THREAT ANALYSIS

Recorded Future®

By Insikt Group®

May 8, 2024

Iran-Aligned Emerald Divide Influence Campaign Evolves to Exploit Israel-Hamas Conflict

Executive Summary

Advanced influence threat actors likely aligned with Iran are conducting a persistent malign influence campaign. This campaign seeks to psychologically manipulate Israeli citizens to take real-world actions that exacerbate ideological divisions within Israeli society and undermine the Israeli government. Insikt Group tracks this influence campaign as being conducted by Emerald Divide, which overlaps with an influence operation Microsoft attributes to likely Iranian state threat actor Storm-1364; it also overlaps with online activities the Shin Bet attributes to Iran's security services.

Since 2021, Emerald Divide has demonstrated the ability to dynamically shift influence operations, activities, and objectives based on Israel's evolving political landscape, most recently seeking to exploit the ongoing Israel-Hamas conflict to sow discontent among Israeli citizens regarding the Israeli government's response to Hamas's attacks. This Emerald Divide influence campaign is ongoing, continually adopting new and innovative influence tactics and techniques, such as using digital emailing campaigns hosted on a crowdfunding platform, social media reference landing pages, and a geographic web mapping platform, as well as emerging technology such as artificial intelligence (AI)-generated deepfakes, likely increasing the campaign's ability to reach targeted audiences and drive engagement. The observed increase in advanced influence threat actors adopting and implementing AI will likely continue to improve over time with advances in technology and repetition of operational employment, likely increasing the overall effectiveness of influence operations to achieve behavioral change in line with a specific objective.

Emerald Divide has consistently used a robust influence infrastructure consisting of over sixteen social media accounts appealing to specific and sometimes conflicting target audiences, thereby playing both sides of contentious socio-political debates and provoking division. Currently, the campaign continues to actively use seven primary social media accounts and a large coordinated inauthentic behavior (CIB) network on social media, demonstrating this campaign's ability to avoid account and network takedowns.

Emerald Divide has likely succeeded in influencing its target audience to engage in specific and observable physical actions, such as purportedly displaying posters and actively participating in anti-government protests, thereby using the information environment to achieve physical results. The campaign has also demonstrated the capability to harvest personally identifiable information (PII) as well as dox Israeli officials. Following Hamas's October 7, 2023, attacks against Israel, Emerald Divide has increased its overall aggressiveness in both stylistic content as well as the nature of its online engagements. Emerald Divide will continue to be a security threat and will likely adapt its approach based on targets of opportunity that present competing opinions within Israeli society, such as, in the near term, the Israeli government's handling of the ongoing hostage crisis, and, in the medium to long term, Israel's next legislative election, which is scheduled to take place in October 2026.

As Emerald Divide persists, collaboration between government, technology companies, and security research organizations to track, monitor, and disrupt this influence network and its associated threat

actors will likely reduce the campaign's effectiveness in its current form. However, the campaign's demonstrated ability to replicate and advance operational tradecraft using new infrastructure suggests the potential to persist in the long term. Additionally, public awareness of this campaign and its corresponding infrastructure will likely reduce the risk of unwitting online users engaging with and subsequently being influenced by the network. Executives and public figures being aware of this campaign will likely mitigate any potential negative impact on personal and organizational brand reputation, as awareness allows them to actively avoid any interaction with this network, including inadvertently providing passive support, such as access to online infrastructure.

Key Findings

- Insikt Group continues to track Emerald Divide as it employs at least seven primary social media accounts and a CIB network of over 250 accounts.
- Emerald Divide continues to demonstrate the ability to dynamically shift influence operations, activities, and objectives based on Israel's evolving political landscape, most recently seeking to exploit the ongoing Israel-Hamas conflict.
- The network has adopted innovative influence tactics, techniques, and procedures (TTPs), such as using a social media reference landing page, Linktree; digital emailing campaigns on the crowdfunding platform Drove; the geographic web mapping platform Google Maps; Google documents; and QR codes.
- Emerald Divide will likely continue to use generative AI to produce influential and deceptive content based on its historical use of deepfake videos impersonating political and religious leaders, which received significant online engagement.
- The network demonstrates the ability to influence and persuade its target audience to take specific physical actions, such as providing information or displaying posters, likely emboldening influence threat actors to replicate and advance similar operational tradecraft in the future.

Background

Advanced influence threat actors likely aligned with Iran continue to conduct a persistent malign influence campaign that began in 2021. This campaign seeks to psychologically manipulate Israeli citizens to increase ideological division on social and political issues. Conducted by Emerald Divide, it has demonstrated the ability to dynamically shift influence efforts and objectives based on Israel's evolving political landscape by rapidly changing and developing new infrastructure and TTPs. Since October 2023, the campaign has transformed its focus to the Israel-Hamas conflict to sow distrust and discontent regarding the Israeli government's response to Hamas's attacks against Israel.

On February 7, 2024, Microsoft attributed activity observed in the most recent campaign operation to influence threat actor Storm-1364, which Microsoft assesses as a likely Iranian state threat actor and which Insikt Group tracks as Emerald Divide. Microsoft's findings are also consistent with the Israel Security Agency (or "Shin Bet") attributing specific social media accounts discussed in this report to Iranian state influence operations targeting Israel.

Additionally, on December 20, 2023, Haaretz Daily Newspaper published an article detailing a two-year-long malign influence campaign targeting Israeli citizens to increase social and political polarization within Israeli society. According to Haaretz, details of the ongoing influence campaign were provided by researchers from Israel-based "disinformation watchdog group" FakeReporter. These Haaretz and FakeReporter findings are also consistent with the Shin Bet's June 2023 disclosure that "Iranian influence activity on social media in Israel … [seeks] to exacerbate the social and political rifts in Israel over the entire political spectrum". In late June 2023, the Shin Bet informed Israeli media outlets of the agency's ongoing "overt and covert activities", referencing its efforts to disrupt the reported Iranian influence activity. Insikt Group notes that the Shin Bet previously voiced concern regarding inauthentic social media accounts attributed to Iran attempting to increase polarization by targeting Israel's political wedge issues during the country's 2022 parliamentary elections. In August 2022, the agency warned that Russia and Iran may amplify polarizing rhetoric and false information to increase social unrest.

Analysis of the Influence Campaign

Insikt Group determined that the current Emerald Divide campaign has three sequential influence operations, each with specific influence objectives and corresponding malign narratives targeting Israeli citizens. This report arranges these influence operations chronologically, from campaign initiation in 2021 to ongoing activity observed up to February 2024. It also breaks down each included influence operation by corresponding narrative, audience, infrastructure, and capabilities.[1] Operation three remains ongoing at the time of writing. The three influence operations' respective objectives in support of the overarching campaign are summarized below:

[1] Throughout this investigation, we used Recorded Future's Diamond Model for Influence Operations, Atlantic Council's SCOTCH Framework, and the Disinformation Analysis and Risk Management (DISARM) Foundation's Red Team and Blue Team Frameworks to identify and summarize the predominant malign influence narratives targeting Israel's domestic population.

- **Operation one influence objective:** increase social conflict between Israel's "ultra-Orthodox" religious groups and Israel's LGBTQ+ community
- **Operation two influence objective:** incite social unrest by pivoting individuals on the left and right of Israel's political spectrum against each other
- **Operation three influence objective:** sow discontent among Israeli citizens regarding the Israeli government's response to Hamas's attacks against Israel

Due to the nature and scope of influence operations, especially covert operations, all numeric values associated with these activities, such as social media posts, likes, shares, and other impressions, remain approximate and ongoing. This report outlines each operation analyzed below with an introduction of the corresponding influence objective, a summary of the narrative and target audience, and a technical analysis of the infrastructure threat actors used and capabilities they demonstrated during the operation. Comprehensive lists of influence operations capabilities observed and demonstrated in each operation are provided in **Appendix A** using Recorded Future's Diamond Model for Influence Operations.

Operation One Influence Objective: Increase Social Conflict Between Israel's "Ultra-Orthodox" Religious Groups and Israel's LGBTQ+ Community

Based on reporting by Haaretz Daily Newspaper, FakeReporter, and the Shin Bet, Emerald Divide's influence campaign began its operations in 2021 with the establishment of multiple social media accounts seeking to increase social conflict between Israel's "ultra-Orthodox" religious groups and Israel's LGBTQ+ community. Emerald Divide used wide-ranging influence TTPs in an attempt to pivot these groups against each other by fabricating and manipulating online content about issues specific to religious and LGBTQ+ communities.

As an example, Emerald Divide developed inauthentic online personas with generative AI to impersonate Israeli rabbis, using the inauthentic accounts to disseminate online content expressing negative sentiment toward the LGBTQ+ community. Simultaneously, Emerald Divide then used additional inauthentic social media accounts aligned with the LGBTQ+ community to criticize the content originally disseminated by the inauthentic rabbis. By creating inauthentic accounts aligned with both communities, Emerald Divide sought to manufacture an online echo chamber capable of inciting social conflict between Israel's ultra-Orthodox religious groups and its LGBTQ+ community.

Narrative and Audience

Narratives in support of this influence objective included inflammatory arguments opposing ideological aspects of groups aligned with ultra-Orthodox beliefs and groups in support of LGBTQ+ rights. This first influence operation had two primary target audiences: Israelis who align ideologically with ultra-Orthodox religious views and Israelis who support the LGBTQ+ community. Throughout this operation, the campaign attempted to pivot these two audiences against each other through various efforts, such as manufacturing a social movement titled "movement to stop the ultra-Orthodox" and a

YouTube channel hosting deepfake videos of Israeli Rabbi Shlomo Moshe Amar condemning LGBTQ+ rights.

Infrastructure and Capabilities

Infrastructure used throughout the first operation of this campaign included social media accounts, primarily on Instagram, Telegram, TikTok, YouTube, and another mainstream social media platform. The development of infrastructure to support this operation surged in 2022 and then culminated in 2023, with three Telegram channels persisting to support the second operation of this campaign. Trends observed during this operation include a shift in the social media platforms being used from primarily Instagram and another mainstream social media platform to Telegram.

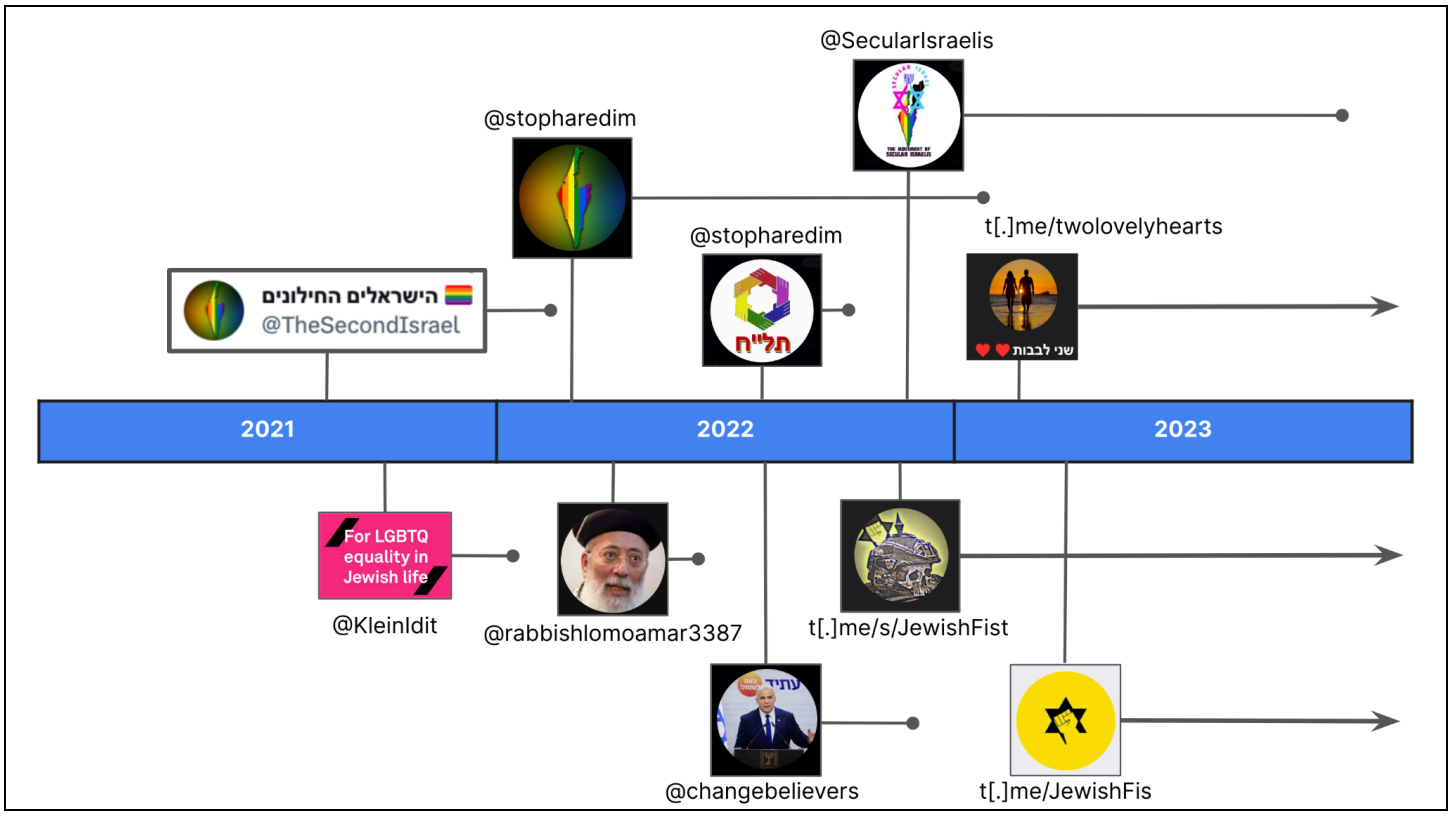


Figure 1: *Timeline of accounts operationalized throughout the first operation of this campaign (Source: Recorded Future)*

In August 2021, the account "הישראלים החילונים 🏳️‍🌈" (@TheSecondIsrael) was created and began reposting content related to the LGBTQ+ community (DISARM Technique T0007: Create Inauthentic Social Media Pages and Groups). From September 2021 through October 2021, the account increased the number of posts featuring original content expressing positive sentiment around issues related to the LGBTQ+ community and posts expressing negative sentiment toward individuals with Orthodox religious views. Notably, in February 2022, the @TheSecondIsrael account posted a video showing what is described as a "second Israel map" posted in Rabin Square, located in Tel Aviv, Israel. This is the first identified instance of Emerald Divide's campaign purportedly persuading individuals to physically

display influential posters, an influence technique that was attempted multiple times throughout this campaign (DISARM Technique T0057.002: Conduct Symbolic Action).

Figure 2: *Screenshot of the "second Israel map" posted in Rabin Square (Source: Mainstream Social Media)*

In October 2021 — two months following the creation of the @TheSecondIsrael account — an account, "Idit Klein" @KleinIdit, was created to impersonate the president of a legitimate LGBTQ+ advocacy group (DISARM Technique T0099: Prepare Assets Impersonating Legitimate Entities). The @KleinIdit inauthentic account consistently reposted content published by the @TheSecondIsrael account to include the aforementioned "second Israel map". Other social media accounts observed posting @TheSecondIsrael content, such as accounts "Fatma Sam" (@FatmaSam9) — notably, this account has posted content involving United States (US) politics — and "Emily Pearl" (@EmilyPearlUS), are assessed to likely be inauthentic based on the date of account creation, duration of observed activity matching that of the @TheSecondIsrael account, and frequency of reposting @TheSecondIsrael account content (DISARM Technique T0090: Create Inauthentic Accounts). Both accounts have been inactive since December 2021, though they remain operational with their account locations listed in the US.

In March 2022, the Instagram account "stopharedim" was created and featured the same profile picture as the @TheSecondIsrael account. The "stopharedim" account posted similar and often identical content as the @TheSecondIsrael account about issues related to the LGBTQ+ community and negative sentiment toward individuals with Orthodox religious views. A notable example of cross-posting content includes a post by the "stopharedim" account featuring the same aforementioned "second Israel map" video, posted ten months after the video was originally posted on a mainstream social media platform (DISARM Technique T0119: Cross-Posting).

Three months after the creation of the "stopharedim" Instagram account, in June 2022, the account "תל"ח" (@stopharedim) was created, featuring similar content; however, it gained negligible online engagement with only two followers. In the same month, the Instagram account "changebelievers" was created, featuring thematically similar content to both the @TheSecondIsrael and "stopharedim" Instagram accounts and receiving relatively low online engagement with 35 followers. An example post provided below demonstrates the intention to pivot different communities against each other. Notably, the post provides a "source" that resolves to an article published by Haaretz, demonstrating an attempt by the influence threat actor to reframe the article's context for psychological effect (DISARM Technique T0023.001: Reframe Context). All three accounts described above have stopped posting content, though they remain operational.

Figure 3: *Screenshot of a post by "changebelievers" attempting to incite social conflict (Source: Instagram)*

Concurrently, in April 2022, the YouTube channel "Rabbi Shlomo Amar" (@rabbishlomoamar3387) was created. This channel features eight videos depicting Rabbi Shlomo Amar, two of which are almost certainly AI-generated deepfakes, as later reported by Haaretz in 2023 (DISARM Technique T0087.001: Develop AI-Generated Videos [Deepfakes]). The videos include sermons and commentary expressing negative sentiment toward LGBTQ+ rights. This activity represents the first of multiple identified instances in this campaign of using AI-generated content to impersonate a key leader to deceive the respective audience. An additional attempt to impersonate a well-known individual occurred in July 2022 with the creation of an account, "Noam Cohen" (@Real_NoamCohen), and a corresponding

Telegram account, *t[.]me/RealNoamCohen*. The @Real_NoamCohen account includes a hyperlink to the inauthentic website "Jewish Guardian of the Torah Movement" (JGTM; *jgtm[.]org*), which is currently offline (DISARM Technique T0013: Create Inauthentic Websites). According to Haaretz, the campaign used the *jgtm[.]org* website to publish pro-Orthodox content.

During September 2022, the Telegram channel "Boxing - Gush Katif - Returning Home" (אגרוף - גוש קטיף-חוזרים הביתה; *t[.]me/s/JewishFist*) — attributed by the Shin Bet to Iran's security services — began posting content that was generally supportive of Israel and focused on national security issues such as Israeli military operations, terrorist arrests, and weapon seizures. A limited number of posts also included derogatory comments and themes directed toward the LGBTQ+ community. The Telegram channel "אגרוף" (Fist; *t[.]me/JewishFistt*), almost certainly a backup account for *t[.]me/s/JewishFist*, began posting identical content in January 2023. Both Telegram channels have persisted throughout each operation in this campaign and remain active, with *t[.]me/s/JewishFist* having 4,980 subscribers. Following Hamas's attacks against Israel on October 7, 2023, both channels increased the frequency of their posts, shifting content focus to the ongoing conflict as well as sharing threats from Hamas and Hezbollah, which are further analyzed in the third operation of this campaign.

In November 2022, the account "ישראל השנייה" (@SecularIsraelis) was created, gaining 815 followers, as well as the TikTok account "ישראל השנייה" (@secularisrael), gaining only nine followers and 103 likes. Both accounts posted similar content as the @TheSecondIsrael account about issues related to the LGBTQ+ community and negative sentiment toward individuals with Orthodox religious views. Two months later, in January 2023, the Telegram channel "Second Israel" (ישראל השנייה; *t[.]me/s/IsraeltheSecond*), which has a similar name to the aforementioned @TheSecondIsrael social media account, was created. Second Israel's profile states: "standing against extremism, fanaticism, racism is our mission. Be our voice!" A second Telegram channel was also identified mirroring the Telegram channel Second Israel; however, it includes a "2" at the end of the account name (*t[.]me/IsraeltheSecond2*), almost certainly representing that this is a backup account in the scenario of an account takedown.

The almost certain backup account *t[.]me/IsraeltheSecond2* has 113 members, including Telegram user "Sarah Efron" (@SarahEfron5), who matches the persona identified by Fakereporter associated with attempts to direct message Israeli activists to deliver posters for use in anti-government protests. The Sarah Efron persona was identified as a member of multiple social media accounts throughout the operations of this campaign, suggesting this persona is almost certainly an inauthentic account operated by Emerald Divide influence threat actors (DISARM Technique T0097: Create Personas).

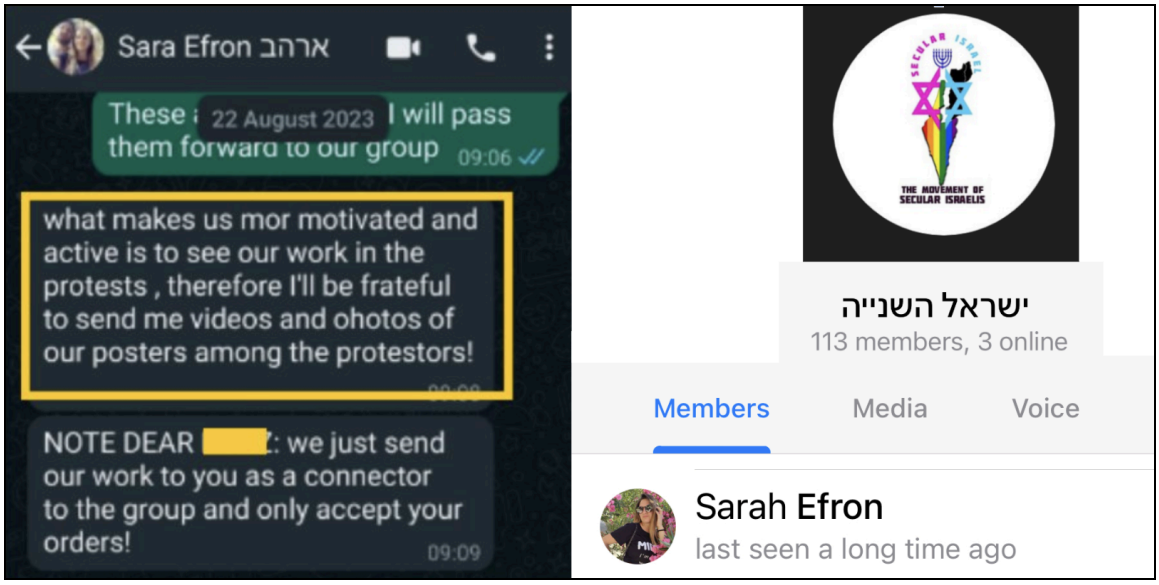


Figure 4: *(Left) Screenshot provided by Fakereporter of persona "Sarah Efron" direct messaging Israeli activists; (Right) screenshot of Telegram account @SarahEfron5, who is a member of t[.]me/IsraeltheSecond2 (Source: Fakereporter, Telegram)*

The final Telegram channel established during this operation in February 2023 was the channel "Two Hearts" (שני לבבות; *t[.]me/twolovelyhearts*). The channel resembles a platform used for Israelis interested in romantic relationships; however, it also posted content initially supporting the LGBTQ+ community and then shifted focus around March 2023 to Israeli politics, specifically criticizing Prime Minister Netanyahu. This activity almost certainly corresponds to an overarching shift of the campaign in February 2023 to the second operation analyzed in the next section of this report. The channel features cross-posted content from the previously described Telegram channel, "Second Israel", and the persona Sarah Efron is among its visible members. The channel has 207 members and remains active, with posts soliciting contact to arrange romantic engagements and posts offering various personal documents for sale, such as driver's licenses, college certificates, weapons licenses, and medical documents. Similar to previously mentioned accounts, content posted on this channel includes almost certainly AI-generated images expressing negative sentiment toward Prime Minister Netanyahu, suggesting regular use of AI across the network to produce content.

Figure 5: *(Left) Screenshot of "Two Hearts" dating channel; (Right) screenshot of political post in the "Two Hearts" dating channel (Source: Telegram[2])*

Operation Two Influence Objective: Incite Social Unrest by Pitting Individuals on the Left and Right of Israel's Political Spectrum Against Each Other

Based on content analysis, Emerald Divide's influence campaign shifted focus around February 2023 from directly targeting Israel's Orthodox religious groups and LGBTQ+ community to attempting to incite conflict among Israelis on both the left and right sides of Israel's political spectrum to increase social unrest. This operation of the campaign centered primarily around three social media accounts identified as "No Voice" (אין כל), "The Hunters" (הציידים), and "Traitors' Trial" (משפט בוגדים), which Microsoft attributed to influence threat actor Storm-1364, which is also described by Microsoft as a likely Iranian state threat actor. All three accounts focused online activity around judicial reforms proposed by Prime Minister Netanyahu and then on Israel's 2023 elections. Compared to operation one, Emerald Divide increased its aggressiveness in both stylistic content produced by the network and the nature of its online engagements.

Narrative and Audience

Narratives amplified throughout this operation centered around social discontentment with — at that time — proposed judicial reforms spearheaded by Prime Minister Netanyahu and, subsequently, with allegations surrounding Israel's 2023 elections that the reforms were part of an attempted coup d'etat.[3] Central to this second operation of the influence campaign were attempts to persuade Israeli citizens to take specific, physical actions, ranging from displaying posters to actively participating in anti-government protests. Similar to the first operation, this operation involved two primary target

[2] *https://t[.]me/twolovelyhearts*
[3] *https://t[.]me/isnotvoice/17*

audiences: Israelis ideologically aligned with what is broadly characterized as the "left" and "right" sides of Israel's political spectrum.

Infrastructure and Capabilities

The infrastructure used throughout the campaign's second operation focused primarily on Telegram and WhatsApp. Infrastructure development in support of this operation occurred in early 2023 while also using infrastructure established during the previous operation, shifting content focus to support the updated influence objective. Trends observed during this operation include using Telegram channels and the social media reference landing page Linktree to direct online users to other platforms, such as WhatsApp and Google Documents, for more direct engagement. The graphic below indicates the dates on which specific accounts were operationalized, including account creation, last observed activity, and accounts that persisted beyond the end of this operation.

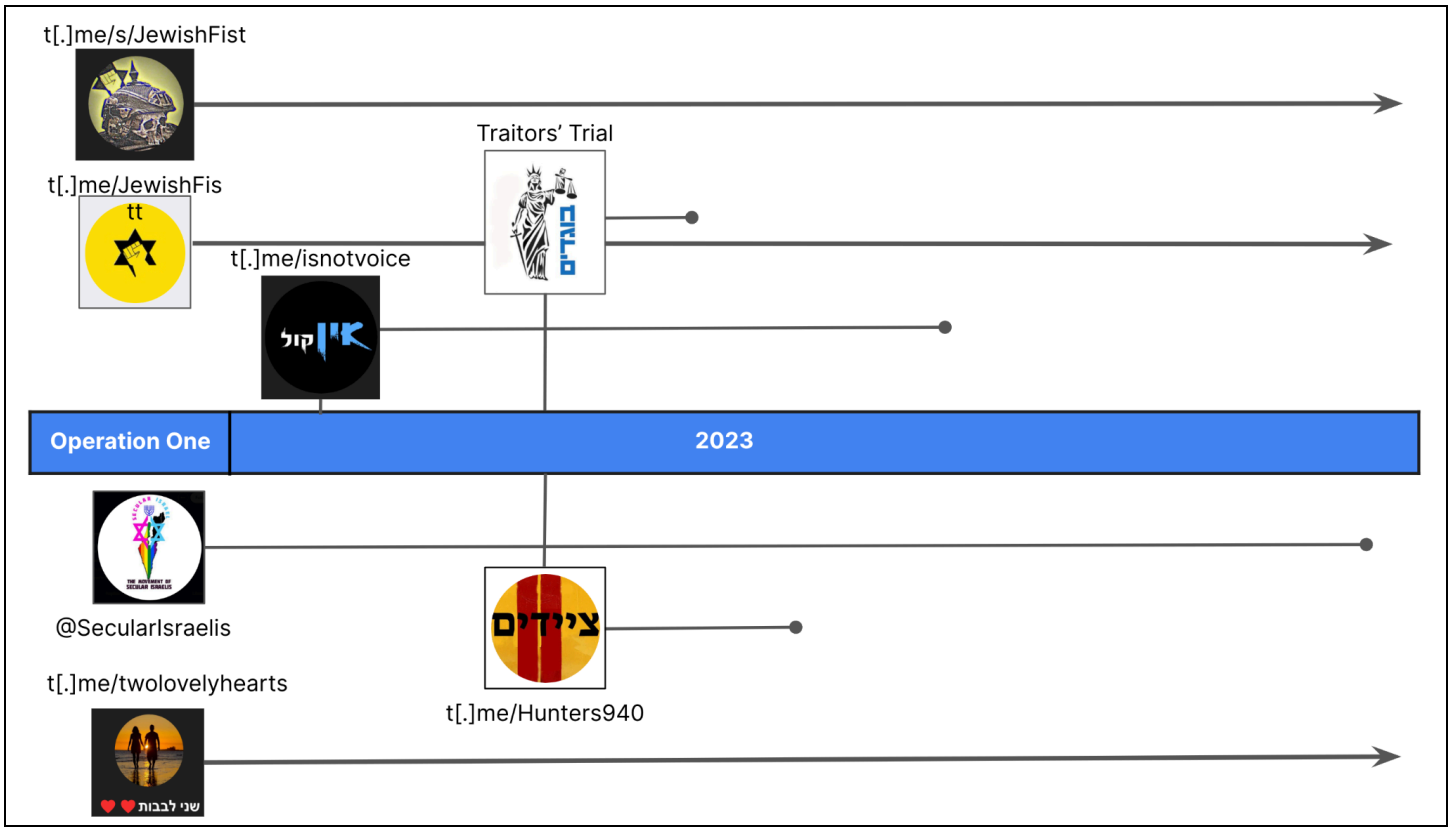


Figure 6: *Timeline of accounts operationalized throughout this operation (Source: Recorded Future)*

In February 2023, the Telegram channel "No Voice" (אין כל; *t[.]me/isnotvoice*) began posting content that actively rejected proposed judicial reforms and supported left-leaning political demonstrations. No Voice shared information about protests, attempting to persuade members of the group to take physical actions, such as posting signs (DISARM Tactic TA10: Drive Offline Activity). The No Voice Telegram channel included a hyperlink to a Linktree landing page that provided additional links to Telegram,

Whatsapp, Facebook, and a Google document (DISARM Technique T0122: Direct Users to Alternative Platforms).

Translated from Hebrew, the Google document stated: "Protests are expanding and continue to grow and we need new partners! Want to cooperate for a better future of the country? Please fill out the form". The document goes on to provide questions soliciting PII (as exemplified in **Figure 7** below), such as full name, phone number, mailing address, physical address, and other specific requests for information, like, "do you have any special skills that you can harness for protest activity" and "the amount [likely referring to monetary compensation] required for cooperation". Notably, under the "special skills" question, the document provides a list of 25 box-check options that included various skills, such as, "graffiti", "delivery", "hovercraft" — likely referring to drones or unmanned aerial vehicles (UAVs) — "communication", "fundraising", "website management", "video editing", "graphic design", and "use of social networks". Based on the information it requested, this Google document is likely a tool Emerald Divide used to recruit individuals to participate in activities supporting the influence campaign, specifically activities related to anti-government protests.

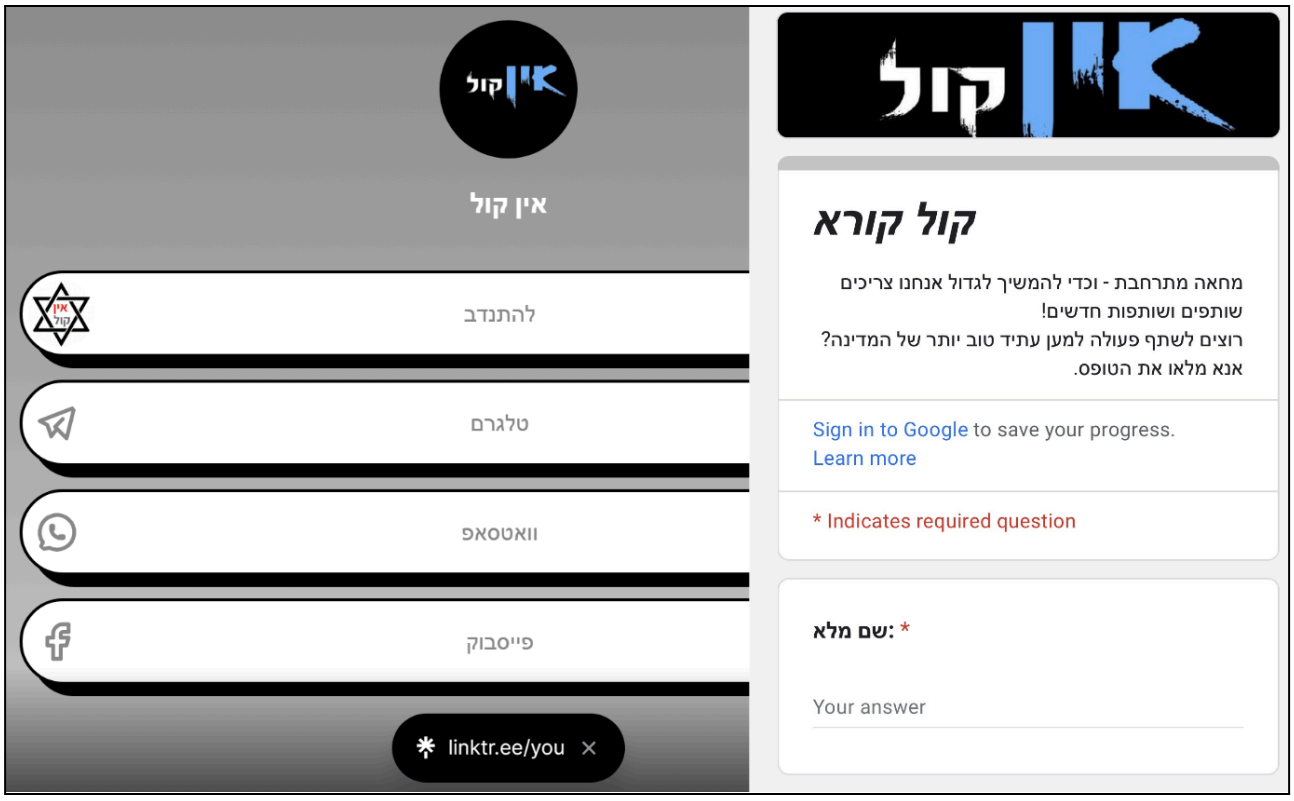


Figure 7: *(Left) Screenshot of No Voice Linktree; (Right) Screenshot of No Voice Google document soliciting PII (Source: Telegram[4])*

According to FakeReporter, the No Voice social media account maintained a presence on a popular US social media platform, promoting the hashtags #novoice and #democracy until the account was

[4] *https://t[.]me/isnotvoice*

suspended in March 2023 (DISARM Technique T0104.006: Create Dedicated Hashtag). According to Haaretz, No Voice also maintained an Instagram account and Facebook group, both of which were suspended in June 2023. The No Voice Telegram channel (*t[.]me/isnotvoice*) has not posted content since July 2023; however, it remains operational, with 776 subscribers. FakeReporter researchers noted that the "No Voice" Instagram page originally listed its location as Iran. Additionally, content analysis conducted by Insikt Group identified posts with direct references to Iran, such as a video using AI-generated voice-overs and fictitious depictions of Israel in 2043 that includes video footage of the flag of the Islamic Revolutionary Guard Corps (IRGC) and what is very likely the IRGC Navy conducting drills, as shown in **Figure 8**.

Figure 8: *Screenshot of a video depicting the IRGC flag (Source: Telegram[5])*

In May 2023, the Telegram channel "The Hunters" (הציידים; *t[.]me/Hunters940*) began posting content that actively supported proposed judicial reforms and corresponding right-leaning political demonstrations. The Hunters primarily used WhatsApp and, according to FakeReporter researchers, actively attempted to infiltrate social groups affiliated with the major right-leaning political party National Liberal Party, commonly referred to as the Likud Party (DISARM Technique T0043.001: Use Encrypted Chat Apps). Multiple posts on The Hunters telegram channel include hyperlinks to a corresponding WhatsApp group invitation (screenshot provided in **Figure 9**), which is almost certainly an attempt to drive online traffic to WhatsApp for further direct engagement. The Hunters Telegram channel (*t[.]me/Hunters940*) has also not posted content since July 2023; however, it remains operational, with 207 subscribers.

[5] *https://t[.]me/isnotvoice*

Figure 9: *Screenshot of The Hunters WhatsApp group invitation (Source: WhatsApp[6])*

According to Haaretz, the social media account "Traitors' Trial" (משפט בוגדים) became active at the same time as "The Hunters" account. It posted the personal details of Israeli law enforcement individuals involved in political demonstrations on social media, exposing their identities in a malicious activity commonly referred to as doxing (DISARM Technique T0048.004: Dox). FakeReporter researchers identified "Traitors' Trial" operating on Telegram and an additional popular social media platform. It also operated on Drove, an Israeli digital media platform that describes itself as a "technological crowdfunding platform that focuses on performance and high conversion rate to maximize ROI" (DISARM Technique T0017: Conduct Fundraising). Notably, the use of Drove to conduct online email campaigns was identified in more than one instance throughout this campaign and is further analyzed in the third operation of this campaign. According to Haaretz, Telegram has suspended the "Traitors' Trial" channel.

Operation Three Influence Objective: Sow Discontent Among Israeli Citizens Regarding the Israeli Government's Response to Hamas's Attacks

Following Hamas's attack on Israel on October 7, 2023, and the ensuing conflict, Emerald Divide's influence campaign shifted focus once again, targeting Israeli citizens' trust and confidence in their government's response to Hamas's attacks against Israel. During the month of October 2023, multiple social media accounts were rapidly developed with the objective of sowing distrust and discontent among Israelis' views of their government's role and response to the attacks. This operation of the campaign remains ongoing and includes a large-scale CIB network actively persisting on at least one mainstream social media platform, demonstrating robust influence infrastructure. Additionally, consistent with operation two, this operation has demonstrated the ability to solicit PII, likely

[6] *https://chat[.]whatsapp[.]com/L3V34t0fPUyLIqUvTr1sYG*

representing a persistent technique of using Google documents to recruit individuals to participate in activities supporting the influence campaign.

Narrative and Audience

Narratives amplified throughout this operation include attempts to frame key leaders within the Israeli government as being responsible for the October 7, 2023, attacks, as well as allegations that certain members of the government had prior knowledge of Hamas's attack plans and chose to remain silent in a deliberate act of betrayal.[7] Additionally, this third operation promoted narratives of consolation, grieving, and retribution, seeking to psychologically manipulate hostage victims' family members into taking specific actions, such as initiating gatherings near the families' homes.[8] This operation's assessed target audience is, broadly, the Israeli citizenry to undermine their trust and confidence in the Israeli government.

Infrastructure and Capabilities

The infrastructure used throughout this operation focused primarily on Telegram and Instagram. Infrastructure development in support of this operation occurred shortly following Hamas's attacks on October 7, 2023, while also using infrastructure established during the previous operation, shifting content focus to support the updated influence objective. Trends observed during this operation include using CIB networks to facilitate online engagement and continuous attempts to orchestrate anti-government protests. The graphic below indicates the dates on which specific accounts were operationalized, including account creation, last observed activity, and accounts that persist.

[7] *https://t[.]me/twolovelyhearts/6616*
[8] *https://t[.]me/BringHomeNow/337*

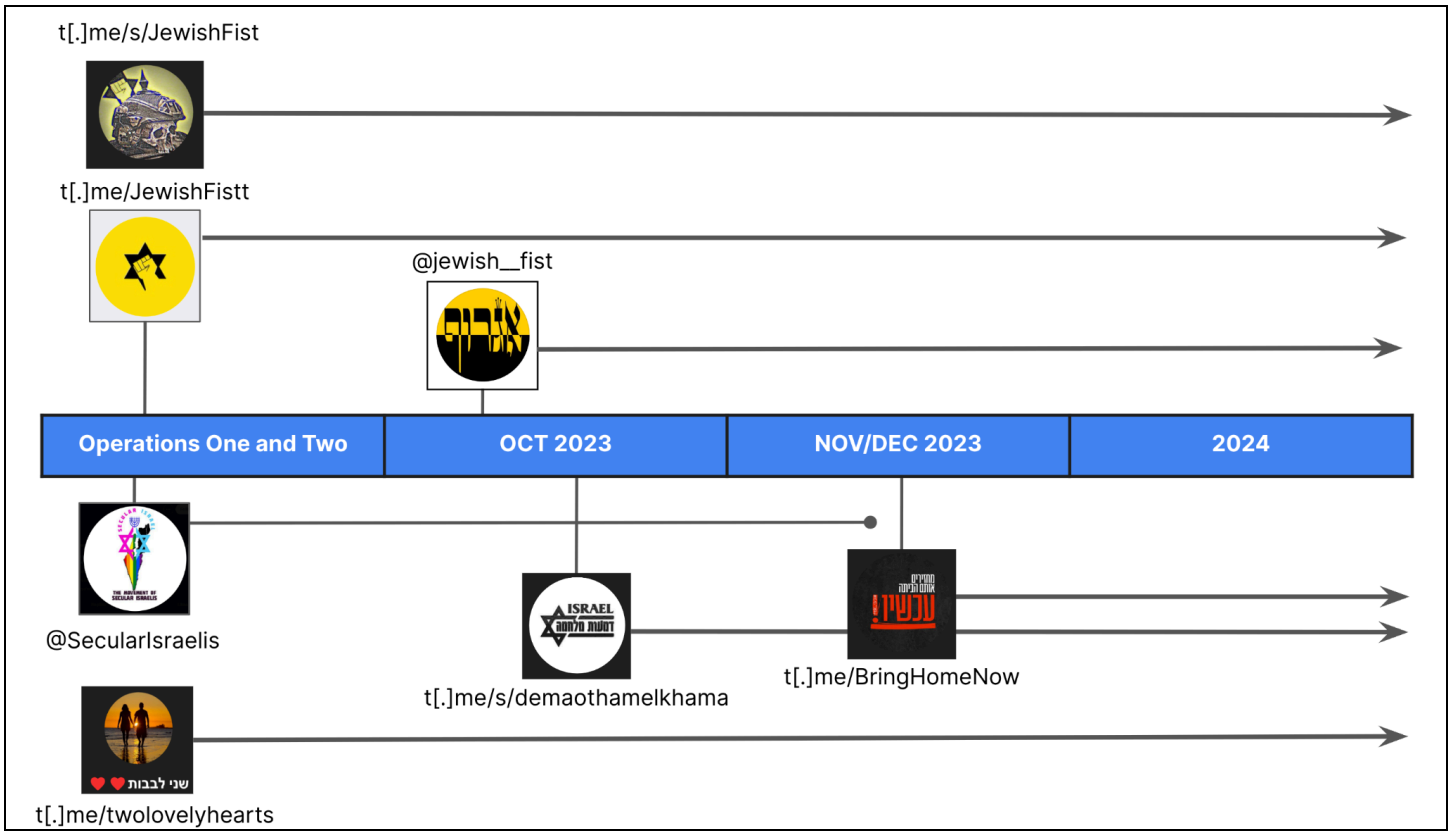


Figure 10: *Timeline of accounts operationalized throughout this operation (Source: Recorded Future)*

Following the October 7, 2023, attacks, previously analyzed Telegram channels "Second Israel" and "Two Hearts" (established during this campaign's first operation) immediately shifted thematic content to focus on the emerging conflict, posting identical images on each account criticizing Prime Minister Netanyahu and suggesting he was to blame for the attacks (DISARM Technique T0082: Develop New Narratives).[9] [10] Other posts promoted calls to action for Israelis to protest against their government as a response to its alleged failure to prevent the Hamas attacks. Example content, which was posted on each platform in the days following the October 7, 2023, attacks, is provided below. Notably, the image on the right includes a caption comparing Prime Minister Netanyahu to a virus, claiming he weakened the "immune system of Israel", thus enabling its enemies to attack.

[9] *https://t[.]me/twolovelyhearts/6778*
[10] *https://t[.]me/IsraeltheSecond/233*

Figure 11: *(Left) Screenshot of a post on both Telegram channels "Second Israel" and "Two Hearts" on October 11, 2023; (Right) Screenshot of a post on both Telegram channels "Second Israel" and "Two Hearts" comparing Netanyahu to a virus (Source: Telegram[11] [12])*

Additionally, Telegram channel "Boxing - Gush Katif - Returning Home" (*t[.]me/s/JewishFist*) — previously established during this campaign's first operation — immediately shifted content focus to the Israel-Hamas conflict, drastically increasing the frequency of its posts per day.[13] [14] Other similar social media accounts on other platforms were also created after the attacks — now hyperlinked in the *t[.]me/s/JewishFist* account profile — such as the Instagram account "אגרוף" (@jewish_fist) and TikTok account "jewishfist" (@jewishfist), which this report further analyzes below.

Content published by the "Boxing - Gush Katif - Returning Home" (*t[.]me/s/JewishFist*) channel, as well as the assessed backup channel "אגרוף" (Fist; *t.me/JewishFistt*), continue to portray a pro-Israel stance; however, its posts also include graphics and videos of Hamas and Hezbollah propaganda threatening Israelis. Notably, some posts also include references to Iran, as featured in **Figure 12**. One post made on December 22, 2023 (**Figure 12** [left]) alludes to the possibility of Iranian arms shipments to the Palestinian National Authority (PA), with Arabic text on the image that translates to "the moment of truth and struggle", with the post itself questioning, "is Iran arming the Palestinian Authority? Is Israel again falling asleep on guard?" Another post on January 9, 2024 — one day after an Israeli airstrike that killed Hezbollah senior commander Wissam Al Tawil — features former IRGC-Quds Force (IRGC-QF) Commander Qassem Soleimani (**Figure 13**). Similar to other posts featuring Hamas and Hezbollah propaganda threatening Israelis, these posts about Iranian arms shipments to the PA and pictures of Soleimani are likely attempts by the influence threat actors to subtly threaten the target audience.

[11] *t[.]me/s/IsraeltheSecond*
[12] *t[.]me/twolovelyhearts*
[13] *https://t[.]me/JewishFist/1775*
[14] *https://t[.]me/JewishFist/1768*

Figure 12: *(Left) Screenshot of a December 22, 2023, post on t[.]me/JewishFistt alluding to possible arms shipments from Iran to the PA; (Right) Screenshot of a February 5, 2024, post on t.me/JewishFistt stating "the lions of the occupied inside will not sleep in their revenge" (Source: Telegram[15] [16])*

Figure 13: *Screenshot of January 9, 2024, post on t[.]me/s/JewishFist featuring Soleimani (Source: Telegram[17])*

Following October 2023, the "אגרוף" (Fist; *t.me/JewishFistt*) backup channel — previously established in the first operation — began posting almost certainly AI-generated graphics that were not featured on the original *t[.]me/s/JewishFist* channel. Many of the graphics included culturally derogatory themes

[15] *https://t[.]me/JewishFistt/5968*
[16] *https://t[.]me/JewishFistt/8165*
[17] *https://t[.]me/s/JewishFist*

graphically depicting Hamas fighters and other individuals as rats and pigs (DISARM Technique T0131.002: Post Borderline Content).[18] [19]

In October 2023, the Instagram account "אגרוף" (@jewish__fist) — also attributed by the Shin Bet to Iran's security services — was created and remains active with 792 followers. The account hosts content about the Israel-Hamas war that is generally pro-Israel and includes commemorative references to Israelis who have been killed in the conflict. At the time of writing, Insikt Group assesses that at least 250 of the 792 Instagram accounts following the @jewish__fist Instagram account are almost certainly inauthentic (DISARM Technique T0092.002: Use Follow Trains). This assessment is based on account characteristics such as the time of registration, the use of likely AI-enabled profile pictures, stolen profile pictures from authentic accounts, low number of online engagements, and irregularities in profile usernames. This activity suggests a large network of inauthentic accounts that is very likely engaged in CIB to support this ongoing operation.[20]

Based on a sample of 250 Instagram accounts following the @jewish__fist Instagram account, 72 of the accounts have a date of registration in November 2023 and 171 in December 2023. These registration dates indicate that roughly 97% of the 250 selected accounts were created after the @jewish__fist Instagram account was created in October 2023, corresponding to the onset of the Israel-Hamas conflict.

Month	Oct. 2023	Nov. 2023	Dec. 2023	Jan. 2024
Total number of new account registrations	6	72	171	1

Additional irregularities are present in the naming conventions for most of the 250 analyzed accounts, such as generic account names that do not match any element of the corresponding username and which are generally common one-word first names in the English language. Out of the 250 accounts analyzed, the names Colton, Jackson, Preston, Hazel, and Landon were each used as account names for eight different accounts, respectively. Other names were also used multiple times for different accounts, as visualized in **Figure 14**.

[18] *https://t[.]me/JewishFistt/8391*
[19] *https://t[.]me/JewishFistt/8056*
[20] *https://www.instagram[.]com/jewish__fist*

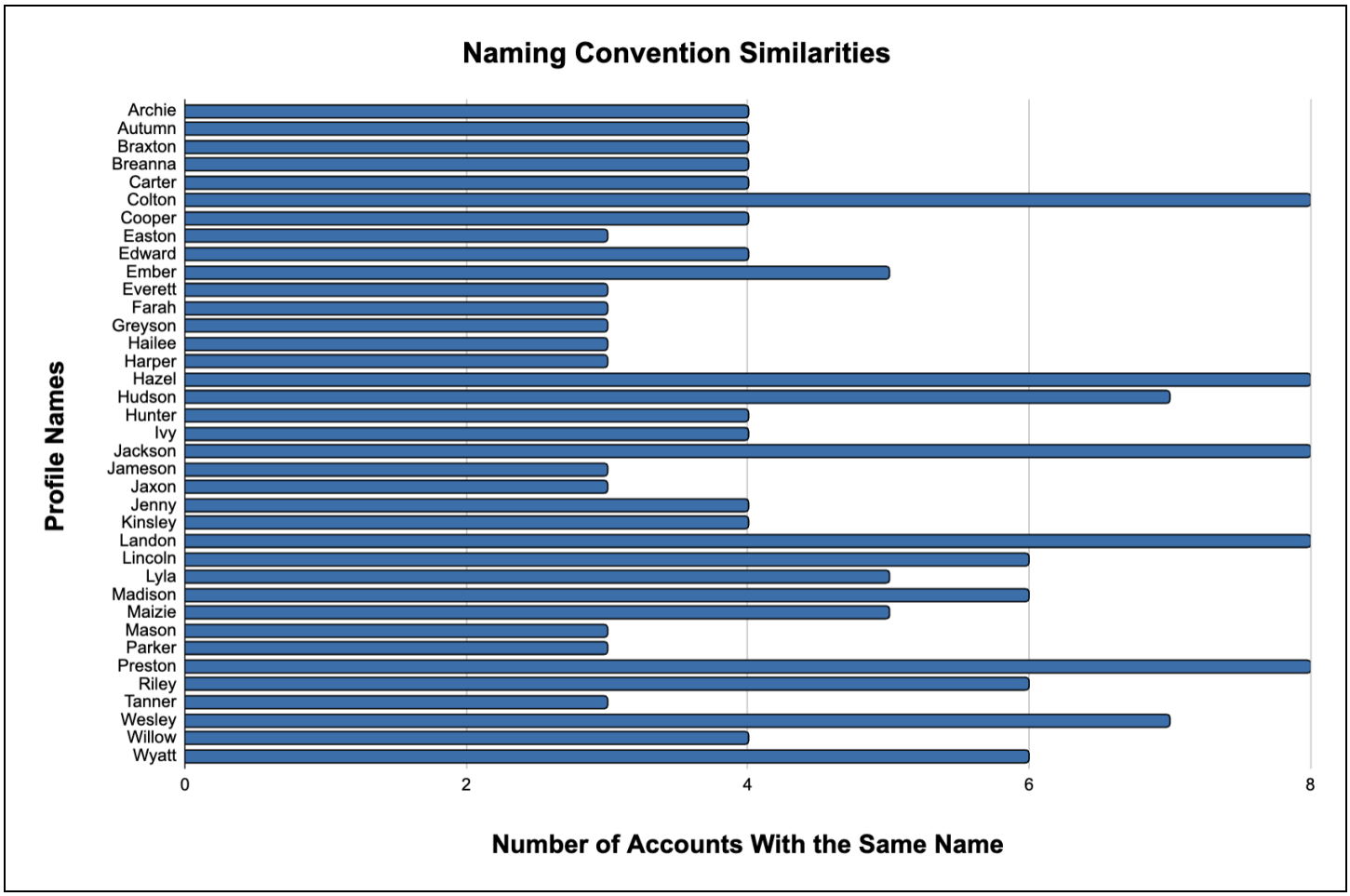


Figure 14: *Naming convention similarities (Source: Recorded Future)*

Other notable inauthentic behavior from the 250 analyzed accounts includes using profile pictures almost certainly stolen from other authentic social media users' accounts as well as using basic digital editing tools to edit images of female members of the Israeli Defense Forces (IDF) to resemble Palestinian resistance fighters, which is notably inconsistent with the majority of accounts that present content generally supportive of Israel (DISARM Technique T0086.003: Deceptively Edit Images [Cheap Fakes]). Additionally, one of the 250 accounts analyzed following the @jewish__fist Instagram account posted a graphic in December 2023 matching a post made by the account "IRNA News Agency" (@IrnaEnglish) — the official mainstream social media account of Iranian state-run news outlet Islamic Republic News Agency (IRNA). The graphic (**Figure 15**) depicts Prime Minister Netanyahu recklessly driving a bus full of people. The image was posted by Instagram account @bring_them_hom, with the caption, "He'll take us to hell".

Figure 15: *Screenshot of graphic posted by @jewish__fist inauthentic account and the official account of IRNA (Source: Instagram, Mainstream Social Media)*

Also in October 2023, the Telegram channel "Tears of War" (דמעות המלחמה; *t[.]me/demaothamelkhama*) — which the Shin Bet also attributed to Iran's security services — began posting content specific to Hamas-captured hostages, missing individuals, and Israeli victims to recruit Israelis to partake in anti-government demonstrations in response to the continuing hostage crisis (DISARM Technique T0083: Integrate Target Audience Vulnerabilities into Narrative). Currently, the channel remains active with 1,990 subscribers and continues to post pictures of abductees and killed individuals while interjecting content suggesting the Israeli government, especially Prime Minister Netanyahu, is responsible for the deaths and continued hostage crisis due to its decision to continue military operations. Multiple posts include the hashtags #remove_now (#הדחה_עכשיו) and #everything_because_of_him (#הכל_בגללו), referring to Prime Minister Netanyahu.

Similar to other accounts previously described, "Tears of War" has also posted content highlighting specific posters featured during demonstrations or displayed in specific locations. Some of these posts also provide coordinates of where the posters were displayed with a link to Google Maps and text "for live location tracking". The posters feature the same "Tears of War" logo as well as QR codes, which provide a hyperlink to the "Tears of War" Linktree, which, like the previously described "No Voice" Linktree, provides follow-on links to the group's Telegram account, Instagram account, and a Google document.[21] The Google document provides questions soliciting PII, such as name, mailing address, phone number, and residential community; it also contains a question that asks, "in what areas can you help us". This last question is followed by a list of box-check options, including "pasting and hanging

[21] *https://t[.]me/s/demaothamelkhama*

funeral notices", "give flowers to bereaved families", "transportation", and "fighting fake news on our Telegram channel".

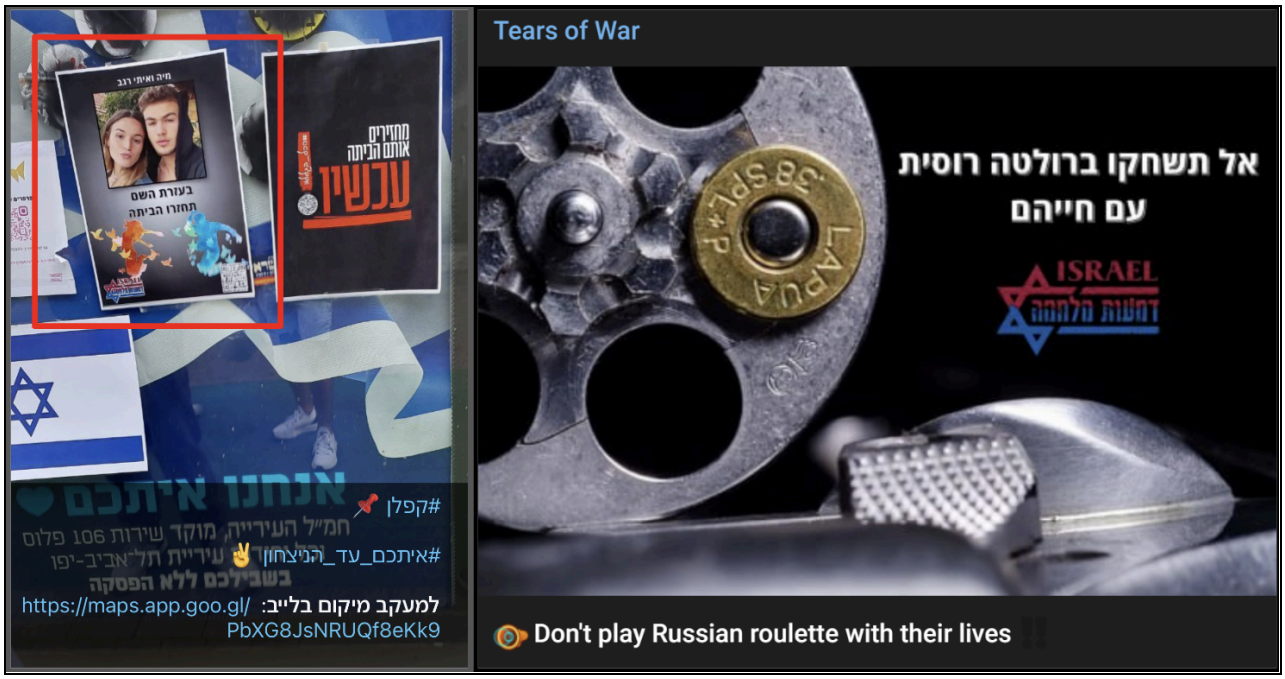


Figure 16: *(Left) Screenshot of the "Tears of War" Telegram post featuring Google Map coordinates; (Right) Screenshot of post comparing Israeli government decisions to hostage crisis (Source: Telegram[22])*

One month later, in November 2023, an additional Telegram channel, "BringHomeNow" (מחזירים אותם הביתה עכשיו; *t[.]me/BringHomeNow*) began posting about individuals Hamas abducted and held hostage. The description of the channel, translated from Hebrew to English, states its purpose is to recruit individuals to provide support to families of those who have been kidnapped or are missing. The channel's logos and design impersonate the nonprofit organization "Bring Them Home Now" (specifically, the organization's Telegram Channel, "BringThemHomeNow"); it creates posts identical to posts on the authentic "BringThemHomeNow" channel, almost certainly in an attempt to deceive social media users (DISARM Technique T0099: Prepare Assets Impersonating Legitimate Entities). Similar to the previously described channels, interjected among most posts on this channel that focus on victims of the Israel-Hamas conflict are posts that provide hyperlinks to alternate platforms soliciting PII. Two specific examples are a hyperlink to a Google document, which exhibits the same stylistic characteristics as both previously discussed Google documents linked to other accounts, and a hyperlink to a digital emailing campaign hosted on *Drove[.]com*. Notably, according to the email campaign's homepage on *Drove[.]com*, by participating in the campaign, a user accepts Drove's "T&C and Privacy Policy including receiving messages from BringHomeNow", which suggests that a participant's email address would be shared with BringHomeNow.[23] The Drove campaign webpage provided by *t[.]me/BringHomeNow* (image provided below) provides an introduction paragraph in Hebrew and translates it to English as follows:

[22] *https://t[.]me/demaothamelkhama*
[23] *https://www.drove[.]com/campaign/65534add6bb75883a536ccdf*

Time is running out! We must save them! Take 2 minutes today and send this important email. Our mission is unwavering: to return the kidnapped to their homes immediately and without any conditions. Together we are a force. Let's bring the children home! The government's policy strengthened Hamas. The government that abandoned our families continues to abandon us, incite, divide and engage in political survival. If after all this we don't replace her, Hamas won. All members of the government, all members of the coalition, should hear the cries of the families every night. We still do not hear about a significant plan for their release. The State of Israel needs elections, we have months and perhaps years of hard fighting, rebuilding, and rehabilitation ahead of us - only a leadership that has won the people's trust (be it right, left, center) can lead in such moments Let's help me make that at the top of our country in our unity.

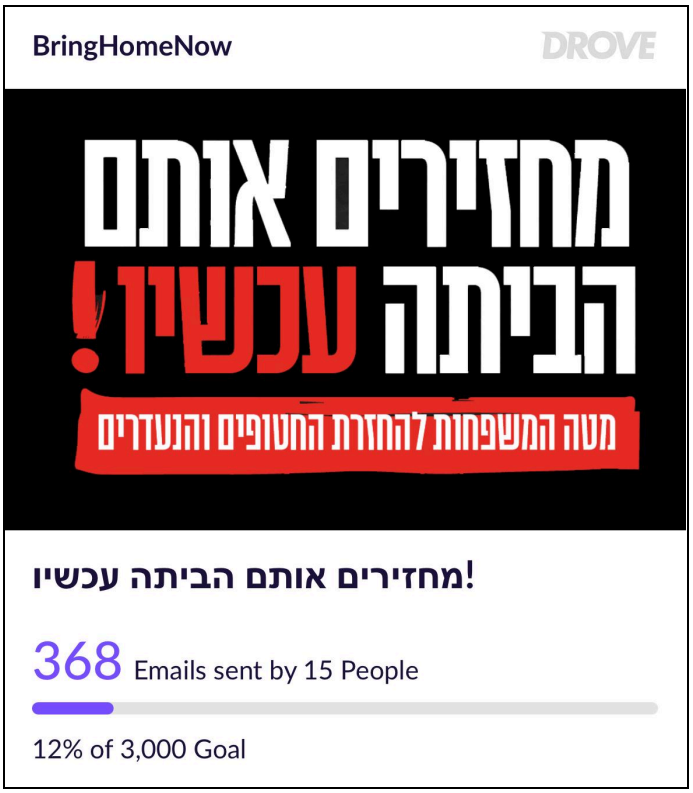


Figure 17: *Screenshot of "BringHomeNow" Drove campaign (Source: Telegram[24])*

[24] *https://t[.]me/BringHomeNow*

Attribution

Emerald Divide's influence campaign is likely being conducted by advanced influence threat actors aligned with Iran. Utilizing the North Atlantic Treaty Organization (NATO) Strategic Communications' attribution framework, the following factors support this attribution.

Behavioral evidence:

- During its third operation, Emerald Divide accounts directly referenced Iran multiple times, such as in a video it posted that used AI-generated voice-overs and fictitious depictions of Israel in 2043, which includes video footage of the IRGC flag and what is very likely the IRGC Navy conducting naval drills. Additional posts include images of Qassem Soleimani as well as an image that suggests the possibility of Iranian arms shipments to the PA.
- In one instance, an Emerald Divide account posted a graphic that matched a post made by the official mainstream social media account of Iranian state-run news outlet IRNA.

Contextual evidence:

- Emerald Divide supports narratives that seek to exacerbate ideological divisions within Israeli society on specific social and political issues and undermine the Israeli government. Notably, these narratives support Iran's top priorities, which include projecting Iran's regional power and influence while curtailing Western and Israeli presence in the region, using both proxy warfare and its "soft war" power to oppose the US and Israel.
- Emerald Divide amplifies these narratives by posting AI-generated images expressing negative sentiment toward Prime Minister Netanyahu and other Israeli political leaders.

Overlap with previous reporting:

- On February 7, 2024, Microsoft attributed three Emerald Divide social media accounts to influence threat actor Storm-1364, which Microsoft also assessed as a likely Iranian state threat actor.
- The Shin Bet attributed specific social media accounts discussed in this report to Iranian security agencies targeting Israeli citizens.

Outlook

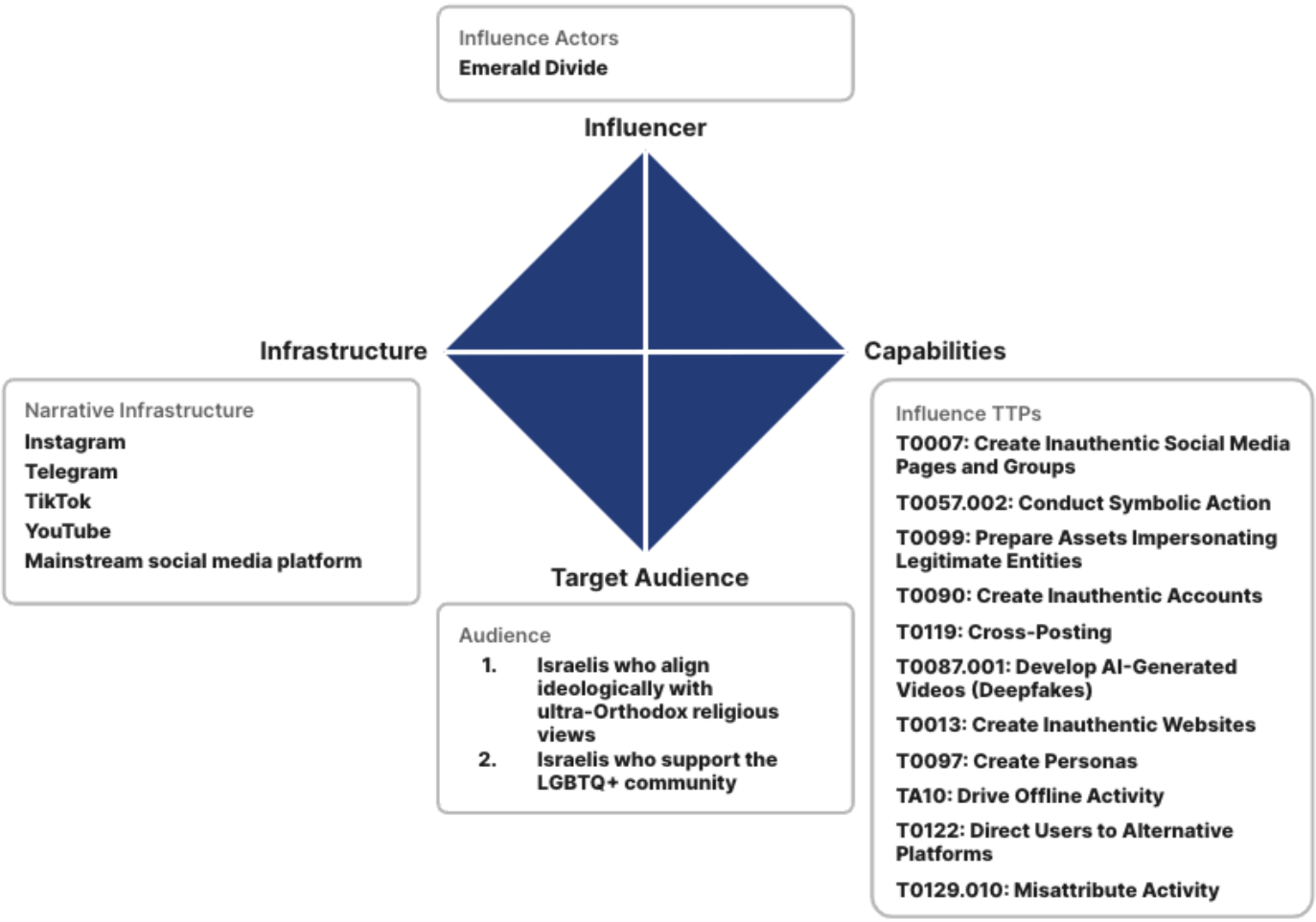
This influence campaign demonstrates a trend of Emerald Divide shifting its operations to primarily Telegram, likely in an attempt to avoid asset seizures or takedowns. Common use of generative AI throughout this campaign very likely indicates that advanced influence threat actors have adopted and implemented AI as a routine capability, which will likely continue to improve over time as the technology advances and as the threat actors apply lessons learned through repeated operational employment. Emerald Divide's limited success in purportedly influencing and persuading its target audience to engage in specific and observable physical actions will likely embolden threat actors to continue using influence operations to achieve specific objectives, especially in complex operational environments in

which the threat actors seek to obfuscate attribution and execute offensive actions below the threshold of armed conflict.

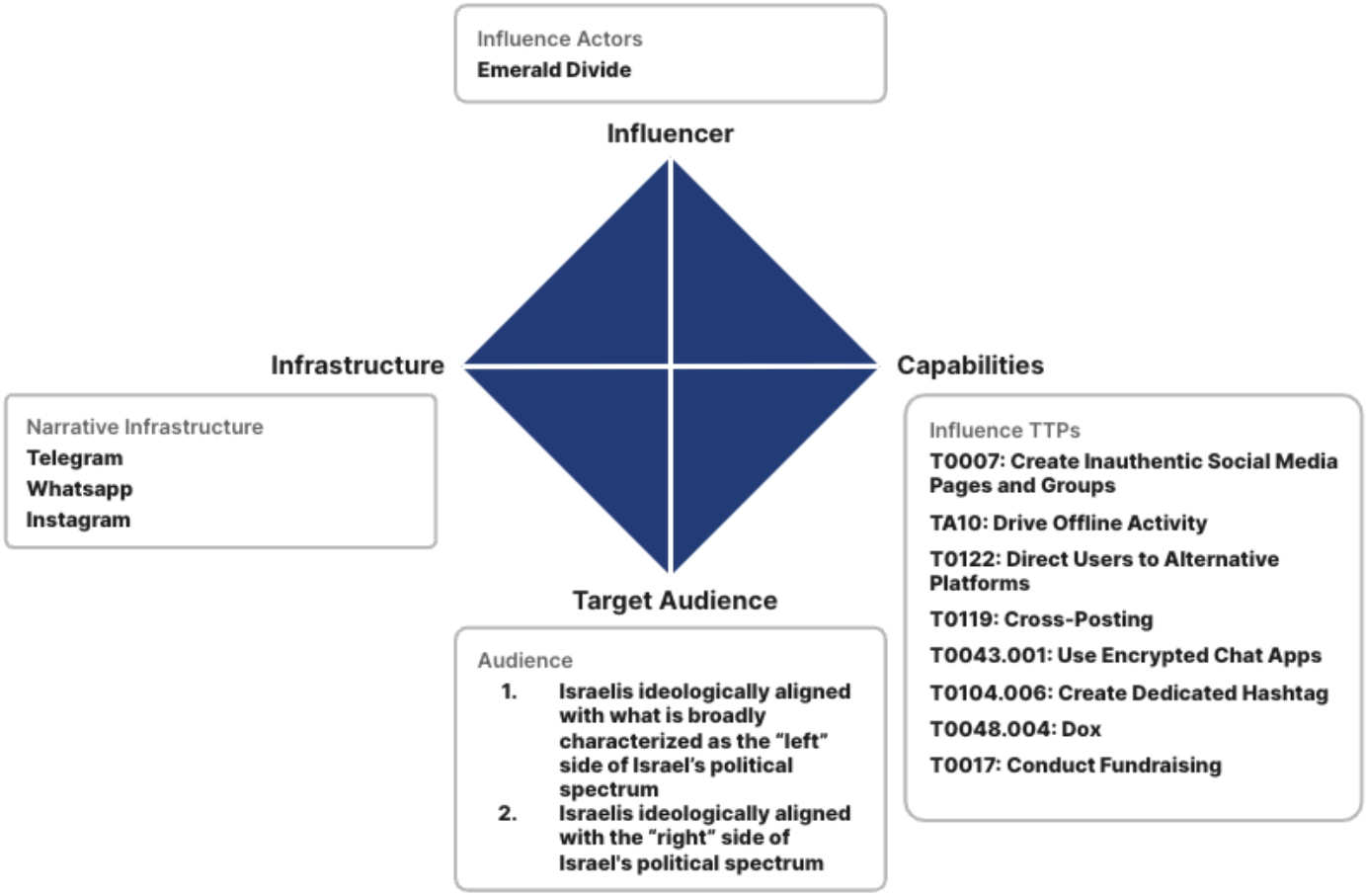
As the Israel-Hamas conflict continues, Emerald Divide will also likely continue taking advantage of dynamic events related to Israel's domestic political landscape to exploit corresponding psychological vulnerabilities. Based on the campaign's historically observed activity, it is also likely that the campaign will change its influence objectives again based on emerging targets of opportunity that trigger competing reactions from various political factions within Israel's government and its broader political system, such as Israel's next legislative election, which is scheduled to take place in October 2026.

Appendix A: IO Diamond Models

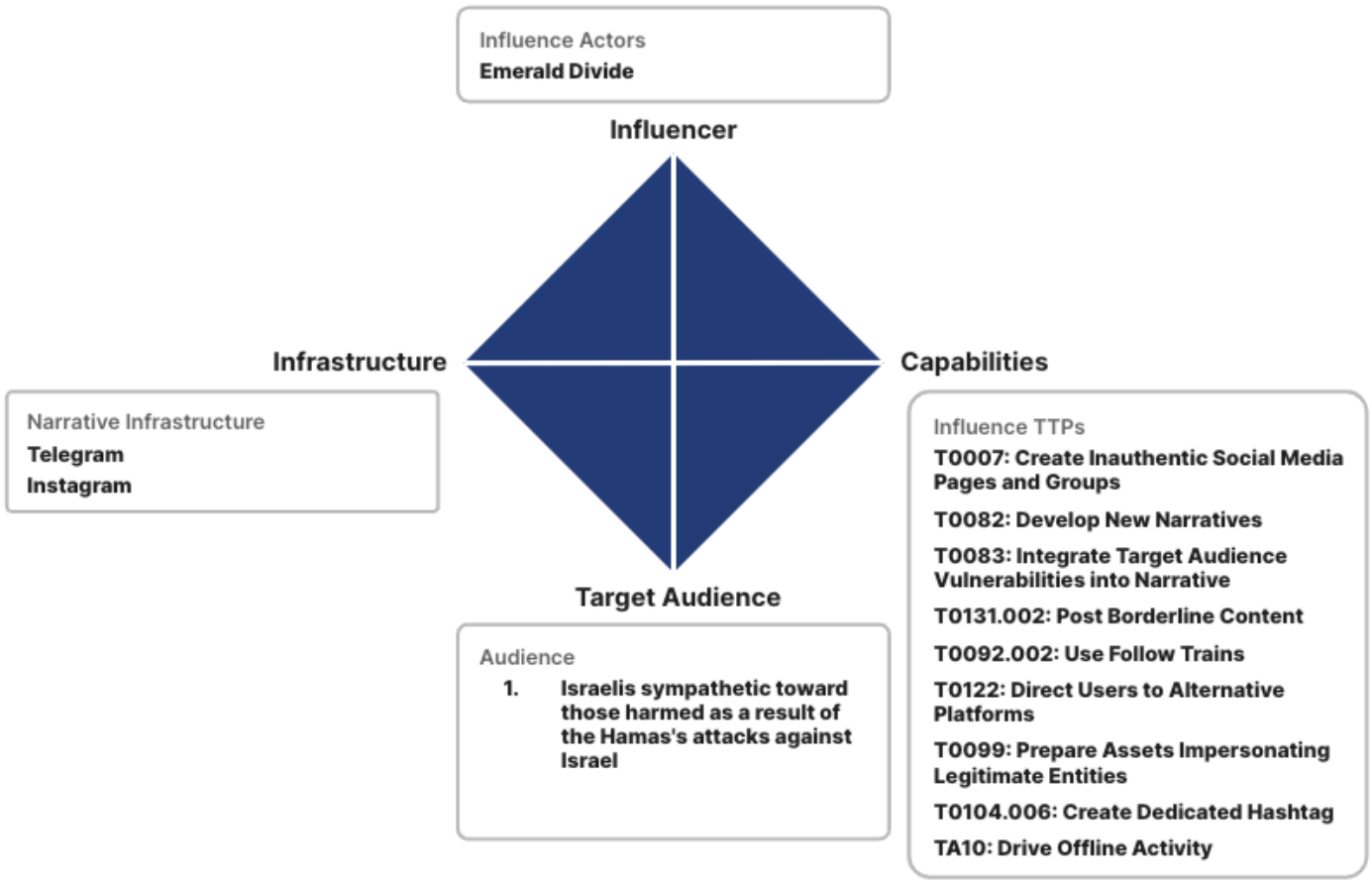
Operation One Influence Objective: Increase Social Conflict Between Israel's "Ultra-Orthodox" Religious Groups and Israel's LGBTQ+ Community



Operation Two Influence Objective: Incite Conflict by Pivoting Individuals on the Left and Right Sides of Israel's Political Spectrum Against Each Other



Operation Three Influence Objective: Sow Discontent Among Israeli Citizens Regarding the Israeli Government's Response to Hamas's Attacks



Recorded Future®

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com