Reichman University
International Institute for Counter-Terrorism (ICT)
With the Support of the Jusidman Foundation

#WeAreNotSafe – Exposing How a Post-October 7th Disinformation Network Operates on Israeli Social Media

Mr. Uri Klempner
February 2024

About the ICT

The International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world. Using a multidisciplinary arpproach, the ICT work to facilitate international cooperation in the global struggle against terrorism.

As an independent think-do-tank, the ICT focuses on themes realted terrorism, counter-terrorism, homeland security, threat vulnerability, risk assessment, intelligence analysis, national security, and defense policy.

Serving as a joint forum for international policymakers and scholars, the ICT draws upon the experiences of a comprehensive and international network of individuals and organizations with unique expertise on terrorism and counter-terrorism research, public policy analysis and education

In addition to publishing research papers, situation reports and academic publications for worldwide distribution, the ICT hosts a number of international seminars, workshops and conferences to discuss and educate followers on global and regional issues of security, defense, and public policy in order to better facilitate the exchange of perspectives, information and proposals for policy action.

Licensing & Distribution

Reichman University
International Institute for Counter-Terrorism (ICT)
With the Support of the Jusidman Foundation

Research Article
February 2024
ict.org.il

Reichman University International Institute for Counter-Terrorism (ICT)
With the Support of the Jusidman Foundation

ict.org.il
International Institute for Counter-Terrorism, (2024)

#WeAreNotSafe – Exposing How a Post-October 7th Disinformation Network Operates on Israeli Social Media

Mr. Uri Klempner

Abstract

This report investigates a sophisticated and extensive coordinate network orchestrating a disinformation campaign targeting Israeli digital spaces since October 7th, 2023. By using digital forensic strategies and network analysis, this research unearths the magnitude of knowledge, organization, and resource expenditure of the campaign. Network analysis indicates the campaign includes thousands of accounts. Though unable to trace the exact origins, phone numbers belonging to accounts have been linked to Jordan and Egypt, and it is alleged that many of the tactics are likely inspired by previous Iranian campaigns. Advanced and novel tactics are unearthed in this report, including evading reverse image search, strategic hashtag use, and meticulous crafting of fake accounts and engagements. These tactics signify a nuanced approach to creating a disinformation network aimed at manipulating public opinion in Israel. This report also examines Meta's responsibilities, highlighting concern over its inaction and staggered transparency. This report contributes crucial insights regarding influence campaigns in Israeli digital spaces and provides valuable learnings for social media platforms in combating disinformation campaign strategies and efforts.

Keywords: Disinformation; Social Media; Coordinated Inauthentic Behavior (CIB); October 7th Attack

Received: 21 February 2024 • Accepted: 21 February 2024.

Introduction

In the wake of the Hamas attack on October 7th, the Israel Defense Forces (IDF) Information Security Department revealed a campaign of Instagram accounts impersonating young, attractive Israeli women who were actively engaging Israeli soldiers, attempting to extract information through direct messages.[1] Coined as an "Avatar Infrastructure," the IDF accuses Hamas of operating this network. This paper exposes a different yet equally alarming aspect of these networks of fraudulent accounts. Beyond espionage, this research unearths a network of accounts geared towards mass disinformation. Particularly on Instagram, Israeli pages have been inundated with comments in broken Hebrew, vehemently criticizing the government and spreading disinformation. These comments, often debating the merits of the war in Gaza and lamenting what they

1 IDF, 2023

believe to be the end of Israel, hint at something more orchestrated. This research has identified hundreds of such accounts — with an estimated total network size in the thousands — operating with high sophistication and intensity. Unlike usual low-effort fake accounts, these accounts meticulously mimic young Israelis. They stand out due to the extraordinary lengths taken to ensure their authenticity, from unique narratives to the content they produce to their seemingly authentic interactions. This not only serves the purpose of convincing the average user of the authenticity of the person behind the username, but it also aims to evade the algorithm's detection as inauthentic.

The phenomenon of fake account networks engineered for disinformation is not novel, and platforms frequently grapple with such issues.[2] The sophistication and dedicated effort observed in this network point to a group's intense commitment to disseminating discord and disinformation within the Israeli segment of Instagram. Their reach and interactive capacity with Israeli users —unimpeded by Meta's efforts[3] to combat disinformation and fake accounts— signal another evolution in bespoke cyberwarfare against Israel.

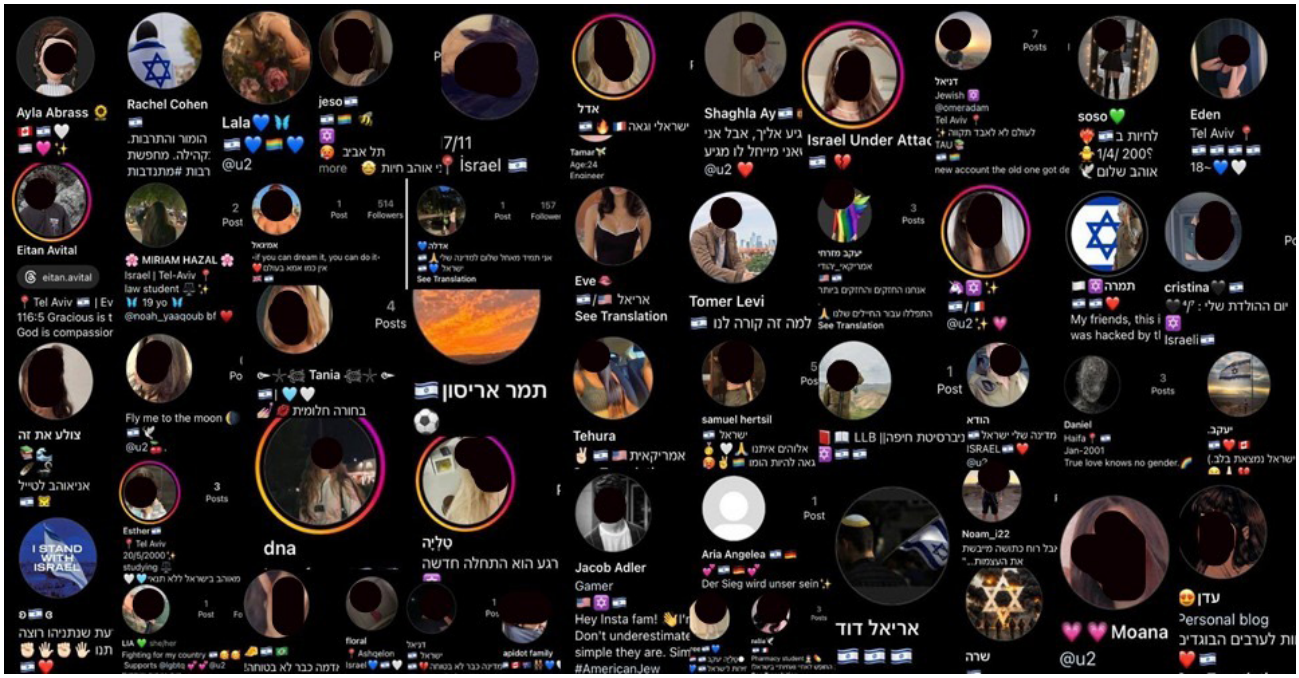

Figure 1 – Selection of accounts identified as belonging to the network.

Profile Formula

A core component of the detection methodology was applying qualitative linguistic analysis. This involved checking the fingerprint of language, syntax, and style used in

2 Dance, 2018

3 Mukherjee, 2023

4 Gleicher, 2018

5 Barojan, 2018

the comments and profile of the suspected account. Each account bio consistently incorporated a combination of specific elements: emojis, nationality, location, educational institution or occupation, age, and a personal quote, sports team or band. The recurrence of this specific formula across multiple accounts hinted at a standardized template for bio construction.

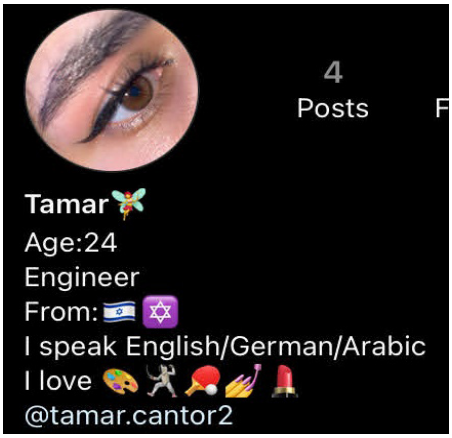

Figure 2 - Profile formula example.

Image Theft

Some profiles underwent a reverse-image search of their photos to ascertain their authenticity. Many of the images searched were found to be appropriated from genuine social media profiles or sites such as Pinterest. When this was the case, the account was marked as confirmed to be inauthentic. One innovative method involves using photos that are initially frames from videos, which allows for evading reverse searches in most cases. This is seen in Figure 4, where an image uploaded by an inauthentic account was a screenshot taken from a TikTok video.

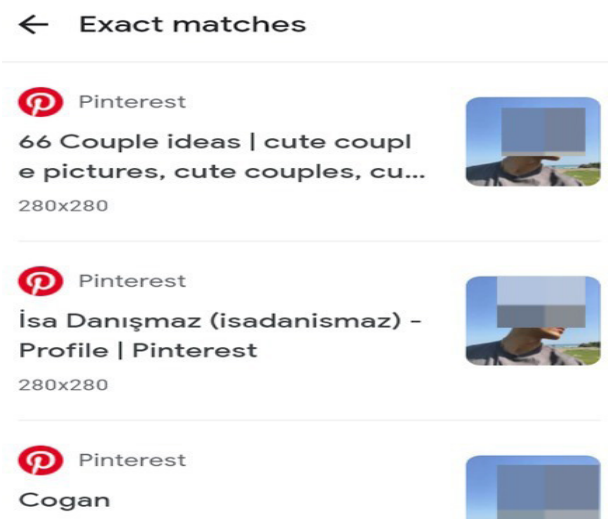

Figure 3 - Pinterest results for profile picture uploaded by one of the accounts.

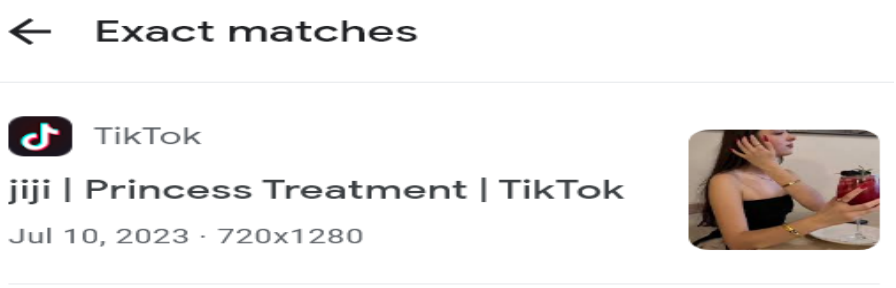

Figure 4 – Reverse image search on photo uploaded by account from the network originating from a TikTok video.

Registration Details

A significant pattern identified was the creation date of these accounts, with all verified accounts being created post-October 2023. This temporal clustering was indicative of the CIB being initiated following the Hamas attack on October 7th.

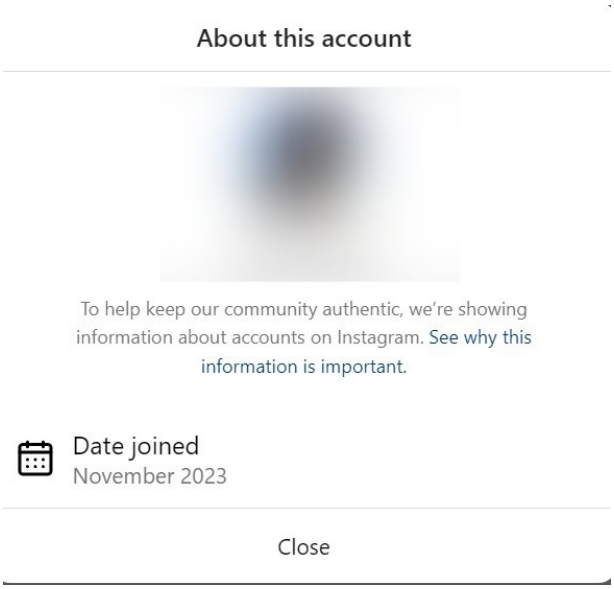

Figure 5 - "About This Account" feature used on one of the accounts from the network

The report uncovered that some accounts were registered using phone numbers originating from Egypt and Jordan. The notable discovery here is that using real, unique phone numbers for account verification suggests a substantial investment in creating these accounts, indicative of an operation with considerable capital. The hypothesis for this interest in registering with a phone number rather than just an email is that it likely increases the legitimacy of an account in Instagram's system. The phone numbers' location does not necessarily link the CIB with the respective countries. In 2021, an Iranian network operating in Israeli digital spaces was operated using accounts traced to Palestinian and Israeli phone numbers.[6]

6 FakeReporter

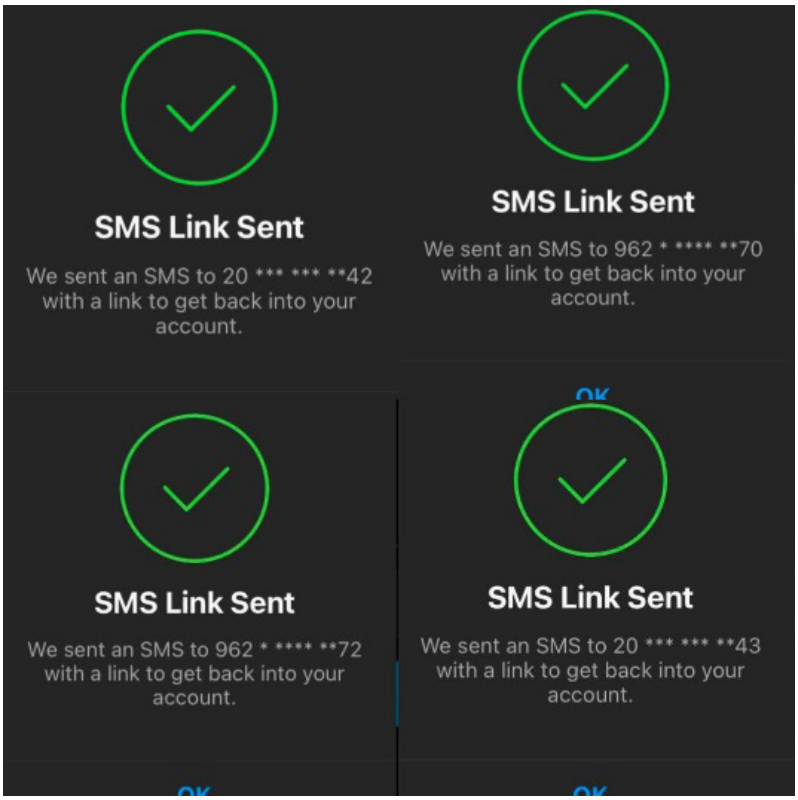

Figure 6 - Accounts linked to phone numbers from Egypt and Jordan

Network Analysis

Using specific OSINT tools enables the extraction of followers and following lists from public Instagram profiles. However, Meta does attempt to limit these tools. A list of 400 accounts, highly suspected of being part of the network, was compiled. It is essential to note this cap of 400 was due to resource constraints of the research, not for lack of more accounts to document.

To approximate the network's scale, a sample of eight verified accounts within the network was analyzed, and their follower lists were extracted, resulting in a total dataset of 2,422 followers. Calculating unique followers from the dataset leads to an overlap result exceeding 47% (1,142 overlapped accounts). These results give a rough estimate that the network is at least in the thousands. The high level of overlap can best be visualized in the below network analysis diagram generated using Gephi, showing the interconnectedness in the following and followed lists of only three confirmed accounts from the network.

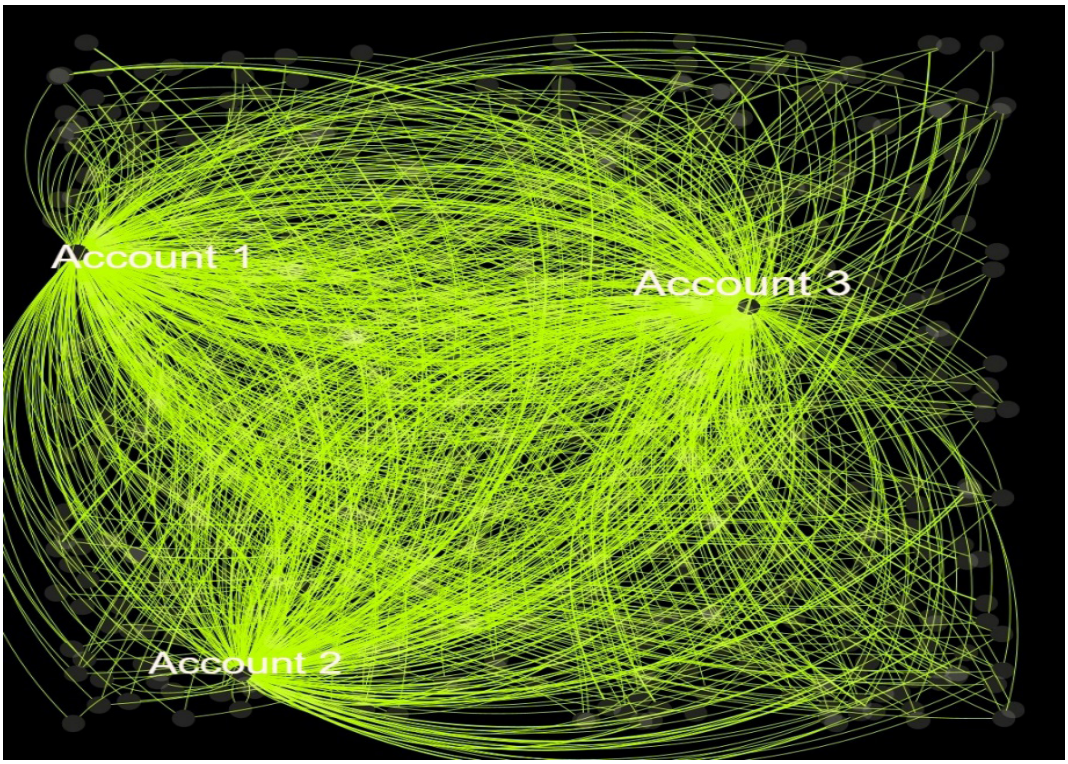

Figure 7 - Data visualization of overlap in the following and follower list of three accounts from the network. The diagram depicts each account as a node, with lines representing connections to or from the three principal accounts, which are marked.

Origins of the Network

The most viable strategy for identifying the network's founders relies on detecting their own (human) errors. Given the vast number of accounts and the content volume generated, reverse-engineering the network to pinpoint its genesis — potentially uncovering links to the creators — is too significant of a challenge. However, some of the content and behavior of this network mimic past suspected and confirmed Iranian CIB campaigns in Israel in the last three years, including during elections[7,8], the May 2021 Gaza War[9], and the 2023 judicial reform protests.[10,11] This will be demonstrated throughout the report.

Network Modus Operandi

Each account was methodically set up with individual phone numbers and email addresses, suggesting a substantial capital investment and working hours. This approach, along with the meticulous crafting of profiles, reflects a significant commitment to the CIB's operational security and authenticity.

7 Siegal, 2022

8 Frenkel, 2021

9 Benjakob & Goichman, 2021

10 Benjakob, Peleg, & Breiner, 2023

11 Ilnai, 2023

Machine Translation

A conspicuous aspect of these accounts is the likely usage of machine-translated Hebrew. The disjointed and linguistically strange comments imply that the CIB's architects are not Hebrew-speaking and likely translate to Hebrew using online tools. There's no official way to confirm that a text is translated, but it is evident when the gender for nouns is incorrect, very unusual words or illogical grammar being used usually lead to the conclusion that the comment was not written by a native speaker that is aware of the nuances of the language.

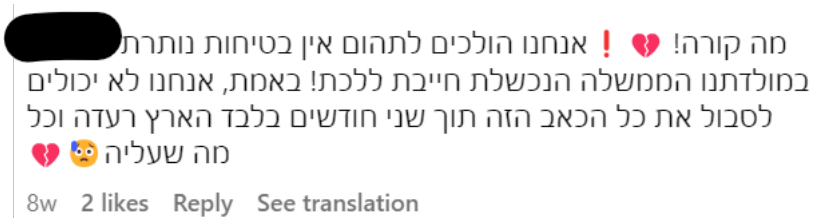

Figure 8 - Comment in Hebrew stating there is no more safety in the country.

Hashtags as an Index

The intricate modus operandi of these fake Instagram accounts includes a novel tactic: the use of a specialized hashtag system, which plays a role in their operational strategy.

The accounts post generic images to fill their account feed to make the account seem real. They then employ a hidden hashtag in their posts, consisting of a seemingly random string of numbers and letters.

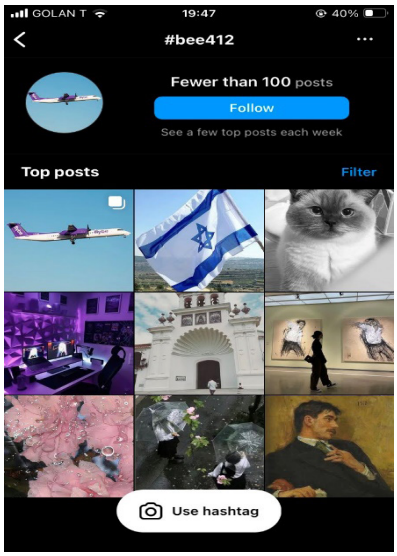

Figure 9 - Posts published under one of the group's unique hashtags on Instagram.

The hypothesis regarding this tactic is that the group orchestrating these accounts utilizes these hashtags as a means of indexing them. This system likely serves a dual purpose: firstly, to keep track of the network's expansive network of accounts and unique

posts, and secondly, to streamline the process of boosting engagement among these accounts. By searching for these specific, unique hashtags, the group can quickly locate posts from their network and engage with them using other fake accounts, thereby artificially inflating the visibility and perceived authenticity of the fake account.

Crafting Organic Engagement

A significant amount of effort is dedicated to crafting what appears to be organic interactions between these accounts. This goes beyond mere comments and likes; the network architects have taken steps to fabricate fictional relationships between different accounts. Such relationships could range from friendships to romantic connections, all designed to add a layer of authenticity and depth to the accounts' online personas. This tactic was also noted in the IDF Information Security Department exposé of the Hamas bot network.[12]

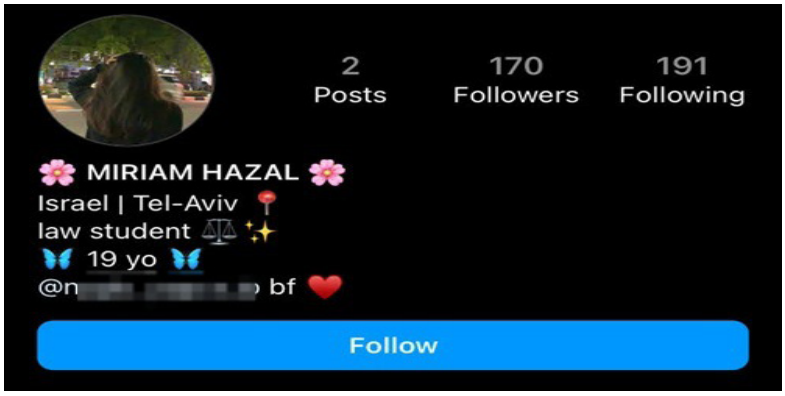

Figure 10 - A fake account tagging another account belonging to the network as a romantic partner.

Figure 11 – Instagram story uploaded by a fake account depicting a relationship with another account from the network.

12 IDF, 2023

The methods of organic account spoofing within the network are a testament to the high level of dedication, attention to detail, and motivation behind the network. It indicates an intricate level of organization and suggests that considerable thought and planning have gone into developing these personas and their interactions. The motivations behind this effort might lie in convincing a passerby of the account's authenticity. Still, it may also be an attempt to limit attention from platform algorithms designed to detect unusual accounts.

Cross-Platform Personas – TikTok, Facebook, and Threads

Another means of creating authentic and organic profiles is connecting Instagram accounts to other social media platforms in a recursive loop of social media accounts. There is a clear and intense effort to create authentic personas using integrated social accounts and to expand engagement.

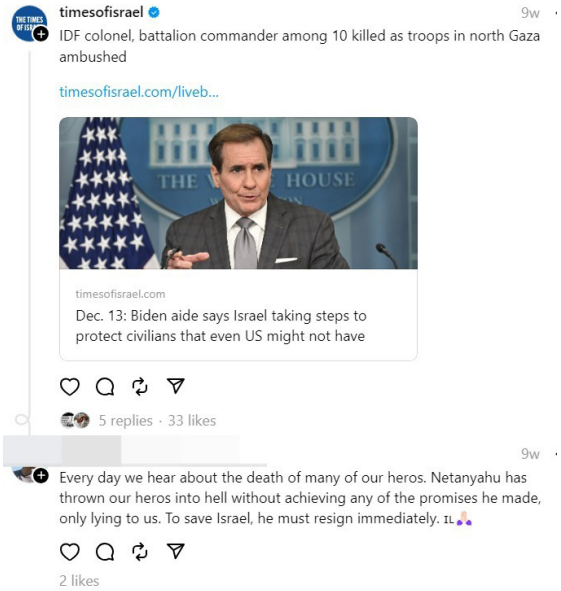

Figure 12 - Fake account responding to Times of Israel's account on Threads.

As seen below with a Facebook profile and Threads account of two highly active accounts that portray themselves as romantic partners. The woman's Facebook profile (see reverse image search in figure 5 earlier) is linked to the fake Instagram account and a TikTok account. The man's account was linked with Meta's Threads, where he posted a screencap from a post on TikTok by an account under the same name. This is a meticulous effort in crafting intricate and layered online personas for accounts. At least 12 Facebook accounts were linked to confirmed inauthentic Instagram accounts, possibly indicating a transition to attempt molding the discourse on other platforms.

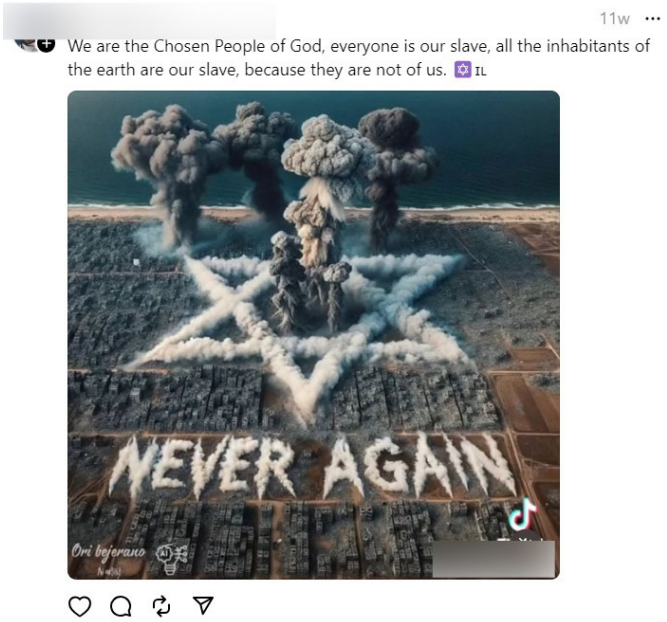

Figure 13 - Threads post of a post on TikTok by an account under the same name.

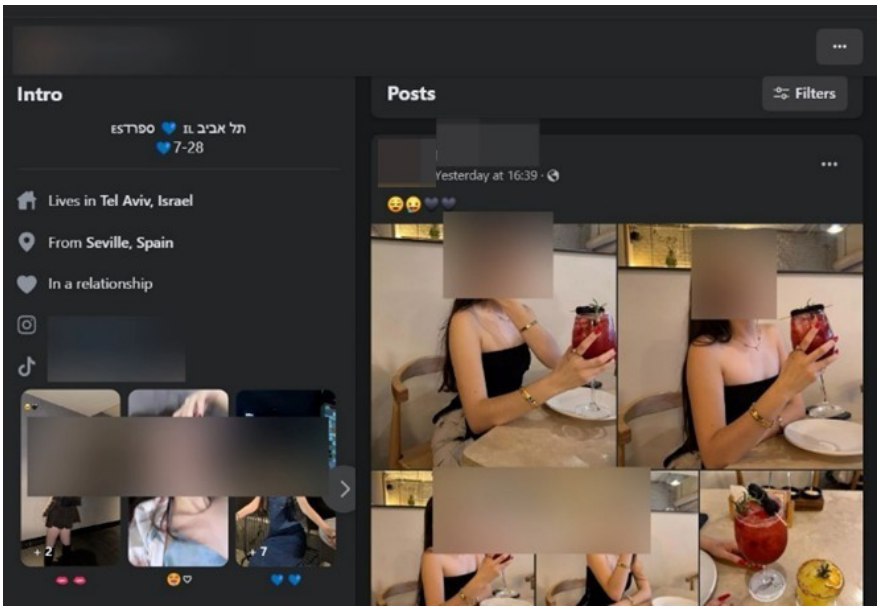

Figure 14 - Facebook profile of the female account from the network.

Cultural Misperceptions

The construction of these profiles offers a window into how the creators perceive Israeli society. The accounts predominantly portray their personas as young Israelis, with many claiming to be engineers or STEM students and a notable number identifying as members of the LGBTQIA+ community. This stereotypical portrayal suggests a superficial, even caricatured, understanding of Israeli demographics and social dynamics.

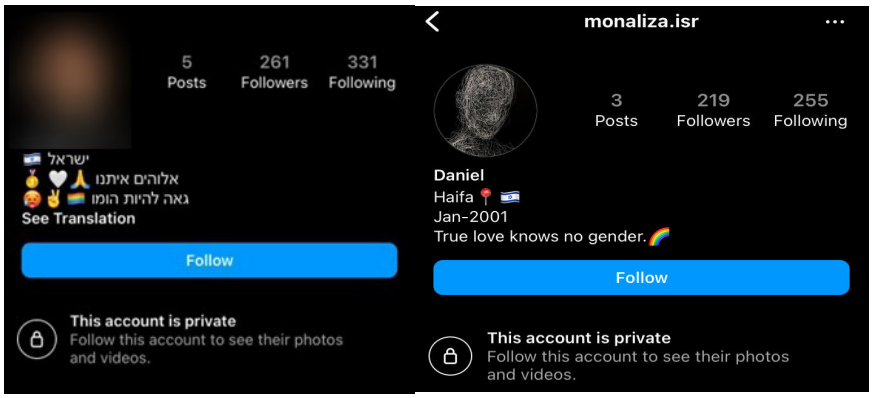

Figure 15 - Accounts from the network with queer identifiers in the bio.

Despite an often superficial understanding of Israeli society, these accounts demonstrate a capability to engage in convincing interactions within larger Israeli comment sections on Instagram. While the creators may lack deep cultural insights, they possess sufficient understanding to superficially mimic authentic engagement, allowing them to pass the "Turing test" among Israeli audiences.

Content Analysis

The accounts are active on Israeli Instagram pages, particularly posts related to the war in Gaza. Their comments and posts are tailored to engage with current events and public sentiments regarding these issues.

Many of the narratives center on accusing the Israeli government, particularly Prime Minister Benjamin Netanyahu, of deceiving the public about the events of October 7th or being unfit to lead. The primary motive behind this is to exploit Netanyahu's well-known polarizing effect on Israeli discourse. This strategy has precedence in CIB campaigns against Israel, with Iranian CIB networks[13] often focusing messaging on polarizing Israelis through Netanyahu.

Figure 16 – Comment on post by Israel's Leader of the Opposition blaming Netanyahu for failing to protect Israelis.

13 FakeReporter

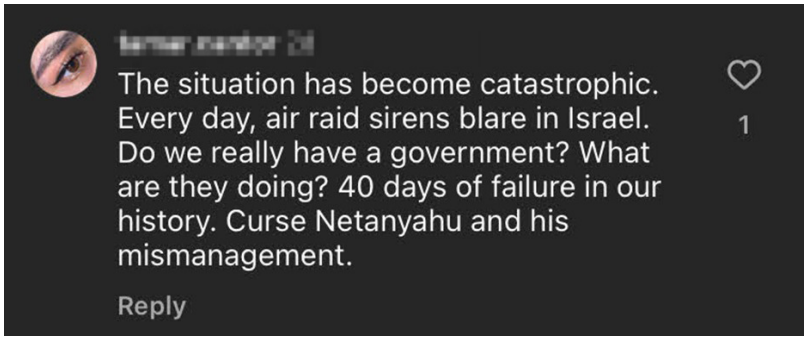

Figure 17 - Comment claiming Netanyahu is mismanaging the war.

Figure 18 - Comments blaming Netanyahu [translation overlaid]

One example of misinformation being spread by the network is the now-debunked video purportedly showing Israeli helicopters attacking civilians[14], which these accounts claim depicts an Israeli assault on attendees of the Nova Festival. This narrative serves a dual purpose: it attempts to minimize the perceived brutality of the October 7th attacks, while shifting the blame for civilian casualties to Netanyahu.

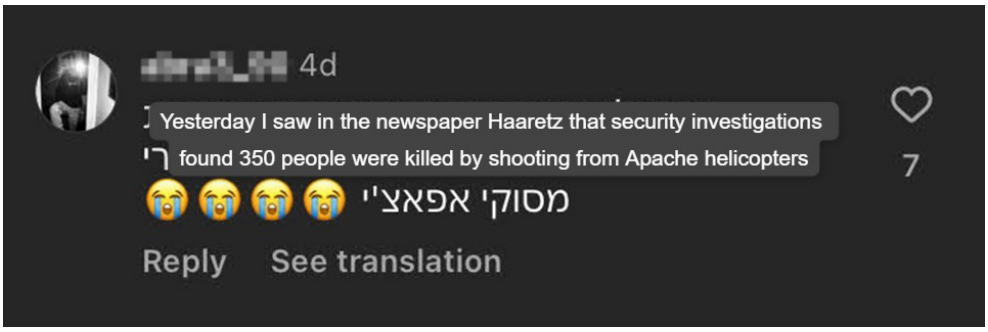

Figure 19 - Comment spreading disinformation [translation overlaid]

14 Abreu, 2023

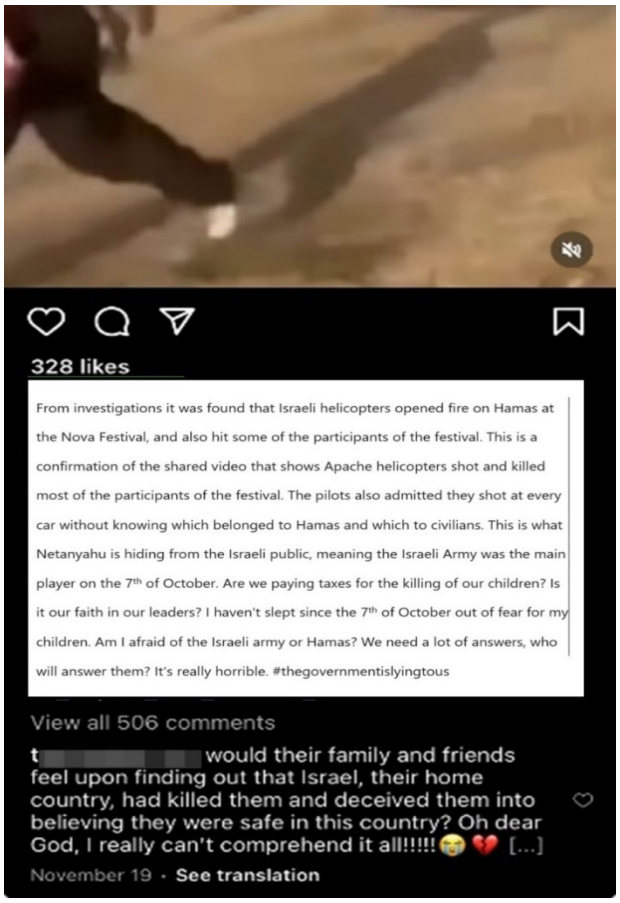

Figure 20 – Popular post by account from the network, spreading disinformation that Israel killed the festivalgoers on October 7th [translation overlaid]

In their posts and comments, accounts persistently claim that the ongoing conflict in Gaza is futile and costly for Israel. It emphasizes the heavy toll of the war on Israel, both in terms of resources and human lives. A significant emotional element is added to this narrative by falsely claiming that Israeli airstrikes in Gaza are resulting in the deaths of hostages, effectively portraying Netanyahu as responsible for the loss of Israeli soldiers and civilians. This narrative strategy is designed to evoke emotional responses and sway public opinion against the war effort.

Push for Emigration

The bottom line of these narratives is the suggestion that Israel is no longer safe and the government is untrustworthy. The accounts frequently express sentiments of lost safety and then reinforce these claims by stating that they, or others, have chosen to emigrate from Israel back to their home countries. Many accounts are claiming there is a "curse of the 8th decade", claiming Israel will not survive past eighty years of existence. This theory is particularly popular in the Arab world and relatively unknown in Israel.[15]

15 Yadid, 2023

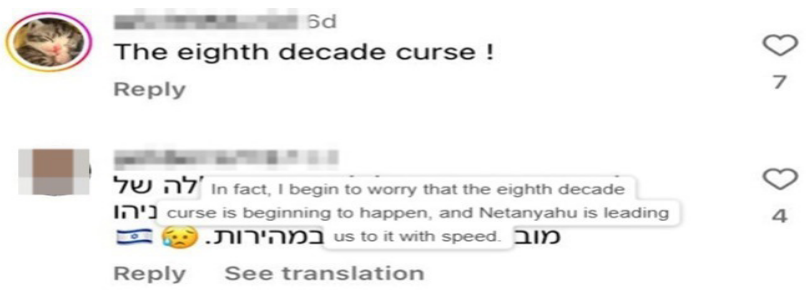

Figure 21 - Comments claiming the eighth-decade curse is real [translation overlaid]

Figure 22 – Comments from fake accounts on a post by Israel's national broadcaster discussing emigration.[translation overlaid]

The narrative is further amplified by a dedicated page, also likely run by the same group, which actively promotes emigration by comparing Israeli cities to safer alternatives in the United States.

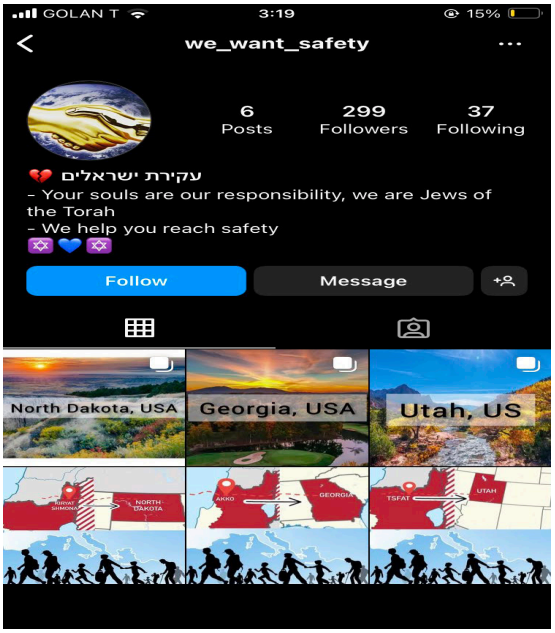

Figure 23 - Page that promotes Jewish emigration from Israel.

A recurring element in the account bios and comments is the portrayal of themselves as dual nationals. This aspect, along with the emphasis on emigration, mainly pushed in comment discussions with real Israelis on Instagram, reflects a misunderstanding of Israeli society by the CIB's orchestrators. They overlook the fact that a significant portion of Israelis are from Arab countries to which they cannot return and that, ultimately, only about 10% of Israelis are dual citizens.[16]

Literal Strawmen

An interesting rhetorical strategy this group employs involves a very literal use of the "strawman argument." This method is executed by having the accounts engage in contrived debates against each other in comment sections.

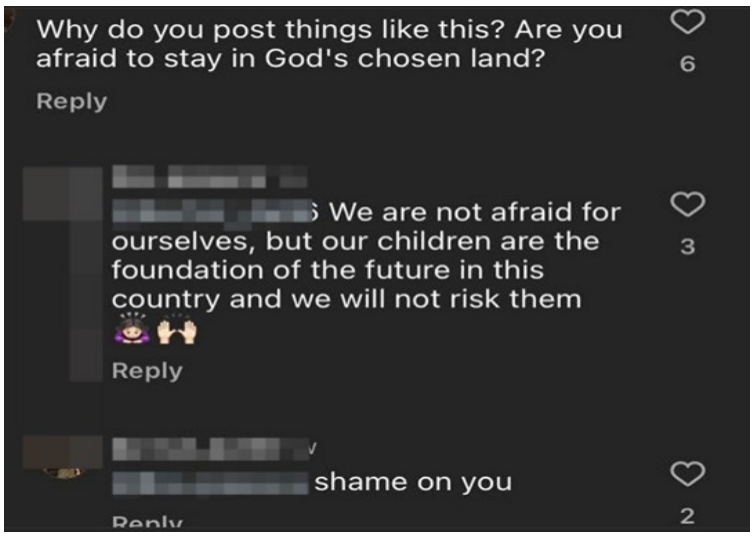

Figure 24 - Fake accounts arguing over emigration from Israel.

This serves a dual purpose: not only does it lend a facade of authenticity to the accounts, but it also frames and influences the parameters of the discourse for any real users observing these interactions.

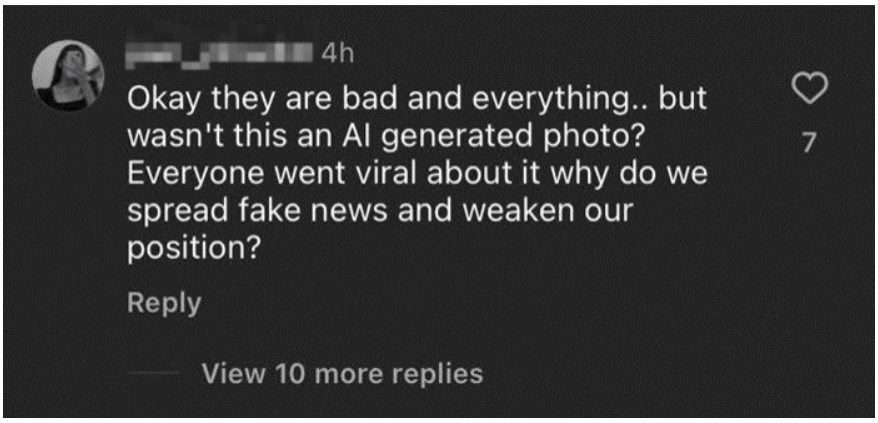

Figure 25 - Account undermining October 7th footage as disinformation.

16 Harpaz & Herzog, 2018, p. 10

This tactic effectively manipulates the audience's perception of what constitutes a valid and prevalent opinion within the community. By witnessing these detailed exchanges, real users may believe that the arguments presented by the fake accounts reflect a legitimate segment of public opinion, even when they are entirely fabricated.

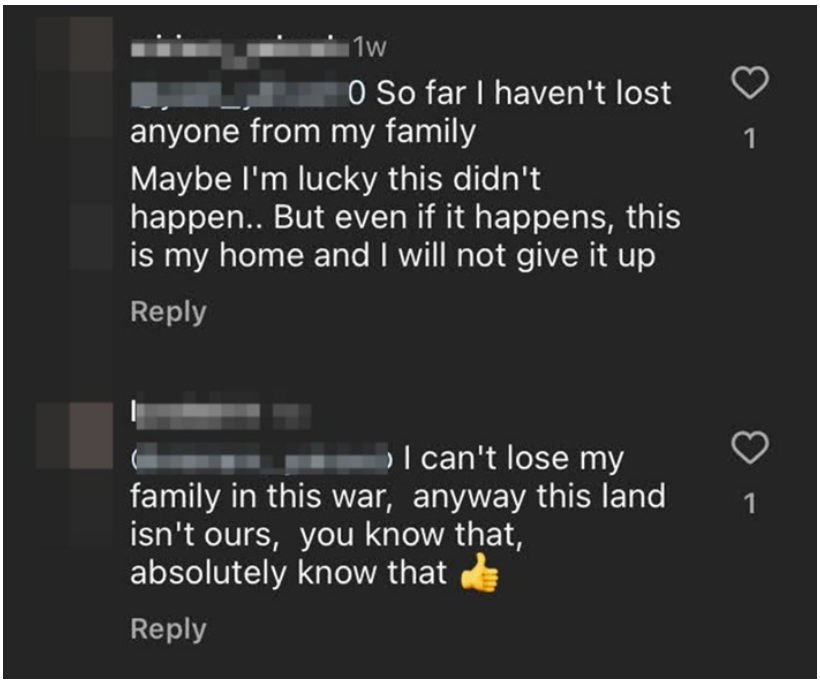

Figure 26 - Fake accounts arguing over emigration from Israel.

Discussion

Despite the apparent gaps in their superficial cultural understanding, the effectiveness of this CIB network in stirring discord is noticeable. Their success lies in infiltrating comment sections on Israeli Instagram pages, where they manipulate conversations. By feigning authentic Israeli perspectives, these accounts have managed to deceive real Israeli users into engaging with their views. These views, which attribute sole blame to Israel for the October 7th incidents, criticize the conduct of the Gaza war, question the competency of the government, and promote the notion of diminished safety in Israel, effectively fuel a narrative of distrust and disillusionment. In doing so, these accounts play a significant role in shaping perceptions and debates surrounding critical national issues, demonstrating the potent impact CIB campaigns can have.

Instagram as a Novel Platform

The network's primary focus on Instagram does represent an unprecedented shift in CIB campaigns targeting Israel, signaling a strategic motivation to influence a younger demographic in Israel, as opposed to other campaigns that were more active on X[17]

17 Siegal, 2022

and, to a lesser extent, Facebook and WhatsApp[18,19], targeting a more adult segment. As detailed in the previous chapter, there is a significant gap in understanding Israel's social and cultural nuances, especially its youth. However, the campaign has a demonstrated interest in engaging this segment that is traditionally less targeted, and this is shown through the constant upkeep of youth-oriented profiles, with daily stories being uploaded and integrated TikTok accounts, resembling an average social-media active youth in Israel.

Meta's Responsibility

Social media platforms, especially Meta, must rigorously monitor and analyze the patterns of behavior presented in this paper. CIB networks, such as this one, must be investigated, and the perpetrators should go through rigorous restrictions to avoid them bypassing a simple ban. Meta has a reporting process across its platforms, yet the system lacks a specific option for reporting inauthentic accounts unless they are impersonating a celebrity or the reporting user. This limitation undermines efforts to combat CIB.

While Meta does provide impressive statistics on the number of fake accounts it acts on and even its proactivity of getting to said fake accounts before they are reported (99.10%!)[20], this transparency extends only to Facebook, claiming metrics for Instagram cannot yet be estimated. In 2021, Meta began publishing monthly "Coordinated Inauthentic Behavior Reports" and, in 2022, addressed CIB through its quarterly "Adversarial Threat Reports." When analyzing all quarterly reports of 2023, through the entire year, Meta reported the removal of 40 Facebook accounts, eight Pages, and one Group linked to CIB targeting Israel. This figure is modest and raises concerns, especially considering Meta's recent significant layoffs, which have affected moderation teams.[21]

Four months have passed, yet the network in this paper continues to grow and operate. Despite deactivating some accounts, Meta's failure to identify and dismantle the entire network contradicts its self-imposed standards for combating CIB.

Conclusion

The process of identifying these sophisticated fake accounts poses a complex challenge, but it becomes more manageable once an initial account is confirmed as fraudulent. The interconnected nature of these accounts, driven by their strategic objective to simulate

18 Benjakob, Peleg, & Breiner, 2023

19 Goichman, 2024

20 Meta, 2023

21 Field & Vanian, 2023

organic engagement, creates a pattern of interaction that can be traced and analyzed in effective mixed-method research. The levels of complexity, thought, resources, and capital expended into creating and maintaining this network are disconcerting. Even after hours of logging accounts, more and more still seem to exist.

The content strategy of these accounts is multifaceted, targeting emotional, political, and societal aspects to influence public opinion. While their tactics demonstrate a certain level of sophistication, the underlying misconceptions about Israeli society hint that the campaign is likely orchestrated by a group with ambitious goals. This research failed to pinpoint the origins of the group. Nonetheless, some of the tactics do have precedent in Iranian campaigns. From the meticulous creation of personas and strategic divisive messaging to a nuanced understanding of domestic politics, this campaign has proven its continuation of Iran's CIB legacy in the Israeli digital landscape. Ultimately, there is a group behind this network, and it is expending significant resources in this months-long campaign, showing that Meta has yet to prove a strategy for mitigating CIB and safeguarding the well-being of the people.

An advance notice of this report and a spreadsheet of suspected accounts were sent to Meta's public policy team in Israel.

References

Abreu, C. M. (2023, November 14). The Israeli army did not fire on its own civilians at the Nova music festival. Retrieved from France24: https://www.france24.com/en/tv-shows/truth-or-fake/20231113-disproving-claims-that-israeli-helicopter-fired-on-their-own-civilians-at-nova-music-festival

Barojan, D. (2018, November 5th). How to Identify Bots, Trolls, and Botnets. Retrieved from Global Investigative Journalism Network: https://gijn.org/stories/how-to-identify-bots-trolls-and-botnets/

Benjakob, O., & Goichman, R. (2021, May 19). 'Abandon Israel': Network of Fake Accounts Tries to Demoralize Israelis During Gaza War. Retrieved from Haaretz: https://www.haaretz.com/israel-news/tech-news/2021-05-19/ty-article/.premium/abandon-israel-fake-accounts-network-tries-to-demoralize-israelis-during-gaza-war/0000017f-ee0f-da6f-a77f-fe0f995b0000

Benjakob, O., Peleg, B., & Breiner, J. (2023, 6 18). Iranian Influence Groups Are Attempting to Deepen Social Rifts in Israel. Retrieved from Haaretz: https://www.haaretz.com/israel-news/security-aviation/2023-06-18/ty-article-magazine/.premium/iranian-influence-groups-are-attempting-to-deepen-social-rifts-in-israel/00000188-c4db-dd1d-ad98-cddb4d2f0000

Dance, N. C. (2018, July 13th). "Battling Fake Accounts, Twitter to Slash Millions of Followers." Retrieved from The New York Times: https://www.nytimes.com/2018/07/11/technology/twitter-fake-followers.html

FakeReporter. (n.d.). Rolling In The Deep. Retrieved from FakeReporter: https://fakereporter.net/pdf/Rolling_in_the_Deep_Summary.pdf

Field, H., & Vanian, J. (2023, May 26th). Tech layoffs ravage the teams that fight online misinformation and hate speech. Retrieved from Meta: https://www.cnbc.com/2023/05/26/tech-companies-are-laying-off-their-ethics-and-safety-teams-.html

Frenkel, S. (2021, July 21). Iranian Disinformation Effort Went Small to Stay Under Big Tech's Radar. Retrieved from The New York Times: https://www.nytimes.com/2021/06/30/technology/disinformation-message-apps.html#:~:text=message%2Dapps.html-,Iranian%20Disinformation%20Effort%20Went%20Small%20to%20Stay%20Under%20Big%20Tech' s,methods%20to%20sow%20discontent%20online.

Gleicher, N. (2018, December 6th). Coordinated Inauthentic Behavior Explained. Retrieved from Meta: https://about.fb.com/news/2018/12/inside-feed-coordinated-inauthentic-behavior/

Goichman, R. (2024, January 18th). 'We're Playing With Israelis' Minds': Inside Telegram Group Helping Thousands Spread Disinformation. Retrieved from Haaretz: https://www.haaretz.com/israel-news/security-aviation/2024-01-18/ty-article/.premium/

exposed-telegram-group-with-thousands-of-pro-palestinian-users-spreading-disinformation/0000018d-1c5c-d022-ad9d-1e7c69830000?lts=1707436343324

Harpaz, Y., & Herzog, B. (2018). Report on Citizenship Law: Israel. Florence: Robert Schuman Centre for Advanced Studies.

IDF. (2023, December 18). Dozens of new fictitious profiles were exposed. These are all the characters published so far.. Retrieved from www.idf.il/153436

Ilnai, I'. (30 06 2023). Dear Israelis, Iran used you to sow chaos in Israel, and you had no idea. YNET: https://www.ynet.co.il/digital/technews/article/r1a489yoh

Meta. (2023, September). Inauthentic Behavior. Retrieved from Transparency Center: https://transparency.fb.com/policies/community-standards/inauthentic-behavior/

Mukherjee, S. (2023, October 13th). Meta takes steps to remove Hamas-related disinformation. Retrieved from Reuters: https://www.reuters.com/technology/meta-takes-steps-remove-hamas-related-disinformation-2023-10-13/

Nimmon, B., Gleicher, N., & Franklin, M. (2023, May). Quarterly Adversarial Threat Report. Retrieved from Meta: https://about.fb.com/wp-content/uploads/2023/06/Meta-Quarterly-Adversarial-Threat-Report-Q1-2023.pdf

Siegal, T. (2022, 10 22). Twitter removes fake profiles promoting friction ahead of the Israeli election. Retrieved from Times of Israel: https://www.timesofisrael.com/twitter-removes-fake-profiles-promoting-friction-ahead-of-israeli-election/#:~:text=Twitter%20has%20removed%20a%20network,of%20the%20November%201%20elections.

Steinberg, J. (2023, October 9th). U2's Bono pays tribute to 'beautiful kids' slain at Israeli desert rave. Retrieved from The Times of Israel: https://www.timesofisrael.com/u2s-bono-pays-tribute-to-beautiful-kids-slain-in-israeli-desert-rave/

Watts, C. (2024, February 6th). Iran accelerates cyber ops against Israel from a chaotic start. Retrieved from Microsoft: https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/

Yadid, B. (2023, March 10). Arab Media Highlights the "Curse of Israel's 8th Decade". Retrieved from Israel Today: https://www.israeltoday.co.il/read/arab-media-highlights-the-curse-of-israels-8th-decade/