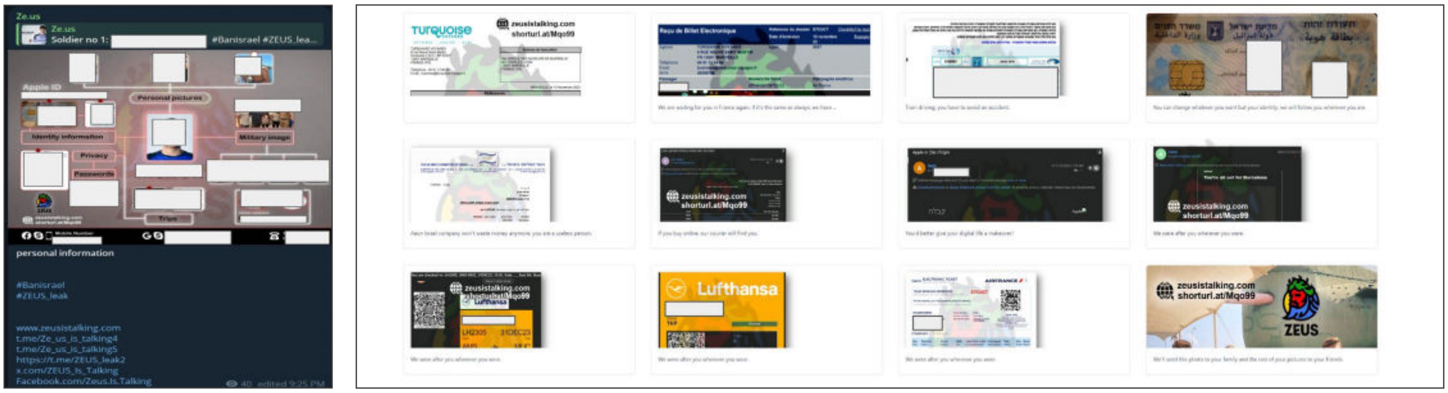
[36] Ari Ben Am, "Memetic Warfare Weekly: Divan e-Tags e-Tabrizi," *Memetic Warfare*, April 5, 2024. (https://www.memeticwarfare.io/p/memetic-warfare-weekly-divan-e-tags)

[37] U.S. Cybersecurity and Infrastructure Security Agency, Department of the Treasury, and Israel National Cyber Directorate, "New Tradecraft of Iranian Cyber Group Aria Sepehr Ayandehsazan aka Emennet Pasargad," October 30, 2024. (https://www.ic3.gov/CSA/2024/241030.pdf)

[38] Ari Ben Am, "Memetic Warfare Weekly: Divan e-Tags e-Tabrizi," *Memetic Warfare*, April 5, 2024. (https://www.memeticwarfare.io/p/memetic-warfare-weekly-divan-e-tags)

[39] Clear, or clearweb, domains are available on the open internet and via any browser. Onion domains are dark web domains that end with a ".onion" top level domain and can be accessed by the TOR or I2P browsers.

domains employed tracking pixels, which are small image files that gather information on visitors, to monitor web traffic. ASA also set up prepositioned backup domains and a large number of backup Telegram channels in case their initial domain, channels, or accounts were taken down.[40] ASA operators then compromised the Israeli Olympic Commission and used the Zeusistalking network to post the personal information and travel accommodations of the Israeli Olympic delegation. CyberCourt announced retroactively that this operation resulted from a CyberCourt "indictment."[41] Just 12 hours after the operation launched, Iranian state media outlet HispanTV began to cover it, showing probable coordination between ASA and Iranian state media outlets.


Ze.us

Ze.us
Soldier no 1: [redacted] #Banisrael #ZEUS_lea...

personal information

#Banisrael
#ZEUS_leak

www.zeusistalking.com
t.me/Ze_us_is_talking4
t.me/Ze_us_is_talking5
https://t.me/ZEUS_leak2
x.com/ZEUS_Is_Talking
Facebook.com/Zeus.Is.Talking

40 edited 9:25 PM

Personal information chart of an Israeli Olympic athlete, posted by Zeusistalking (left). Screenshots of travel documents, accommodation reservations, and personal information of Israeli Olympic athletes from the Israeli Olympic Commission (right). Source: Memetic Warfare.

For the second operation targeting the Israeli Olympic delegation, ASA set up "RGUD," whose name is a reference to the now defunct French far-right group Groupe Union Défense (GUD). RGUD then sent text messages and emails with death threats to Israeli athletes. RGUD also sent texts to multiple Israelis in Hebrew, inviting recipients to the funerals of specific Israeli athletes.[42]

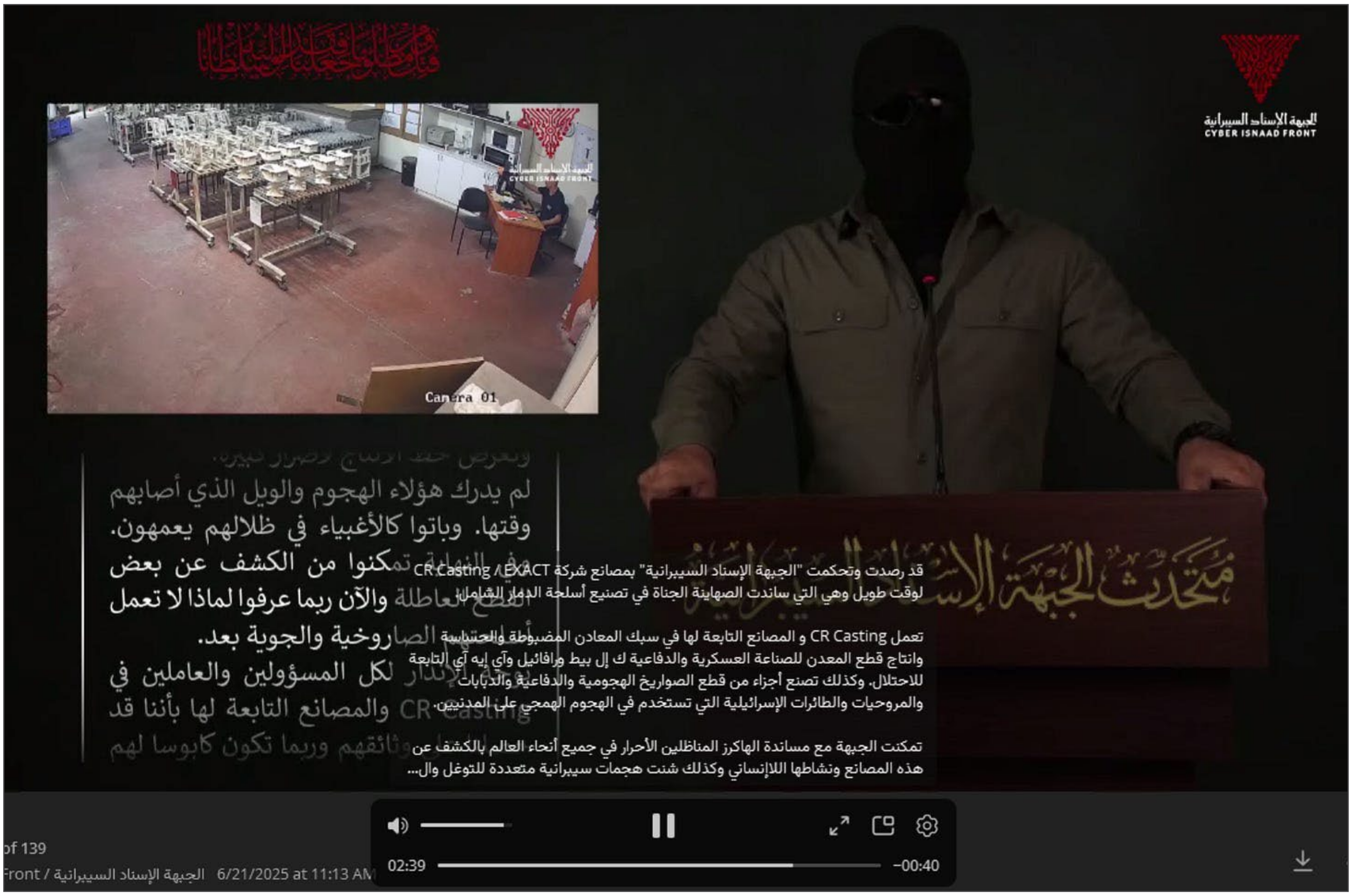
ASA continues to target Israel. During Israel's Operation Rising Lion, ASA appears to have created a new hacktivist front, the "Cyber Isnaad Front." The Cyber Isnaad Front is an Arabic-language group active on Telegram and an Onion domain and has targeted Israeli defense contractors and other military and government targets in the short time that it has been operational, leaking data online and doxxing employees.[43] Multiple technical and behavioral elements of the Cyber Isnaad Front align with past ASA operations. In a notable development, the Cyber Isnaad Front uses a human actor in multiple-minute-long videos to showcase their intrusions into Israeli companies.

40. Ari Ben Am, "Chadhaus," *Memetic Warfare*, July 29, 2024. (https://www.memeticwarfare.io/p/chadhaus)

41. Ari Ben Am, "Unity of Hacktivist Fronts: Iranian Cyber-Enabled IO Targeting Israel," *CYBERWARCON*, November 22, 2024. (https://www.cyberwarcon.com/unity-of-hacktivist-fronts-iranian-cyber-enabled-io-targeting-israel)

42. Ibid.

43. Ari Ben Am and Max Lesser, "Israeli Companies Under Attack by Hacktivists With Likely Ties to Iran," *Foundation for Defense of Democracies*, July 2, 2025. (https://www.fdd.org/analysis/2025/07/02/israeli-companies-under-attack-by-hacktivists-with-likely-ties-to-iran); الجبهة الإسناد السيبرانية / Cyber Isnaad Front, *Telegram*, June 29, 2025. (https://t.me/CyberIsnaadFront1/309)


الجبهة الإسناد السيبرانية
CYBER ISNAAD FRONT
Camera 01
لم يدرك هؤلاء الهجوم والويل الذي أصابهم
وقتها. وباتوا كالأغبياء في ظلالهم يعمهون.
تمكنوا من الكشف عن بعض
والآن ربما عرفوا لماذا لا تعمل
روخية والجوية بعد.
لكل المسؤولين والعاملين في
والمصانع التابعة لها بأننا قد
وثائقهم وربما تكون كابوسا لهم
متحدث الجبهة الإسناد السيبرانية
of 139
Front / الجبهة الإسناد السيبرانية 6/21/2025 at 11:13 AM
02:39
−00:40

قد رصدت وتحكمت "الجبهة الإسناد السيبرانية" بمصانع شركة CR Casting / EXACT
لوقت طويل وهي التي ساندت الصهاينة الجناة في تصنيع أسلحة الدمار الشامل.

تعمل CR Casting و المصانع التابعة لها في سبك المعادن المضبوطة والحساسة
وانتاج قطع المعدن للصناعة العسكرية والدفاعية ك إل بيط ورافائيل وآي إيه آي التابعة
للاحتلال. وكذلك تصنع أجزاء من قطع الصواريخ الهجومية والدفاعية والدبابات
والمروحيات والطائرات الإسرائيلية التي تستخدم في الهجوم الهمجي على المدنيين.

تمكنت الجبهة مع مساندة الهاكرز المناظلين الأحرار في جميع أنحاء العالم بالكشف عن
هذه المصانع ونشاطها اللاإنساني وكذلك شنت هجمات سيبرانية متعددة للتوغل وال...

Screenshot of a Cyber Isnaad Front video uploaded to its Telegram channel showing an alleged intrusion into the CCTV network of Israeli firm CR Casting.

One significant constraint on ASA was its difficulty acquiring hosting services from U.S. and European providers. This meant that Iranian operators likely had to invest considerable time and resources in setting up backups and finding willing hosting services. ASA's creation of front companies to procure hosting services emphasizes how critical hosting infrastructure is to these operations. Israeli government agencies are also increasingly adept at publicly identifying and reporting influence operations to social media platforms and messaging applications, forcing ASA to preposition backup infrastructure prior to a given operation.

Online Influence Operations

Before October 7, Iran employed botnets and inauthentic accounts, but their efforts rarely amounted to complex, coordinated operations.[44] These were small-scale efforts to sow discord by exploiting fault lines in Israeli domestic politics.[45] Since the war began, the pace and scale of Iranian operations have escalated. Iranian threat actors have experimented with generative AI, although they seem reliant on commercially available tools. These actors have also

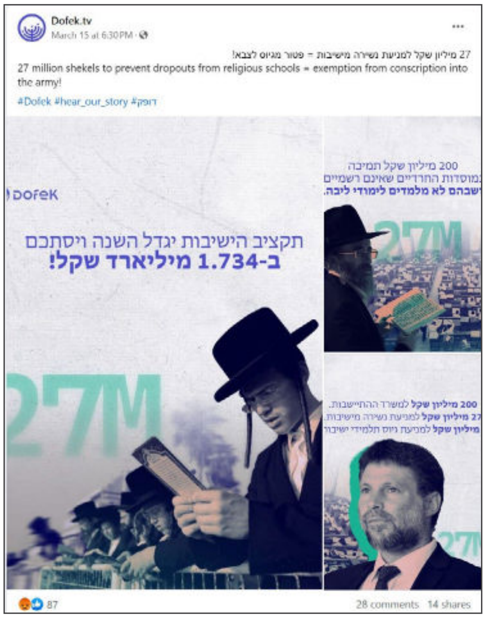
[44] Tal Shahaf, "הם נראים ישראלים, אבל הם לא: רשת הפרופילים המזויפים שמפלגת את המדינה [They Look Israeli, but They're Not: The Network of Fake Profiles That Divides the Country]," *Ynet* (Israel), December 8, 2024. (https://www.ynet.co.il/digital/technology/article/r1fxvz74kx)

[45] Inbal Orpaz and David Siman-Tov, "Foreign Interference and Iranian Influence on Social Networks in Israel," *Institute for National Security Studies*, November 13, 2024. (https://www.inss.org.il/publication/iranian-influence)

made innovative use of nontraditional platforms for influence operations, such as messaging applications and Google tools. In some instances, the inauthentic nature of the Iranian operations is readily apparent.

Iran-promoted content now emphasizes divisions about the conduct of the war, perhaps with an eye toward weakening the Israeli resolve to fight. Key themes include Netanyahu's alleged prolonging of the war to maintain his grip on power, the reliance of Netanyahu's coalition on far-right parties, the exemption of ultra-Orthodox Jews from the draft, and tensions in U.S.-Israel relations.[46]

One indicator of the growing ambition of Iranian efforts to deceive Israeli audiences is the creation of websites posing as authentic Israeli news organizations. In February 2024, Iran created Dofek TV, a centralized network comprised of a domain, Facebook page, and accounts on Instagram and other platforms, yet poor operational security ensured its exposure as a fraud. An investigation showed that Dofek TV's Facebook page operators were based in Lebanon, and Arabic file names were visible in its source code. Dofek used Facebook and Instagram ads to improve its reach, but most of the network's content still received only dozens or hundreds of views.[47] Memetic Warfare first exposed Dofek as an inauthentic network, and Israeli media outlet Walla covered the operation in April 2024.[48] Meta dismantled Dofek's accounts later that year.[49]



Dofek.tv
March 15 at 6:30PM ·

27 מיליון שקל למניעת נשירה מישיבות = פטור מגיוס לצבא!
27 million shekels to prevent dropouts from religious schools = exemption from conscription into the army!
#Dofek #hear_our_story #דופק

dofek
תקציב הישיבות יגדל השנה ויסתכם
ב-1.734 מיליארד שקל!
27M
200 מיליון שקל תמיכה
במוסדות החרדיים שאינם רשמיים
ושבהם לא מלמדים לימודי ליבה.
200 מיליון שקל למשרד ההתיישבות.
27 מיליון שקל למניעת נשירה מישיבות.
מיליון שקל למניעת גיוס תלמידי ישיבו

87
28 comments 14 shares

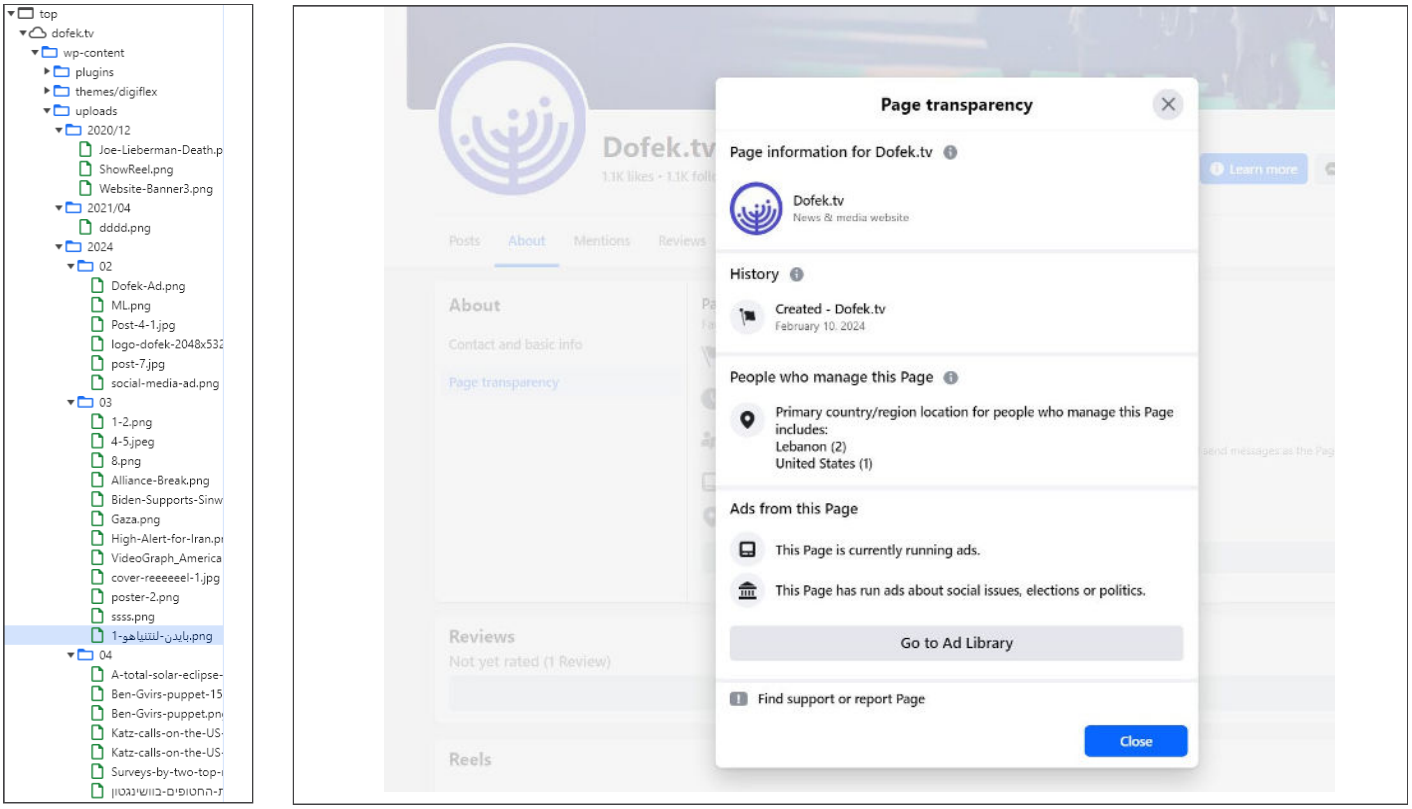
Content sample from the Dofek TV Facebook page, showing content meant to sow strife between secular and religious Israelis. Source: Memetic Warfare.

[46] **46.** Shlomi Heller and Bini Ashkenazi, "חשיפה: אתר חדשות ישראלי מופעל לכאורה ע"י גורמים זרים - ומשפיע על עשרות אלפי ישראלים [Exposure: Israeli News Website Allegedly Operated by Foreign Entities - and Affecting Tens of Thousands of Israelis]," *Walla News* (Israel), April 18, 2024. (https://news.walla.co.il/item/3659026)

[47] **47.** Ari Ben Am, "The Mauve Cyb3rAv3nger," *Memetic Warfare,* April 11, 2024. (https://www.memeticwarfare.io/p/the-mauve-cyb3rav3nger)

[48] **48.** Shlomi Heller and Bini Ashkenazi, "חשיפה: אתר חדשות ישראלי מופעל לכאורה ע"י גורמים זרים - ומשפיע על עשרות אלפי ישראלים [Exposure: Israeli News Website Allegedly Operated by Foreign Entities - and Affecting Tens of Thousands of Israelis]," *Walla News* (Israel), April 18, 2024. (https://news.walla.co.il/item/3659026)

[49] **49.** Margarita Franklin and Mike Torrey, "Q3 2024 Adversarial Threat Report," *Meta*, December 2024. (https://transparency.meta.com/sr/Q3-2024-Adversarial-threat-report)



```
top
  dofek.tv
    wp-content
      plugins
      themes/digiflex
      uploads
        2020/12
          Joe-Lieberman-Death.p
          ShowReel.png
          Website-Banner3.png
        2021/04
          dddd.png
        2024
          02
            Dofek-Ad.png
            ML.png
            Post-4-1.jpg
            logo-dofek-2048x532
            post-7.jpg
            social-media-ad.png
          03
            1-2.png
            4-5.jpeg
            8.png
            Alliance-Break.png
            Biden-Supports-Sinw
            Gaza.png
            High-Alert-for-Iran.p
            VideoGraph_America
            cover-reeeeeel-1.jpg
            poster-2.png
            ssss.png
            1-بايدن-لنتنياهو.png
          04
            A-total-solar-eclipse-
            Ben-Gvirs-puppet-15
            Ben-Gvirs-puppet.pn
            Katz-calls-on-the-US-
            Katz-calls-on-the-US-
            Surveys-by-two-top-
            ת-החטופים-בוושינגטון
```

Page transparency

Page information for Dofek.tv

Dofek.tv
News & media website

History

Created - Dofek.tv
February 10, 2024

People who manage this Page

Primary country/region location for people who manage this Page includes:
Lebanon (2)
United States (1)

Ads from this Page

This Page is currently running ads.

This Page has run ads about social issues, elections or politics.

Go to Ad Library

Find support or report Page

Close

Arabic-language file name on the Dofek TV domain (left). Dofek TV's Facebook page's transparency section, exposing two managers in Lebanon (right). Source: Memetic Warfare.

Several months later, Iran launched a similar effort, this time called "Israel in a Minute."[50] Its operators used commercially available AI tools to generate two inauthentic news anchors.[51] Much of the operation's video content was AI-generated as well, and many of its accounts utilized generative adversarial networks (GAN)[52] to create images for profile pictures.[53] Its content, however, garnered fewer than a few hundred views.

Meta linked Dofek, Israel in a Minute, and a third effort, "Halalom Israel," to Lebanese operators with ties to the pro-Hezbollah,[54] Bahraini outlet LuaLua TV, whose web domain the U.S. Department of Justice (DOJ) seized in 2021 due to violations of sanctions on Iran.[55] Accordingly, Meta dismantled the accounts of all three.[56] While Meta did not directly attribute the operation to Iran, the direct involvement of pro-Hezbollah and sanctions-violating media outlets point to regime control or guidance.

[50] Ari Ben Am, "The Mauve Cyb3rAv3nger," *Memetic Warfare*, April 11, 2024. (https://www.memeticwarfare.io/p/the-mauve-cyb3rav3nger)
[51] Ibid.
[52] Generative Adversarial Networks can be used to create new content by randomly merging various elements of data from a training set. GAN images are often used in influence operations, including freely available tools such as thispersondoesnotexist.com.
[53] Margarita Franklin and Mike Torrey, "Q3 2024 Adversarial Threat Report," *Meta*, December 2024. (https://transparency.meta.com/sr/Q3-2024-Adversarial-threat-report)
[54] "Israel blocks pro-Iran Al-Mayadeen TV website over security concerns," *i24 News* (Israel), November 13, 2024. (https://www.i24news.tv/en/news/israel-at-war/1699896177-israel-blocks-pro-iran-al-mayadeen-tv-website-over-security-concerns)
[55] "U.S. blocks websites linked to Iranian disinformation," *Reuters*, June 22, 2021. (https://www.reuters.com/world/middle-east/notices-iran-linked-websites-say-they-have-been-seized-by-us-2021-06-22)
[56] Margarita Franklin and Mike Torrey, "Q3 2024 Adversarial Threat Report," *Meta*, December 2024. (https://transparency.meta.com/sr/Q3-2024-Adversarial-threat-report)

Decentralized influence operations, such as X botnets or masses of inauthentic accounts, are also a recurring feature of Iranian influence operations targeting Israel. Israeli NGO FakeReporter and news outlet Ynet exposed one cluster of suspicious accounts on X, Facebook, and Instagram with significant reach among Israelis.[57] Posting in a coordinated fashion across multiple platforms, the cluster generated inauthentic images of Israeli politicians and soldiers and posted incendiary content. One image showed Netanyahu holding a gun to an Israeli hostage's head, with the caption "I'm sorry, but I have to stay in power." The network uploaded content in Hebrew (likely AI-generated), English, Russian, Spanish, and Amharic, all languages commonly spoken in Israel. In contrast to the networks that Meta identified, this cluster achieved greater exposure among Israelis. According to FakeReporter and Ynet, the network was active in over 1,200 Israeli Facebook groups.

Emerald Divide

One of the most prolific online influence campaigns, dubbed Emerald Divide,[58] created different personas, groups, and channels on WhatsApp, YouTube, Instagram, TikTok, and especially Telegram to target a broad spectrum of Israelis. Emerald Divide created fronts like "Jewish Fist" to masquerade as far-right Kahanist groups, while "The Secular Israelis" and other fronts pretended to be groups opposed to ultra-Orthodox Jews. The operation exploited the religious-LGBTQ divide, left/right partisanship, and discontent with the elected coalition following October 7.

Emerald Divide also created operations focused on Israeli casualties of war and hostage families. Its "Tears of War" Telegram channel, for instance, posted information on Israeli soldiers killed in action. The channel also shared pictures of Israeli hostages to promote protests against the government. Narratives and campaigns exploiting topics such as volunteering for hostage families gained some limited traction in Israel, although the overall impact is hard to measure. Recorded Future sampled the followers of one of Emerald Divide's Instagram accounts and found that the majority were likely inauthentic bots.[59]

Emerald Divide also distinguished itself through its use of Google Forms and online petitions. At least two Emerald Divide entities urged viewers to register on Google Forms for fictional volunteering opportunities or protests. Those who signed up provided the Iranian operators with their personal information.

Employing the same tactic, the Emerald Divide Telegram channel "Traitor Trial" created a petition on Drove, an Israeli public petition site, to garner signatures calling for trials of right-wing Israelis supportive of highly controversial judicial reform legislation. Traitor Trial used generative AI to write the petition, and the overwhelming majority of its more than 10,000 signatures appear to be inauthentic.[60] Another Emerald Divide entity circulated a Drove petition calling for the return of Israeli hostages. Real Israelis appear to have signed the petition, in the process turning over their email address and basic personal information to the Iranian operators. The utilization of a domestic Israeli platform like Drove demonstrates a level of awareness of Israeli society on the part of the operators.

Emerald Divide (and other Iranian operations) also tricked Israeli influencers on Telegram into spreading Iran's propaganda. Tears of War, for example, paid Israeli influencer Daniel Amram to unwittingly promote its channel

[57] Tal Shahaf, "הם נראים ישראלים, אבל הם לא: רשת הפרופילים המזויפים שמפלגת את המדינה [They Look Israeli, but They're Not: The Network of Fake Profiles That Divides the Country]," *Ynet* (Israel), December 8, 2024. (https://www.ynet.co.il/digital/technology/article/r1fxvz74kx)

[58] Insikt Group, "Iran-Aligned Emerald Divide Influence Campaign Evolves to Exploit Israel-Hamas Conflict," *Recorded Future*, May 8, 2024. (https://go.recordedfuture.com/hubfs/reports/ta-2024-0508.pdf)

[59] Ibid.

[60] Ari Ben Am, "Memetic Warfare Weekly: Telegram Traitor Trials?" *Memetic Warfare*, June 11, 2023. (https://www.memeticwarfare.io/p/memetic-warfare-weekly-telegram-traitor); Insikt Group, "Iran-Aligned Emerald Divide Influence Campaign Evolves to Exploit Israel-Hamas Conflict," *Recorded Future*, May 8, 2024. (https://go.recordedfuture.com/hubfs/reports/ta-2024-0508.pdf)

to his then 378,000 followers.[61] This tactic was affordable, with a single post on Amram's channel costing only 800 NIS, or approximately $220. The ability of the Iranian operators to pay for the ads suggests there may be vulnerabilities in Israeli financial enforcement mechanisms.

Iranian online influence operations ramped up significantly in June due to Israel's Operation Rising Lion. Multiple new Iranian influence networks began to operate in the early stages of the 12-day war with Israel. Many of these networks' operations openly branded themselves as pro-Iranian, rather than engaging in inauthentic behavior. One operation, "Attack Alarm," which unnamed Israeli sources attributed to the IRGC Intelligence Organization, posted information about Iranian missile attacks against Israel to spread fear.[62]

FDD identified one multiplatform influence operation, "Iran Hayom," run by a former employee of an Iranian state media outlet. The operation overtly targets Israelis with content meant to instill fear and intimidate the Israeli population.[63] Some Iranian operations also utilized crowdsourcing. For example, the "Car Online" network publicly called on and guided Iranians to create X accounts masquerading as Israelis and post demoralizing content. It provided them with instructions, lists of Hebrew names to use, and even guides on how to use ChatGPT to create content in Hebrew. Iranian media outlets have also joined the fray, with one pro-regime outlet named "Farhiktegan" creating a forged list of Israeli pilots and publishing it in an attempt to intimidate actual Israeli pilots.[64]

Physical Influence Operations

Physical influence operations leverage espionage, infiltration, and even sabotage and attempted assassinations to influence a population. In recent years, Iran has increasingly turned to physical influence operations. This may be because they tend to have a greater impact: the intended target is more susceptible to the influence because a fellow citizen undertakes the activities. A target who realizes a foreign country is behind the intrusion is likely to feel a greater sense of vulnerability to future attacks. Some of these operations make national or even international headlines, achieving greater reach than the operator could otherwise.

The prevalence of Iranian physical influence operations following October 7 stems from Iran's successes in recruiting human intelligence assets in Israel. While the operations themselves have enjoyed only minor success, this remains a potent vector of influence because of the perception (rather than reality) of the operation's efficacy. Physical influence operations can also further Iran's ability to conduct online influence operations. Photographs from protests and military sites can be used to create new fake content for online influence campaigns.

Iran has achieved unusual success in recruiting human intelligence assets in Israel since October 7. The ISA saw a meteoric 400 percent jump in counter-espionage-related arrests in 2024 compared with 2023. The Shin Bet reportedly busted 13 Iranian cells and issued 27 indictments against Israelis spying for Iran.[65] Iranian intelligence

[61] Mor Speyer, "'עצרנו את הפרסום': האיראנים הפיצו קמפיין אנטי-ישראלי בערוץ הטלגרם של דניאל עמרם ['We Stopped the Advertising': Iranians Spread Anti-Israel Campaign on Daniel Amram's Telegram Channel]," *Israel Hayom* (Israel), May 16, 2024. (https://www.israelhayom.co.il/news/local/article/15759658)

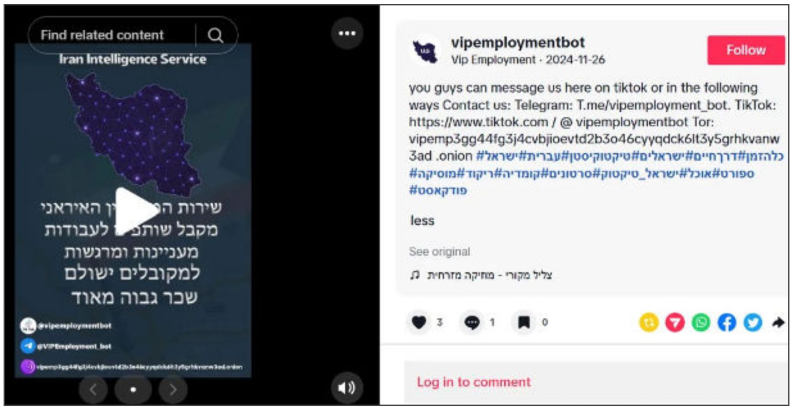
[62] Yinon Ben Shoshan, "האקרים איראנים טוענים שצה"ל משתמש באזרחים כמגנים אנושיים - וצייצו מחדש את פרשן חדשות 21 [Iranian Hackers Claim the IDF Is Using Civilians as Human shields - and Retweeted the News 12 Commentator]," *Walla Tech*, June 16, 2025. (https://tech.walla.co.il/item/3757778)

[63] Max Lesser, "FDD Connects Anti-Israel Network on Social Media to Iranian Website, Pro-Regime Actor," *Foundation for Defense of Democracies*, July 1, 2025. (https://www.fdd.org/analysis/2025/07/01/fdd-connects-anti-israel-network-on-social-media-to-iranian-website-pro-regime-actor)

[64] Ibid.

[65] Amir Bohbot, "סוכלו 040,1 פיגועים ו-007 מתקפות סייבר: דו"ח שב"כ ל-4202 [1,040 Terrorist Attacks and 700 Cyber Attacks Were Thwarted: ISA's 2024 Report]," *Walla News* (Israel), July 1, 2024. (https://news.walla.co.il/item/3715808)

officers first contacted many of the individuals in these cells over Telegram and other platforms. Tehran paid recruits with cryptocurrency to conduct espionage, sabotage, physical influence operations, and assassination attempts.[66]



vipemploymentbot
Vip Employment · 2024-11-26

you guys can message us here on tiktok or in the following ways Contact us: Telegram: T.me/vipemployment_bot. TikTok: https://www.tiktok.com / @ vipemploymentbot Tor: vipemp3gg44fg3j4cvbjioevtd2b3o46cyyqdck6lt3y5grhkvanw 3ad .onion #כלהזמן#דרךחיים#ישראלים#טיקטוקיסטן#עברית#ישראל #ספורט#אוכל#ישראל_טיקטוק#סרטונים#קומדיה#ריקוד#מוסיקה #פודקאסט

♫ צליל מקורי - מוזיקה מזרחית

Suspected Iranian human asset recruitment operation targeting Israel, posted in November 2024. Source: Memetic Warfare.

Despite the Shin Bet's efforts, Iranian human asset recruitment continues unabated. Iran set up one overt recruitment operation appealing to Israelis via TikTok and Telegram in August 2024.[67] Authorities blocked it, but this type of overt recruitment may stoke fears of Iranian infiltration of Israel. In January 2025, the Israel Police published a video in Hebrew, Arabic, and Russian encouraging those contacted by Iranian intelligence officers to contact the police immediately.[68] While the operation was exposed, this type of overt asset recruitment is in itself a form of influence operation, triggering concerns of Iranian infiltration of Israeli society.

Despite Iran's success in recruiting some Israelis, these recruits have so far had limited impact. Tehran has often employed them to conduct low-level influence operations rather than espionage targeting sensitive sites. This lack of success may be at least partially attributed to the fact that Iran often recruits from marginalized groups whose members do not have access to sensitive military information.[69] Instead, recruits put up posters, set fires, deface ATMs, spray graffiti, and photograph political activists.[70] Disconcertingly, however, Iran has also used these human assets to track the movement of an Israeli nuclear scientist and even attempted to arrange the scientist's assassination in exchange for $60,000.[71] In another high-profile case, an Israeli man, who Iranian intelligence officers contacted over Telegram, was arrested after placing explosives near the residence of the Israeli defense minister in a failed attempt to assassinate him.

Accepting assignments to conduct influence operations may prepare Israeli recruits for higher-value work. At first, individuals may balk at requests to photograph a sensitive installation or carry out an assassination but agree to put up posters in exchange for a few hundred dollars. Once comfortable with working for Iranian intelligence and proven willing to carry out basic tasks, the recruit may accept more challenging work. For example, an Israeli soldier (and later reservist) accepted a request to conduct an influence operation because he believed the work was

[66] Oren Aharoni, "חשיפה: כך מגייסים האיראנים סוכנים בישראל [This Is How the Iranians Recruit Agents in Israel]," *FakeReporter* (Israel), April 29, 2024. (https://fakereporter.net/exposures/חשיפה-כך-מגייסים-האיראנים-סוכנים-בישר)

[67] "Working 9 to Fars," *Memetic Warfare*, January 20, 2025. (https://www.memeticwarfare.io/p/working-9-to-fars)

[68] Yaniv Kubovich, "Israel Struggles With Iran's Recruiting of Its Citizens for Spying," *Haaretz* (Israel), January 31, 2025. (https://www.haaretz.com/israel-news/security-aviation/2025-01-31/ty-article/.premium/israel-struggles-with-irans-recruiting-of-its-citizens-for-spying/00000194-bd2b-d5a7-ab9d-ffbb55ca0000)

[69] "Ramat Gan Man Accused of Working for Iranian Agent, Hanging Posters Encouraging Military Coup," *The Times of Israel* (Israel), August 19, 2024. (https://www.timesofisrael.com/liveblog_entry/ramat-gan-man-accused-of-working-for-iranian-agent-hanging-posters-encouraging-military-coup)

[70] "Israeli Couple from Lod, Man from Bnei Brak Are Latest Charged With Spying for Iran," *The Times of Israel* (Israel), October 31, 2024. (https://www.timesofisrael.com/israeli-couple-from-lod-man-from-bnei-brak-are-latest-charged-with-spying-for-iran)

[71] Julian Borger and Jamal Risheq, "A text, a Telegram link, then an offer of money: how Iran sought to recruit spies in Israel," *The Guardian* (UK), July 6, 2025. (https://www.theguardian.com/world/2025/jul/06/how-iran-sought-to-recruit-spies-in-israel)

easy money. The Iranian operator at first asked the soldier to spray pro-Iran graffiti, and only later tasked him with filming a classified Iron Dome system. The individual has since been arrested and is awaiting trial.[72]

Israel's Response

Israel has only begun to adjust to the threat posed by online influence operations. The ISA, which is the body responsible for countering all forms of foreign interference, mainly operates covertly. The public nature of foreign interference clashes with covert collection methods, leaving the public unaware and uninformed of the threat. In addition, the ISA, like the Israeli defense apparatus overall, relies mainly on closed or classified sources, such as human, imagery, and signals intelligence. These are often unsuitable for sharing with the Israeli public, lest the information jeopardize sources and methods. By contrast, monitoring online influence activity at scale both effectively and legally requires open-source intelligence methodology and tools.

In a sign of progress, the ISA has begun publishing advisories on Iranian interference activity, but the information provided is often published without context or the technical details, known as threat indicators, which enable other organizations working to counter online interference to identify the same or similar threats.[73]

The Israel National Cyber Directorate (INCD) has attempted to remediate the situation by exposing Iranian threat actors. At Israel's Cyber Tech conference in April 2024, for example, the INCD's director-general exposed the "Black Shadow" threat actor as being run by an MOIS-affiliated front company.[74] The INCD also published reports and advisories on Iranian fronts, such as Zeusistalking,[75] and collaborated with U.S. counterparts on a joint advisory about ASA.[76] However, INCD's response time is often slow and irregular — for example, at the time of this writing, the INCD has yet to publish any alerts on foreign influence operations that took place during Operation Rising Lion.

Nevertheless, the INCD is the logical body to complement the ISA with more public-facing counter-influence work. To do so, however, it needs to mature its public communications and a settled legal framework for countering online influence operations. The government's response to Iranian hackers' penetration of the Ministry of Justice illustrates the need for updated thinking on the legal front. After the hack, the ministry issued a gag order (which remains in effect) on the details and content of the hack.[77] While the gag order prevents publishing about the hack in Israel, foreign news outlets have published on the leaks, making the impact of the gag order minimal. Indefinite gag orders also prevent researchers from publishing analysis and threat indicators, reducing the preparedness of other potential targets and limiting free speech.

[72] "שני חיילי מילואים חשודים בריגול: 'מידע מאוד רגיש על כיפת ברזל הועבר לאיראן' [2 Reservists Suspected of Espionage: 'Very Sensitive Information on Iron Dome Was Transferred to Iran']," *Ynet News* (Israel), June 30, 2024. (https://www.ynet.co.il/news/article/skgmhh4okl)

[73] Yoav Zitun, "Shin Bet discloses Iran's social media strategy to recruit Israelis," *Ynet News* (Israel), May 2, 2025. (https://www.ynetnews.com/article/hjwqhnmka)

[74] Israel National Cyber Directorate, Press Release, "Head of the Israel National Cyber Directorate Gaby Portnoy at the Cybertech Conference: The intensity of cyber attacks has increased threefold during the war," April 10, 2024. (https://www.gov.il/en/pages/cyber_tech_2024)

[75] Israel National Cyber Directorate, "קמפיין מדינתי כנגד המשלחת הישראלית לאולימפיאדה [National Campaign Against the Israeli Olympic Delegation]," July 31, 2024. (https://www.gov.il/BlobFolder/reports/alert_1781/he/ALERT-CERT-IL-W-1781.pdf)

[76] U.S. Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, National Security Agency, Environmental Protection Agency, Israel National Cyber Directorate, and Canadian Centre for Cyber Security, "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities." December 18, 2024. (https://www.cisa.gov/sites/default/files/2024-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors.pdf)

[77] Omer Benjakob, "After Iran Steals Sensitive Israeli Data, Israel Tries to Censor the Internet," *Haaretz* (Israel), August 21, 2024. (https://www.haaretz.com/israel-news/security-aviation/2024-08-21/ty-article-magazine/.premium/israels-futile-war-against-massive-iranian-hack-of-secret-data/00000191-6bd7-d1ee-afb5-6bff8a510000)

Recommendations

U.S. policymakers and Western hosting services and social media platforms can learn four lessons from Iranian influence operations and Israel's responses. The high tempo and volume of the operations can make it hard to respond in a timely manner to hostile narratives. However, the United States and its partners can and should degrade Iran's and other adversaries' abilities to conduct influence operations.

1. **Strengthen know-your-customer (KYC) processes for hosting services in America and Europe:** The need to secure domain hosting continues to limit the scale of Iranian influence operations. Without hosting services, threat actors cannot create and maintain websites and other digital infrastructure. Western hosting services tend to be more reliable and less likely to attract scrutiny from governments or users. To access these services, Iranian operators often rely on front companies to evade sanctions and other regulations. If America and its allies require hosting servers to strengthen their KYC processes, Iran and other adversaries will have a harder time accessing the infrastructure they need for influence campaigns (and other malicious activity in cyberspace).

2. **Remove and prevent the creation of fake accounts on social media:** Most influence operations rely on easily acquired fake accounts to promote their content online. Social media companies already take down numerous fake accounts while relying on various screening measures to prevent the creation of new ones, yet their efforts do not match the scale of the problem. More can be done.[78] Platforms should redouble their investment in information security, counterintelligence, and trust and safety teams to holistically understand and preempt the exploitation of their platforms not only for influence operations but also for recruitment efforts and cyber operations.

3. **Empower agencies to utilize open-source intelligence to counter foreign malign influence:** Leveraging open sources for intelligence collection enables defenders to operate at a pace closer to that of the adversary. The U.S. intelligence community and government as a whole should adopt open-source intelligence methodologies and tooling to support efforts to counter malign foreign influence. Government agencies should not only leverage information available on social media but should also increasingly look at messaging applications and newer forms of online social media as part of open-source collection.

   In parallel, these agencies should publish detailed technical reports and advisories on a regular basis. The U.S. government's response to foreign interference in the 2024 presidential election illustrates how proactive investigation and response to foreign influence operations, even without open-source evidence to substantiate claims, can take the edge off of adversarial operations.[79] France's VIGINUM and its detailed technical reporting on Russian influence operations is another useful example, empowering governments and companies worldwide to identify and act against exposed infrastructure and assets. High-quality and technical open-source intelligence reporting can also be a useful vector for laundering data gleaned from closed-source or technical collection methods, enabling the U.S. government to bring to bear its full apparatus of collection sources and methods.

4. **Develop a strategy for covert influence operations that seek to actively degrade adversarial capabilities:** In addition to strengthening its defenses against influence operations, the United States needs to go on the offensive to degrade the capabilities of its adversaries in cyberspace. The government should consider how and when

[78] Max Lesser, Sophie McDowall, and Cat Smith, "Nip the Bots in the Bud: Proactively Taking Down and Preventing the Creation of Inauthentic Social Media Entities," *Foundation for Defense of Democracies*, October 10, 2024. (https://www.fdd.org/analysis/2024/10/10/nip-the-bots-in-the-bud)

[79] Max Lesser, "America Resilient in the Face of Aggressive Foreign Malign Influence Targeting the 2024 U.S. Elections," *Foundation for Defense of Democracies*, December 18, 2024. (https://www.fdd.org/analysis/2024/12/18/america-resilient-in-the-face-of-aggressive-foreign-malign-influence-targeting-the-2024-u-s-elections)

to adapt adversarial influence operation tactics and employ them at ethical and effective opportunities. The cognitive domain should extend not only to winning the hearts and minds of a given state's populace but also to degrade the capabilities and subvert the fortitude of an adversarial authoritarian regime. This strategy should include the full spectrum of influence operations, including cyber-enabled and physical, and should include consideration of when and how such operations are permitted against adversaries and how those operations should be combined with cyber or military operations.

Conclusion

Iran and Israel are no longer openly at war, but their multi-decade conflict in the shadows has resumed. Iranian cyber-enabled influence operations targeting Israel continue unabated and have a high probability of continuing even after the Israel-Hamas war officially ends. As Israel continues to adapt to the threat, the United States should closely monitor the lessons Jerusalem learns and share those of its own hard-won experience. All democratic nations should consider changing their strategic posture by complementing stronger defensive measures with an aggressive stance toward their adversaries in the cyber domain. With the right changes, democracies can not only compete but also thrive in the gray zone.

Appendix: Threat Indicators

The following indicators are those identified in investigations performed by the author and published by FDD or in a personal capacity and do not represent a comprehensive or exhaustive list of all indicators.

Indicator Type:	Indicator:	Operation:
X Account	x[.]com/idfleaks	IDFLeaks
Forum Profile	nulled[.]to/user/6007603-idfleaks	IDFLeaks
Forum Profile	https://leakbase[.]io/members/idfleaks.60020	IDFLeaks
Youtube Account	www.youtube[.]com/@IDFLeaks	IDFLeaks
Eitaa (Messaging)	eitaa[.]com/idfleaks	IDFLeaks
Eitaa Messaging	eitaa[.]com/nezamitarinn	IDFLeaks
Domain	idfleaks[.]info	IDFLeaks
Domain	idfinfo[.]pw	IDFLeaks
Domain	idf[.]pic	IDFLeaks
IP Address	37.143.129[.]182	IDFLeaks
IP Address	31.14.115[.]152	IDFLeaks
SSL Certificate	5f8b29c0cf898ed4f92cba7a700a1031f2a16f646b64b5c31ffda493a1aac436	IDFLeaks
SSL Certificate	D285088E8ED733F5167CE824207926BE0F418B09F9D131EC8DEB226A701E6655	IDFLeaks
Domain	wildideamarketing[.]net	IDFLeaks
Domain	digi-baman[.]com	IDFLeaks
IP Address	213.142.130[.]227	IDFLeaks
Domain	chonburiisuzu[.]com	IDFLeaks
Domain	calechedor[.]xyz	IDFLeaks
Domain	staticpanis[.]xyz	IDFLeaks

Indicator Type:	Indicator:	Operation:
Domain	servp[.]xyz	IDFLeaks
Domain	aguda90[.]co.il	IDFLeaks
Domain	viptekgroup[.]com	IDFLeaks
Telegram Channel	t[.]me/Hunt3rkill3rs1	IDFLeaks
Domain	Cybercourt[.]site	CyberCourt
Domain	Cybercourt[.]io	CyberCourt
Telegram Channel	t[.]me/cybercourt_io	CyberCourt
Telegram Channel	t[.]me/makhlab_al_nasr	CyberCourt
X Account	x[.]com/ananitv	CyberCourt
YouTube Channel	Youtube[.]com/@nethunt3r	CyberCourt
Leakbase Account	Leakbase[.]io/nethunt3r	CyberCourt
Altenens Account	altenens[.]is/members/nethunt3r/1461588	CyberCourt
XSS account	xss[.]is/members/363554	CyberCourt
Nulled Account	nulled[.]to/user/6094541-nethunt3r	CyberCourt
Cracked[.]io Account	cracked[.]io/Nethunt3r	CyberCourt
Craxpro Account	craxpro[.]io/nethunt3r	CyberCourt
Reddit Account	Reddit[.]com/u/sea-objective-7126	CyberCourt
IP Address	85.239.60[.]208	CyberCourt
IP Address	91.234.199[.]180	CyberCourt
IP Address	194.11.226[.]119	CyberCourt
IP Address	79.133.46[.]99	CyberCourt
IP Address	194.11.226[.]16	CyberCourt
SSL Certificate	50277183d5c53d98390a536689405b3828d3031a	CyberCourt
SSL Certificate	d6af0fab7c4f1c7ce73f56ea3af3eff2496a6a7e	CyberCourt
SSL Certificate	168dd25bbadac2a4c728192ebad318b3c15debc0	CyberCourt
SSL Certificate	c291064b30068d0733e6688f3638ad16fd2fcf6b	CyberCourt
SSL Certificate	338515e5d76bac69c6205ed72b5a3601b48be4ed	CyberCourt
SSL Certificate	278e63dc35e270a93c99cf2969aabd2e48d4f1b0	CyberCourt
SSL Certificate	9a1b5ce905f91cf6469097225ca2d101ba18dbf7	CyberCourt
Telegram Channel	t[.]me/anonymous_south_africa	CyberCourt
Telegram Channel	t[.]me/ALtahrea	CyberCourt
Telegram Channel	t[.]me/CyberToufanBackup	CyberCourt
Telegram Channel	t[.]me/CyberToufan	CyberCourt
Telegram Channel	t[.]me/jambiya_yemen	CyberCourt
Domain	Zeusistalking[.]com	Zeusistalking
Domain	Zeusistalking[.]net	Zeusistalking

Indicator Type:	Indicator:	Operation:
Telegram Channel	t[.]me/ze_us_is_talking4	Zeusistalking
Telegram Channel	t[.]me/ze_us_is_talking5	Zeusistalking
Telegram Channel	t[.]me/ZEUS_Is_Talking	Zeusistalking
Facebook Page	Facebook[.]com/Zeus.Is.Talking	Zeusistalking
X Account	X[.]com/ZEUS_Is_Talking	Zeusistalking
IP Address	91.222.173[.]155	Zeusistalking
IP Address	162.255.119[.]81	Zeusistalking
IP Address	213.109.147[.]63	Zeusistalking
Onion Domain	du3th2b4pvhidh5guvmb2g5hy7cepzl7wahnfnoxl7gynaxvljhhxbad[.]onion	Zeusistalking
SSL Certificate	f06126d6db98ff8cf1237f190cc0a0b0bbf26e36	Zeusistalking
Domain	rgud-group[.]com	RGUD
Domain	rgud-group[.]net	RGUD
IP Address	193.233.201[.]43	RGUD
IP Address	194.61.120[.]26	RGUD
Onion Domain	3ad7bsgkcph5qh74f6dcv6eviixb5ppbo7k3yivzd7sph7hotvfvcyad[.]onion/rgud.html	RGUD
Email Address	info@rgud-group[.]net	RGUD
Facebook Page	facebook[.]com/rg.ud0	RGUD
X Account	x[.]com/RGUD181178	RGUD
Telegram Bot	t[.]me/RGUD_bot	RGUD
Telegram Channel	t[.]me/RGUD_chanel	RGUD
TikTok Account	tiktok.com/@israel.in.a.minute	Israel In a Minute
X Account	x[.]com/israelinamin	Israel In a Minute
Linktree Account	Linktr[.]ee/israelinaminute	Israel In a Minute
Instagram Account	instagram[.]com/israelinamin1	Israel In a Minute
Facebook Account	facebook[.]com/profile.php?id=61565867583463	Israel In a Minute
YouTube Channel	https://www.youtube[.]com/channel/UC-xn7U0YfbkvtMRSZJ5n_1g	Israel In a Minute
Domain	dofek[.]tv	Dofek TV
Instagram Account	instagram[.]com/dofek_tv	Dofek TV
YouTube Channel	youtube[.]com/@TvDofek	Dofek TV
TikTok Account	tiktok[.]com/@dofektv	Dofek TV
IP Address	216.172.184[.]194	Dofek TV
SSL Certificate	5056422f9d8068365d4da3c0565ec33ebeea976a	Dofek TV
Facebook Account	Facebook[.]com/profile.php?id=61556322872538	Dofek TV
Telegram Bot	t[.]me/VIPEmployment_bot	IIS Recruitment
TikTok Account	tiktok[.]com/@vipemployment	IS Recruitment
Onion Domain	vipemp3gg44fg3j4cvbjioevtd2b3o46cyyqdck6lt3y5grhkvanw3ad[.]onion	IS Recruitment

Foundation for Defense of Democracies (FDD)

FDD is a Washington, DC-based nonpartisan research institute focusing on national security and foreign policy.

FDD's Center on Cyber and Technology Innovation

FDD's Center on Cyber and Technology Innovation (CCTI) seeks to advance U.S. prosperity and security through technology innovation while countering cyber threats that seek to diminish it. CCTI promotes a greater understanding within the U.S. government, private sector, and allied countries of the threats to and opportunities for national security presented by the rapidly expanding technological environment..

Ari Ben Am is an adjunct fellow at FDD's Center on Cyber and Technology Innovation. His research focuses on emerging threats, influence and information operations, cyber operations, and hybrid warfare. Ari is an open-source intelligence analyst by trade and the co-founder of Telemetry Data Labs, a Telegram data analytics and investigation platform.

FDD values diversity of opinion and the independent views of its scholars, fellows, and board members. The views of the author do not necessarily reflect the views of FDD, its staff, or its advisors.