

Influence Under Fire: Mapping Wartime Information Operations in the Middle East, 2023–2025

By Tamar Mitts and Eden Kaduri



IGP Institute of
Global Politics

CONTENTS

Executive Summary	2
Introduction	4
A Framework for Understanding Wartime Information Operations	6
Who Is Behind the Operation?	6
What Are Their Goals and Who Are They Targeting?	7
Where Are They Operating?	7
How Are They Seeking to Influence Their Target Audience?	7
Mapping the Information War	9
The Actors and Their Operations	14
Israel's Wartime Influence Efforts	14
Hamas's Influence Campaigns	17
Iran's Digital Operations	20
Influence Operations by Hezbollah and the Houthis	23
Hezbollah	23
The Houthis	24
A Case in Focus: Online Influence Amid the Israel-Iran Escalation of June 2025	26
1. Competing Claims of Victimhood and Legitimacy	26
2. Your Leadership Is Against You: Operations Aimed at the Adversary's Public	28
3. Efforts to Intimidate and Demoralize	30
Conclusion: Lessons from the Information Front	33
Appendix	36
Data Collection Methodology	36
Campaign-Level Dataset of Reported Operations	36
Post-Level Social Media Dataset	37
Detecting AI-Generated Multimedia	38
Additional Results	40
Endnotes	41
About the Authors	50

© 2026 Institute of Global Politics (IGP)

The findings, interpretations, and conclusions expressed in this publication are entirely those of the author(s) and do not necessarily reflect the views of the Institute, its leadership, Columbia University, or the School of International and Public Affairs (SIPA). Any external support for this research did not influence its content.

Influence Under Fire: Mapping Wartime Information Operations in the Middle East, 2023–2025

Tamar Mitts and Eden Kaduri
Columbia University
October 2026

We thank Matthew Francis, Camille Francois, Joshua Goldstein, Kevin Greene, Martin Innes, Erica Loneragan, David Rogers, Jacob Shapiro, and Laura Smith for their terrific comments. We also thank Eden Cohen, Ian Kearns, Christine McNeill, Brian Andres Palacios Paz, Ethan Sheinker, and Elizabeth Yee for their research assistance. This report was partially funded by the Department of Defense Minerva BARI Grant, “Influence, Manipulation, and Information Threats as Adversarial Techniques: Events, Evolution, and Effects.”

EXECUTIVE SUMMARY

Information operations have become increasingly embedded in the conduct of modern warfare. Digital platforms now give armed actors a way to narrate conflict in real time, shape how different audiences understand violence, and influence the political pressures surrounding the use of force. The information space has therefore become a central venue where conflict actors try to justify their actions, weaken adversaries, mobilize supporters, and shape the constraints under which war is fought.

This report examines these dynamics through the Gaza war and its regional spillovers between January 2023 and August 2025, focusing on influence activity linked to Israel, Hamas, Iran, Hezbollah, and the Houthis. Drawing on an original dataset of 291 publicly reported information operations and cyber operations, alongside a cross-platform dataset of more than 1.7 million social media posts linked to the principal actors in the conflict, the report maps wartime influence campaigns through a common framework focused on actors, target audiences, strategic goals, and methods of influence. The data captures publicly documented activity and provides evidence of the visible information war. What enters the public record depends on what journalists, cybersecurity firms, platforms, governments, NGOs, and open-source researchers are able to detect and disclose. This approach provides a systematic view of how influence operations evolved across the conflict and how they related to broader wartime strategy.

Several patterns stand out. First, documented online influence activity expanded sharply as the conflict intensified, with visible surges after October 7, 2023, and again during the June 2025 Israel–Iran confrontation. Second, these campaigns were often directed at specific audiences. Messaging aimed at enemy publics frequently sought to intimidate, demoralize, or drive wedges between civilians and political leadership, while messaging aimed at international audiences more often sought to garner sympathy, shape media coverage, and apply external pressure. Third, information operations and cyber activity were often connected in practice, despite often being conceptualized as analytically distinct. Hacks, leaks, spoofed alerts, impersonation, official messaging, proxy amplification, and AI-generated media were often folded into broader efforts to shape perceptions.

The June 2025 Israel–Iran escalation illustrates these dynamics especially clearly. Both sides moved quickly to frame the conflict in terms of victimhood, legitimacy, and self-defense. Both targeted the adversary’s public with messages designed to undermine confidence in political leadership. Both paired cyber activity and threats with dramatic visual content, including synthetic or manipulated media. The episode showed how quickly wartime influence campaigns can be deployed during a fast-moving military crisis, and how closely they can track events on the battlefield.

The report shows how the struggle to shape narratives has become a regular feature of contemporary conflict. The Middle East is the empirical focus here, but the broader development is not unique to this case. Modern wars increasingly unfold in an environment in which coercion, diplomacy, cyber activity, and information campaigns are closely intertwined. This creates a growing policy gap. The cross-platform, multilingual, conflict-sensitive monitoring capacity needed to understand wartime influence operations is ever more difficult to sustain, even as these campaigns become more frequent

and complex. Platforms also need policies that are better tailored to armed-conflict conditions, including real-time response capacity, specific rules for labeling, limiting, or removing synthetic media, and more transparent standards for official, semi-official, and proxy accounts during war.

This report does not settle the question of how effective these campaigns are in changing beliefs or behavior. It does show that they have become a recurrent and strategic part of warfare. Understanding contemporary conflict therefore requires taking seriously the contest over how war is interpreted across audiences, and building the institutional capacity to study and respond to that contest as it unfolds.

INTRODUCTION

Modern warfare is not confined to the exchange of firepower on the battlefield. It is also fought, sometimes just as fiercely, in the contest to shape perceptions and legitimacy. As a result, the information space has become a widely contested battle space. Political leaders, militaries, and armed groups now treat social media and digital platforms as a central front in conflict, with events unfolding simultaneously on the ground and across global social media feeds.

A large part of this shift is the result of changes in how information is captured and shared. Never before have there been so many cameras in the hands of so many participants and observers. The prevalence of smartphones, internet connectivity, and social media platforms means that nearly every act of war can be recorded and shared within seconds. In earlier eras, governments could more effectively control or censor what the public saw from the battlefield; information that reached external audiences was often filtered through official communiqués and news agencies. But in modern conflicts, that monopoly has eroded. In its place is a radically more transparent but also more saturated information environment, crowded with competing narratives from state governments, militant groups, civilians, and a range of informal online actors.¹

For parties involved in these conflicts, this visibility has become a strategic tool. Combatants now publicize their own operations, sometimes in real time, in order to intimidate enemies or rally supporters. They coordinate messaging campaigns to undermine opponents' credibility or sow confusion. They tailor messaging to different audiences, such as domestic constituencies, adversary populations, or international audiences, and distribute it through both overt media channels and covert online networks. In effect, they are fighting on multiple fronts at once: on the ground, in cyberspace, and—through both—in the minds of the audiences whose perceptions they hope to shape.

Nowhere have these dynamics been more visible than in the conflicts that unfolded across the Middle East between 2023 and 2025, beginning with the war in Gaza and expanding into a broader confrontation between Israel and the “Axis of Resistance”—Iran, Hamas, Hezbollah, and the Houthis. Influence operations among these actors are not new; they have long been part of the region's political and military maneuvering. But since the Hamas-led attack on Israel on October 7, 2023, and the escalation that followed across multiple theaters, these campaigns have intensified in sophistication and reach. They have become a central feature of how the conflict has been interpreted and contested by publics on all sides.

This report examines these operations in depth. It offers a structured framework for understanding how influence campaigns are conducted during wartime, mapping the key actors involved, their strategic objectives, the audiences they target, the arenas in which they operate, and the tactics they employ. Existing reporting has documented many individual influence campaigns in these conflicts, often in considerable detail. Journalists and investigators have uncovered specific networks, incidents, and tactics used by different actors.² But this work is necessarily fragmented: It tends to focus on particular episodes or single actors and thus does not offer a systematic account of how information operations evolved across the broader regional conflict over time. One of this report's central contributions is to bring these efforts into a common analytic frame, which allows us to compare how

multiple actors used information operations to target audiences across various phases of the conflict.

We adopt a broader lens than formal government communications and official media statements, which typically reflect only a small segment of the influence activity surrounding armed conflict. Instead, we include campaigns carried out by networks that support an actor's agenda, whether they are operating overtly or through more covert means. These may include affiliated media outlets, cyber units, and networks of sympathizers that consistently amplify an actor's messaging. Cyber and influence operations do not always travel together. Some remain analytically distinct; others are tightly fused, with hacks, leaks, or service disruptions folded into broader information campaigns to shape perceptions and behavior. We distinguish between such coordinated efforts and the spontaneous activity of individual users. Although any social media user who shares or reacts to content may, in some sense, participate in an information campaign, our analysis focuses on organized operations—those that exhibit some degree of coordination, repetition, or strategic intent. Attribution is not the primary basis for inclusion in our analysis; indeed, many of the most high-impact campaigns blur the lines between state-run operations and deniable proxies.³ When attribution can be established with confidence—for example, in the case of official accounts or clearly affiliated networks—we note it and treat it as substantively meaningful. But for analytical clarity, we focus on the structure and content of campaigns themselves, not on resolving authorship in every case.

We focus on campaigns directed at international audiences and the populations of direct adversaries. For the actors involved in this conflict, these audiences often carry important strategic priority: Enemy populations are key targets for efforts to erode morale, sow division, or undermine political leadership, while international audiences can shape outcomes through diplomatic pressure or shifts in global opinion. Although domestic populations are an important part of the broader influence ecosystem, we give them less attention here, as tracking domestic influence is more difficult to do empirically. For instance, nearly all domestic news broadcasts could, in principle, serve as vehicles of influence, making it difficult to distinguish specific campaigns from routine media activity. Including them would risk overshadowing the cross-border operations that are the central focus of this report. We thus pinpoint our attention on enemy and international audiences, where it is easier to observe influence efforts.

The sections that follow proceed in four steps. First, we introduce a conceptual framework that categorizes influence operations in armed conflict by their key components: actors, objectives, target audiences, operational arenas, and tactics, which provides a basis for systematic comparison across cases. Second, we provide a bird's-eye view of campaigns conducted between January 2023 and August 2025, mapping them according to our framework. Third, we turn to detailed descriptions of each actor's operations to illustrate patterns and innovations. Finally, we focus on a case study, the June 2025 escalation between Israel and Iran, in which the information war unfolded alongside kinetic exchanges in ways that illuminate both the possibilities and the limits of contemporary influence strategies.

Our goal is not to adjudicate the legitimacy of any actor's claims, but rather to document and analyze how information operations function as a feature of modern warfare. In doing so, we hope to paint a clearer picture of how the struggle for narrative control intersects with the physical conduct of war, and to lay the groundwork for future research on the effectiveness, or limitations, of these campaigns in achieving their intended outcomes.

A FRAMEWORK FOR UNDERSTANDING WARTIME INFORMATION OPERATIONS

If the information space is now a central front in warfare, then its “terrain” is measured not in square miles but in audiences. Influence operations are designed to reach these audiences, shape what they see, and ultimately condition what they do. The framework we use in this report maps this battle space by focusing on three broad audience categories: domestic, adversary, and international, and the distinct objectives that actors pursue with each (Figure 1). Our framework structures each case around four questions: who is conducting the operation, what their goals are and who they are targeting, where they are operating, and how they seek to influence their target audiences.

If the information space is now a central front in warfare, then its ‘terrain’ is measured not in square miles but in audiences.

This approach builds on existing frameworks for the study of information operations, but adapts them to the wartime context. Frameworks such as DISARM have helped standardize the description of tactics, techniques, and procedures, while the ABC and ABCDE approaches help separate questions about actors, behavior, content, distribution, and effects.⁴ We draw on these insights, but place greater emphasis on how influence operations function within an ongoing conflict. In wartime, the analytic question is not only what tactic was used or whether a message was deceptive. It is also which audience the operation sought to reach; what perception or constraint it attempted to shape; how it related to battlefield developments; and whether official messaging, proxy activity, cyber operations, and synthetic media were operating together. The four-question schema used here is therefore helpful for identifying how individual campaigns fit into broader military and political strategy. We briefly explain each dimension below.

WHO IS BEHIND THE OPERATION?

Armed conflicts today feature a wide range of actors conducting information campaigns: state militaries, intelligence agencies, political leaders, armed groups, and affiliated networks of activists, propagandists, or covert online operatives. Identifying the actor is a matter of attribution, as well as a matter of anchoring the campaign in its institutional and political context. Whether acting overtly or covertly, directly or through intermediaries, different actors bring distinct capacities and styles to the information space.

WHAT ARE THEIR GOALS AND WHO ARE THEY TARGETING?

No campaign is audience neutral. Messaging is crafted with a specific public in mind, whether it is the domestic population whose resilience and support are vital to sustaining the war effort, the enemy population whose morale or cohesion the actor seeks to weaken, or the broader international community whose perceptions can influence diplomatic, economic, or military interventions.⁵ Goals can vary widely, even within the same audience category, and may include intimidating opponents, boosting morale, polarizing rival factions, mobilizing protests, or generating sympathy abroad.⁶ Understanding the intended audience and the strategic goal helps us better understand the political and military function of the campaign.

WHERE ARE THEY OPERATING?

The “where” of information operations refers not only to physical geography but also to the arenas (online, offline, or hybrid) through which actors seek to shape perceptions and behavior. Operations may unfold in highly visible digital channels such as social media or television; in the physical world, where information might be transmitted by dropping leaflets or hacking billboards; or in a hybrid format, where on-the-ground influence efforts are amplified online to reach broader audiences.⁷ Identifying the arena in which a campaign is conducted helps clarify its intended reach and the speed at which messages can circulate. In this report, our focus is on the online sphere, and primarily on social media.

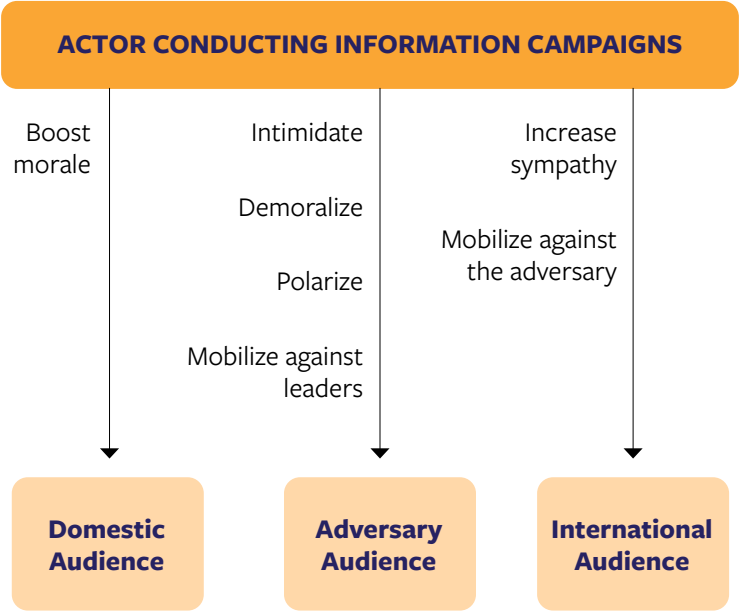
HOW ARE THEY SEEKING TO INFLUENCE THEIR TARGET AUDIENCE?

The “how” captures the range of methods used to shape perceptions and behavior. This includes what messages are conveyed, how they are framed, and how they are distributed (often referred to as the analysis of tactics, techniques, and procedures).⁸ Combatants may deploy overt messaging campaigns such as speeches delivered through official channels to shape audience perceptions, or may rely on more covert operations, such as the use of inauthentic accounts or false-front media outlets, to obscure their involvement. They may also use other types of cyber operations, such as denial-of-service attacks or database breaches, to intimidate audiences or demonstrate technological capacity.⁹ What distinguishes these tactics is their mode of delivery and their alignment with specific strategic aims. Although the same method—a video, a hack, an inauthentic account—can be deployed through different channels, its function varies with its target and objective. Analyzing the “how” thus helps reveal how different methods are adapted to serve specific ends in specific contexts.

By breaking each campaign down along these dimensions, our framework provides a common analytic language for comparing operations across actors and over time. It helps identify patterns, such as recurring tactics targeting particular audiences, or shifts in operational arenas during different phases

of the conflict, and helps us ground the examples that follow, which offer details on the influence efforts of Israel, Iran, Hamas, Hezbollah, and the Houthis. The framework thus brings structure to what might otherwise appear as a tangle of disconnected incidents and offers a clearer view of how the struggle over narratives unfolds alongside the physical conduct of war.

Figure 1: Conceptual Framework for Analyzing Wartime Information Operations



MAPPING THE INFORMATION WAR

We begin with a systematic analysis of online influence operations conducted during the recent period of escalating conflict in the Middle East. Our objective is to trace how these operations evolved over time, in terms of both frequency and strategic intent, and how they responded to various developments in the war. The dataset spans from January 2023, through Hamas's October 7, 2023, attack on Israel, and to August 2025, shortly after the direct confrontation between Israel and Iran in June 2025.

This two-and-a-half-year period witnessed a dramatic expansion of regional conflict. The Hamas-led assault on October 7, 2023, resulted in the deaths of more than 1,200 people in Israel and triggered a large-scale military campaign in Gaza.¹⁰ By the summer of 2024, over 71,000 Palestinians had been killed, and much of Gaza's infrastructure lay in ruins.¹¹ The conflict gradually spilled into Lebanon and Yemen, with Hezbollah and the Houthis launching attacks and engaging in parallel information campaigns. In June 2025, Israel and Iran entered the third round (and by far the most intense round of the study period) of direct confrontation, in a series of escalations. The information war during this phase expanded in volume, sophistication, and reach, with digital campaigns operating at a scale and intensity that represented a quantitative leap in the region's information warfare.

To analyze how these events unfolded in the digital domain, we compiled two complementary datasets. The first is a campaign-level dataset of publicly reported information and cyber operations during this period, based on open-source intelligence investigations, publications, and media reports. Each observation in this dataset is a distinct reported campaign or incident, which might involve multiple accounts, posts, or platforms. For each campaign, we recorded the date of its execution or reporting, the actor responsible, the intended audience, and the specific tactics employed to influence that audience. We define *information operations* as coordinated efforts by state or non-state actors to shape public opinion through digital media. *Cyber operations*, by contrast, refers to technical interventions aimed at compromising information systems, such as hacks, leaks, espionage, or infrastructure disruption, that might or might not be coupled with messaging campaigns.¹²

Within this framework, campaign tactics were coded according to their operational goal—for example, intimidation, polarization, or mobilization against the enemy—and their delivery method (see Figure 2). These methods were categorized into overt media campaigns (such as public statements by leaders), covert media campaigns (such as coordinated networks that impersonate the target audience using sock-puppet accounts), and cyberattacks designed to disrupt infrastructure or steal information. In total, we identified and coded 291 distinct operations during this period.

The data captures publicly visible and publicly reported operations during the conflict. It should therefore be treated as a record of documented activity, not as a complete census of all influence efforts. What enters the dataset depends on the sources available to identify and disclose campaigns: journalists, cybersecurity firms, platforms, governments, NGOs, and open-source researchers. Those sources vary in their access, the languages and media environments they are able to monitor, technical capacity, and disclosure practices, which means that the public record is likely uneven. Some operations leave clearer traces than others. Campaigns reported through platform takedowns, government statements, threat-intelligence reports, or cybersecurity investigations are easier to document than

campaigns that circulate through closed groups, temporary accounts, proxy channels, or local media environments. The patterns below should therefore be interpreted as patterns in the visible and documented information war. They show where online influence activity could be identified and coded with sufficient confidence, while likely understating activity in less observable arenas. The data we collected [can be accessed here](#).

To complement the campaign-level dataset, we also collected a second dataset that captures the content of social media posts disseminated by official and unofficial networks affiliated with the five principal actors: Iran, Israel, Hamas,¹³ Hezbollah, and the Houthis. This collection includes more than 1.7 million posts on Facebook, Instagram, Telegram, TikTok, X, and YouTube. We use this data to analyze the narratives and messaging strategies deployed by these actors over the course of the conflict. Table 1 summarizes the number of accounts and their posts by actor. The Appendix provides more details on the data collection.

Figure 2: Campaign Tactics Broken Down by Delivery Methods and Operational Goals

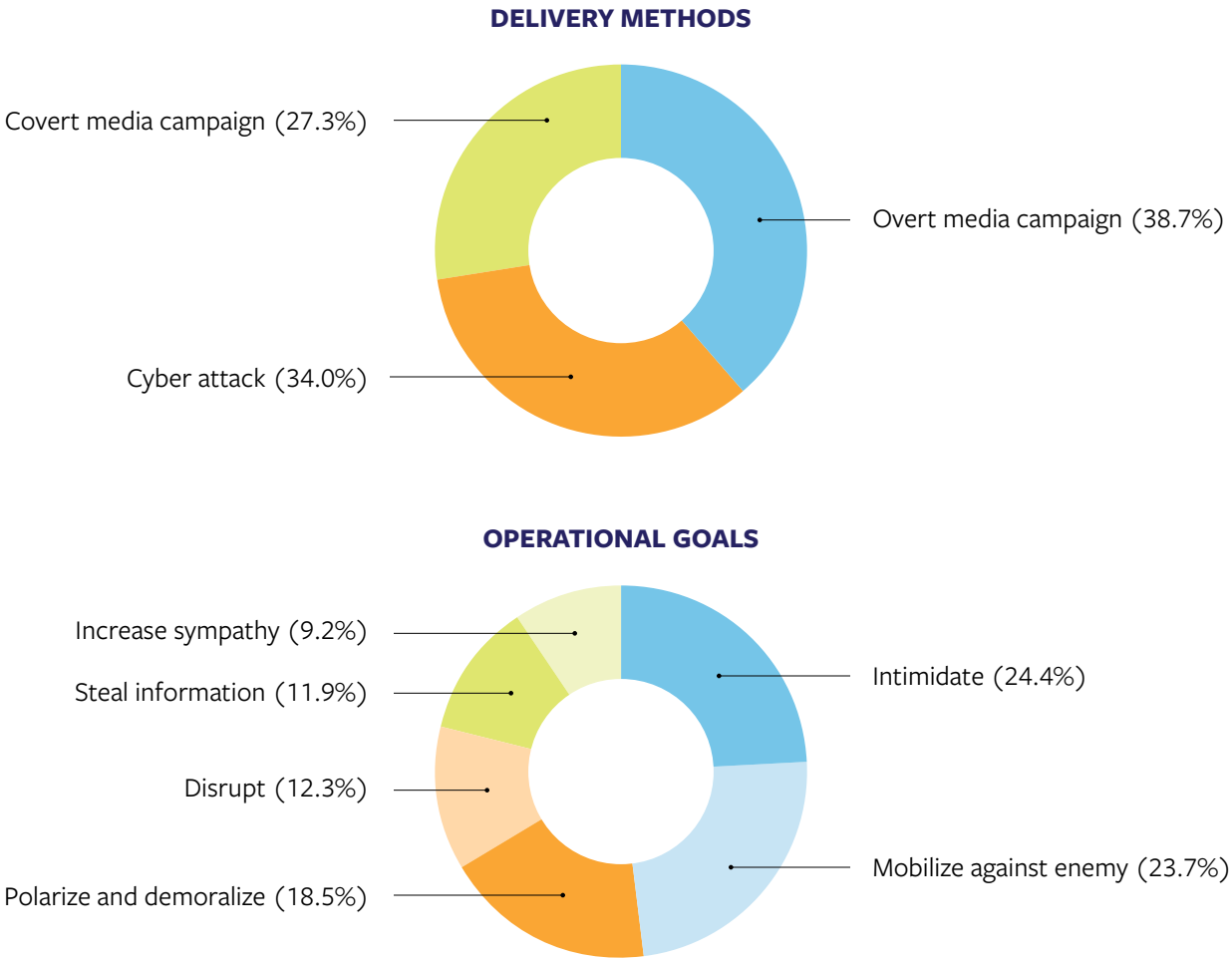


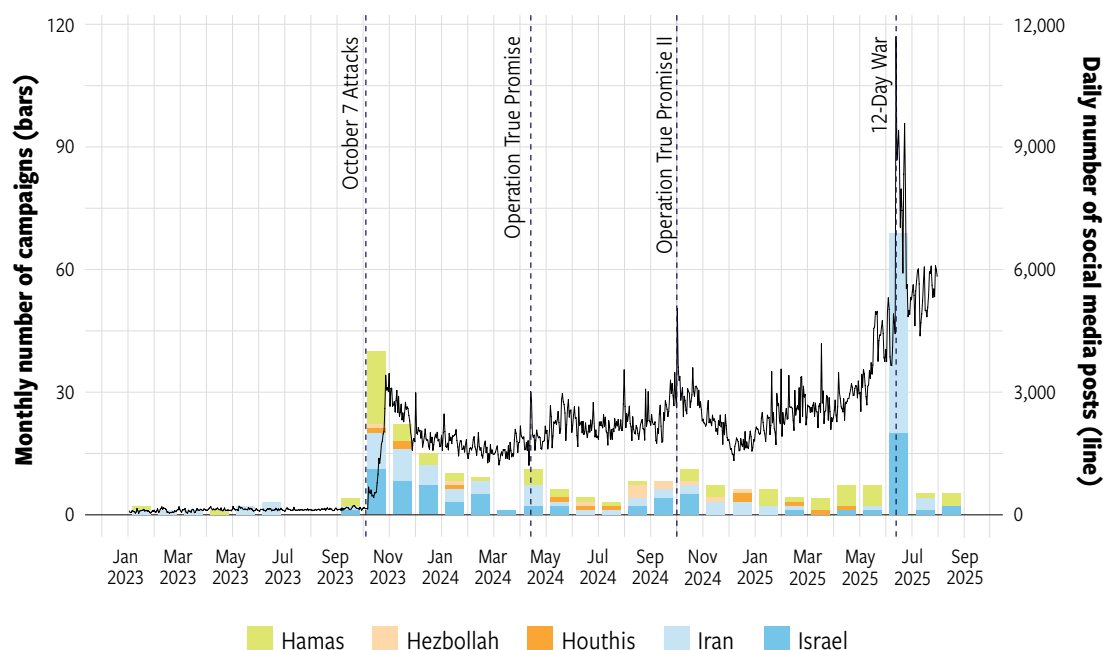
Table 1: Number of Accounts and Posts by Actor

Actor	Accounts	Posts
Iran	120	406,750
Israel	97	182,448
Hamas	42	1,024,229
Hezbollah	32	149,369
Houthis	14	18,443

Figure 3 shows trends in influence operations during our study period. The bars represent the number of campaigns launched each month (left y-axis), disaggregated by the actor whose narrative they promoted, and the line shows the daily volume of posts (right y-axis) from accounts affiliated with or supportive of these actors. We find several notable patterns. First, both data sources show a sharp increase in online influence operations after October 7, 2023. Although activity was present before then, averaging about 3.5 reported campaigns per month and roughly 100 posts per day, it rose dramatically after that date. In October 2023 alone, we identified 38 different online influence campaigns launched by Israel, Hamas, Iran, Hezbollah, and the Houthis or networks supporting them, and nearly 40,000 posts disseminated by affiliated accounts across multiple platforms (Figure C1 in the Appendix shows the volume of posts by actor).

Second, we find that all actors have been active in trying to influence other publics throughout the period, but campaigns by Hamas, Iran, and Israel have been the most prevalent. Third, the activity of Israel and Iran surged during the June 2025 escalation—the “12-Day War”—when the two sides launched over 65 distinct influence operations and promoted an unprecedented volume of social media content.

Figure 3: Trends in Information and Cyber Operations During the Conflict



Bars (left axis): monthly operations by actor (covert activities, cyber attacks, social media campaigns).

Line (right axis): daily posts by affiliated networks.

Sources: reports, publications, open-source investigations, and social media data.

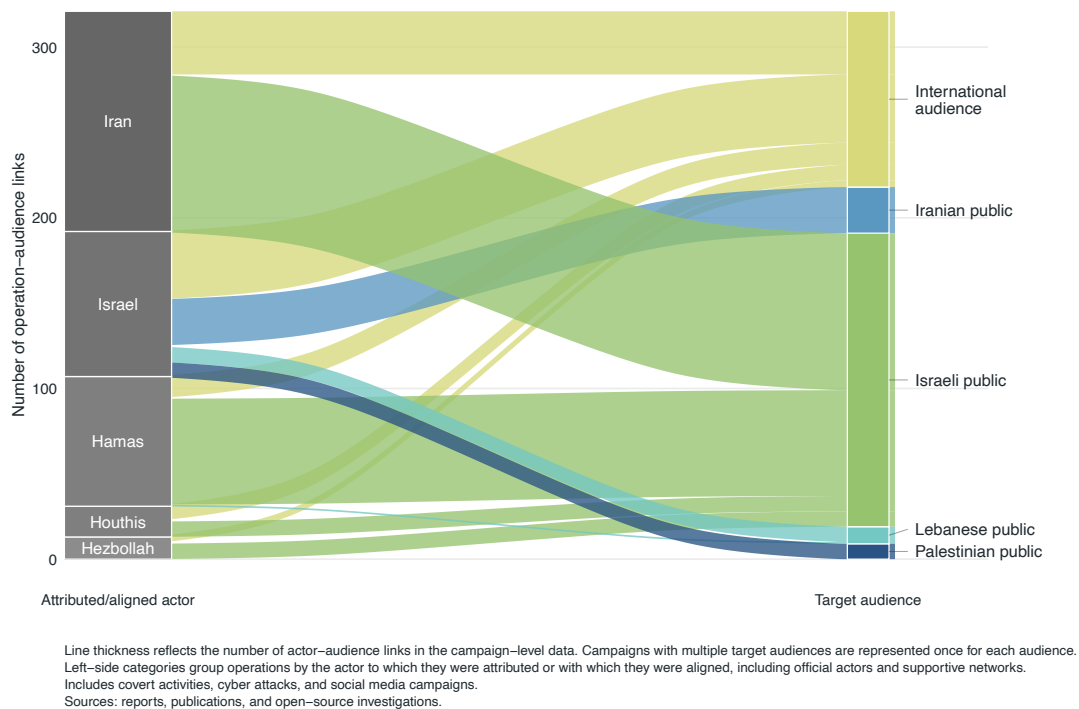
In Figure 4, we illustrate patterns of who targeted whom during this period, focusing only on cross-border campaigns. The figure groups campaigns by their origin—meaning the actor to which they were attributed or with which they were aligned—on the left, and by their target audience on the right, with connecting lines proportional to the volume of activity. In the publicly reported campaign record, the Israeli public appears as the most frequent target, especially with operations linked to Iran and Hamas. Among coded goals in campaigns targeting Israelis, the most common were intimidation (27 percent), demoralization (23 percent), and efforts to mobilize against the Israeli government (22 percent). Disruption and information theft, which were often associated with cyber operations, together accounted for another 26 percent.

The second most common target was the international audience, which all actors sought to influence. Campaigns directed abroad most often sought to mobilize opposition to an enemy (35 percent) or increase sympathy for one's side (24 percent). Campaigns targeting Iranian, Lebanese, and Palestinian publics were less common in public reporting and originated primarily from Israel or pro-Israeli networks. These campaigns were most often coded as efforts to intimidate, disrupt, steal information, or mobilize opposition to adversary leaders.

The limits of a publicly reported campaign-level dataset are especially important for this comparison across target audiences. The large number of campaigns targeting Israelis reflects the visibility of those campaigns in the documented record; it may also reflect differences in what public sources

made visible. Similarly, the smaller number of documented campaigns targeting Iranian, Lebanese, and Palestinian publics should be interpreted cautiously as an indicator of fewer existing campaigns, because operations directed at those audiences may have been less reported on or harder to verify using public sources. Figure 4 also excludes domestic propaganda and purely offline influence efforts, such as leaflet drops by the Israel Defense Forces (IDF) in Gaza, which have long been part of wartime communication. Even with these limitations, however, the broader trend is clear: Documented online influence operations expanded sharply after the start of the Gaza war and surged again during the June 2025 Israel–Iran escalation. This makes it important to examine these campaigns more closely, both in their individual execution and in the broader patterns they reveal.

Figure 4: Who Targets Whom with Information Operations and Cyber Operations



THE ACTORS AND THEIR OPERATIONS

Building on the framework and descriptive patterns outlined above, we now turn to the five main actors in this conflict—Israel, Hamas, Iran, Hezbollah, and the Houthis—and examine how each engaged in cross-border information operations. The discussion draws on the campaign and social media datasets introduced above, using specific examples to illustrate broader patterns in each actor’s messaging and tactics. Although their strategies varied in scale and sophistication, all five used digital tools in an effort to intimidate adversaries, shape international perception, and reinforce their broader wartime goals. These campaigns drew on a diverse mix of tactics, including official messaging, covert impersonation networks, cyberattacks, and the circulation of battlefield footage, adapted to the narrative and operational needs of each actor.

ISRAEL’S WARTIME INFLUENCE EFFORTS

From the earliest days of the conflict, Israel’s messaging was shaped by two central objectives: to consolidate international support for its military campaign and to erode the morale and cohesion of its adversaries. These goals were pursued through a constellation of media and government offices, including the prime minister’s office, the IDF spokesperson’s unit, the Ministry of Foreign Affairs, and affiliated diplomatic and cyber teams, as well as looser networks of unofficial accounts aligned with the Israeli side. Messaging was calibrated to different audiences and disseminated in Arabic, Hebrew, English, and Persian, using a mix of official and unofficial content, and covert influence campaigns.

To **international audiences**, Israel’s messaging focused on efforts to frame its military campaign in Gaza as morally justified and conducted in accordance with international law. This imperative took on particular urgency as global media coverage increasingly highlighted the humanitarian toll of the war. In response, Israeli officials and affiliated media outlets adopted a narrative structure that highlighted the brutality of Hamas, portrayed Palestinian suffering as either staged or manipulated, and emphasized Israeli efforts to minimize harm to civilians.¹⁴

A centerpiece of this campaign was the production and international screening of *Bearing Witness to the October 7th Massacre*, a 47-minute compilation of footage documenting Hamas’s attacks on civilians.¹⁵ The film, shown to diplomats, journalists around the world, and Hollywood executives, was designed not only to document atrocities but to situate Israel’s military response within the broader narrative of the global war on terror. The rhetorical equation of “Hamas is ISIS” often served as the backbone of this messaging strategy, linking Israel’s actions to a familiar moral framework and attempting to forestall criticism by placing the conflict within a shared security lexicon.¹⁶

At the same time, Israeli messaging worked to discredit visual evidence of civilian casualties in Gaza (see Figure 5). Accusations that such documentation was fabricated (a trope widely referred to as “Pallywood”) were circulated by official spokespeople and media allies.¹⁷ Content also sought to showcase the ideological threat posed by Hamas. In one instance, the IDF reported discovering an annotated copy of *Mein Kampf* in a child’s bedroom in Gaza,¹⁸ a detail emphasized in Hebrew-language and

English-language outlets as emblematic of the group's ideological extremism.¹⁹ These narratives did not explicitly deny the existence of civilian suffering, but seem to have sought to reframe its meaning as either the result of Hamas's tactics, or an unreliable signal shaped by manipulation and propaganda.

A related strand of messaging focused on Israel's efforts to comply with international law, often framed through references to civilian protection. Israeli officials repeatedly emphasized that adversaries had embedded military infrastructure in civilian areas, leaving Israel with no choice but to strike targets that would inevitably do collateral damage.²⁰ These claims were supported with visual evidence drawn from military operations: intercepted phone calls allegedly revealing the misuse of ambulances,²¹ videos of tunnels beneath hospitals,²² and satellite images identifying Hamas and Hezbollah positions near schools and mosques.²³ Such materials were disseminated in multiple languages, including Arabic and Persian, and served to frame Israeli strikes as acts of military necessity.

In tandem, Israeli messaging campaigns employed direct-to-civilian communication that also seemed to function as a public signal of restraint in Israel's military conduct. On October 9, 2023, for example, the IDF spokesperson posted in Arabic urging Gaza residents to evacuate areas expected to see ground operations.²⁴ These warnings were repeated in subsequent weeks via various media outlets, and could be read as part of a broader effort to present Israel as taking steps to reduce civilian harm. At the same time, Israeli channels accused Hamas of blocking civilian evacuations, reinforcing a recurring theme in Israeli communications that Hamas bore responsibility for civilian casualties in Gaza.²⁵

Beyond official messaging, networks supporting the Israeli side also engaged in covert online influence operations that targeted global publics—especially in the United States. In June 2024, for example, reporting revealed that Meta and OpenAI uncovered a campaign run by STOIC, a Tel Aviv-based political marketing firm, which launched shortly after October 7, 2023. The campaign deployed more than 160 fake and AI-generated accounts impersonating Jewish students, Black Americans, and concerned citizens.²⁶ These accounts posted pro-Israel content, discredited campus protests, and criticized the United Nations Relief and Works Agency (UNRWA), the UN body responsible for humanitarian aid and services in Gaza.²⁷ Although it was difficult to trace with precision, *The New York Times* reported that the campaign was carried out at the direction of Israel's Ministry of Diaspora Affairs and targeted Democratic lawmakers in an effort to bolster support for Israel's military campaign and promote pro-Israel messaging through inauthentic accounts on social media.²⁸

In addition to global audiences, Israel targeted **enemy publics** with messaging intended to intimidate, often carrying implicit signals for enemy leaders. These campaigns relied on visible demonstrations of military capability and operational reach. Following high-profile assassinations of senior Hamas figures, for instance, Israeli officials released statements and imagery to Arabic-language channels emphasizing the IDF's ability to strike operatives wherever they were located.²⁹ After a July 2024 strike that killed Hamas commander Mohammed Deif, Prime Minister Netanyahu warned that “all of Hamas's leaders are marked for death,” a statement repeated across various platforms.³⁰

Operational demonstrations reinforced this intimidation strategy. One of the most dramatic, and widely reported, examples occurred on September 17, 2024, when hundreds of pagers distributed to Hezbollah operatives across Lebanon and Syria exploded nearly simultaneously. Prime Minister Netanyahu officially claimed responsibility for the operation two months after its occurrence.³¹

Hezbollah reported substantial casualties, including fighters, civilians, and the Iranian ambassador to Lebanon, while Lebanese officials confirmed the death toll and injuries. In a statement, Hezbollah's leader vowed to retaliate against Israel; this was followed by a period of intensified rocket fire by the organization.³² Reporting and expert commentary emphasized that the operation was intended both to degrade Hezbollah's operational capacity and to demonstrate Israel's ability to infiltrate secure supply chains and internal communications.³³

Israel also sought to drive wedges between enemy leaders and the broader publics they claimed to represent. These campaigns combined direct appeals from Israeli officials with other messages that sought to encourage civilians to question the motives of the Iranian regime, Hamas, and Hezbollah.

Targeting the Iranian public. In multiple speeches, Prime Minister Netanyahu addressed the Iranian public directly (sometimes in Persian), voicing support for anti-regime protesters and blaming the Islamic Republic for the Gaza war and broader regional instability.³⁴ He repeatedly emphasized that Israel's conflict was with the regime, not the people, asserting that "the day of your liberation is close," and suggesting that Iran could even join the Abraham Accords "if the people rise."³⁵ Other Israeli officials amplified these messages, framing Israel as an ally of the Iranian people in their struggle against repression. These efforts invoked widely recognized symbols of dissent, such as the Woman, Life, Freedom movement,³⁶ and sought to portray Supreme Leader Ali Khamenei as a "bloodthirsty dictator" and the Islamic Republic as a "murderous regime" that oppresses its own citizens.³⁷

Messaging aimed at Lebanese and Palestinian publics. Similar influence efforts targeted Lebanese and Palestinian civilians. In August 2024, for instance, media outlets reported that an Israeli drone flew over southern Lebanon broadcasting Arabic-language messages through a loudspeaker, urging residents to "turn against Hezbollah" and blaming the group for the attacks on southern Lebanon.³⁸ In Gaza, Israel dropped thousands of leaflets seeking to undermine Hamas's authority and encouraging civilian cooperation. Some urged residents to turn against Hamas and inform on its members,³⁹ while others offered financial incentives or mocked Hamas leaders for living in comfort while Gazans suffered.⁴⁰

Figure 5: Israeli Official Messaging Targeting International Audiences

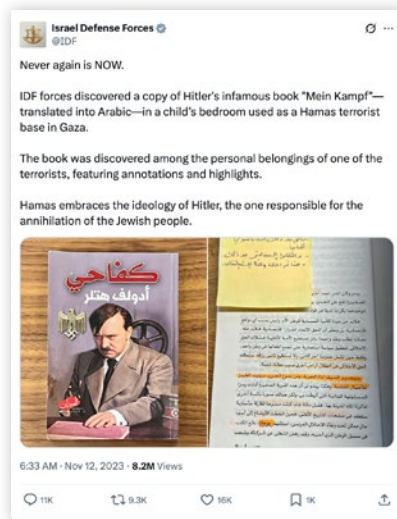
**A) FRAMING
HAMAS AS ISIS**



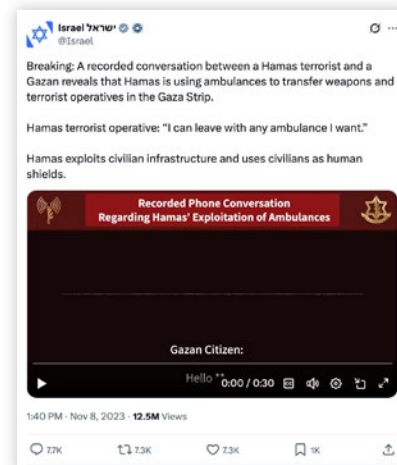
B) PALLYWOOD POST



**C) DISCOVERING
MEIN KAMPF IN GAZA**



**D) EXPLOITING CIVILIAN
INFRASTRUCTURE**



HAMAS'S INFLUENCE CAMPAIGNS

Hamas, like Israel, treated the online information ecosystem as an extension of the battlefield. But whereas Israel relied on a large institutional apparatus spanning government ministries, military spokesperson units, and diplomatic channels, Hamas's strategy leaned heavily on semi-official outlets and social media-based unofficial networks. Across these channels, Hamas pursued two main goals: to intimidate and demoralize the Israeli public, and to increase global sympathy for its cause. These efforts escalated rapidly after October 7, 2023, and evolved in tandem with developments on the ground.

Toward **Israeli publics**, Hamas's first major information effort unfolded in the opening stages of the October 7 attack. Many militants carried helmet-mounted cameras or recorded footage on mobile

devices that captured first-person videos of the breach of the border, the attacks on civilians, and the abduction of hostages. These materials were posted to Hamas-linked Telegram channels within minutes and circulated widely on other platforms.⁴¹ In some cases, Hamas fighters used victims' own Facebook, Instagram, and WhatsApp accounts to post graphic content or livestreams.⁴² While the footage later figured prominently in Hamas's international messaging, its initial impact seemed to have been directed at Israeli audiences. The images highlighted the scale of the security failure and the penetration of civilian areas, and helped shape the informational context in which Israelis first encountered the attack.⁴³

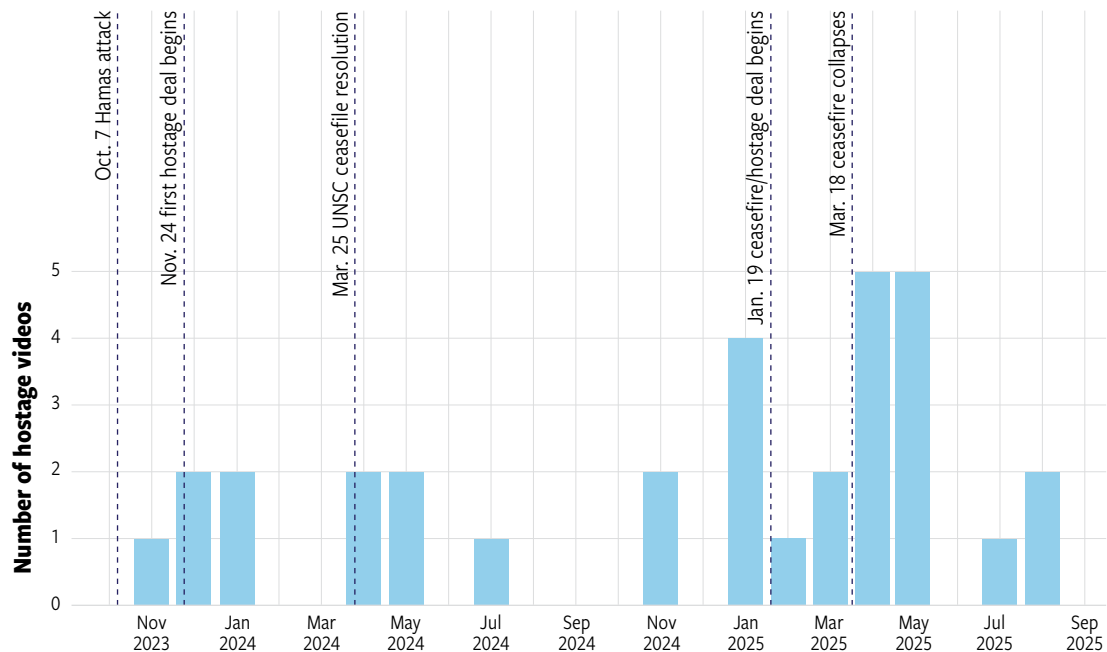
In addition to footage from the attack, Hamas activists and supporters targeted the Israeli public with a wave of cyberattacks that appeared designed to intimidate. Shortly after the attack, pro-Hamas hackers defaced or disrupted the websites of municipal governments, media outlets, and prominent institutions such as the Maccabi Tel Aviv basketball team, albeit for a short time.⁴⁴ In other Israeli towns, digital billboards were hijacked to display Palestinian flags and slogans in Hebrew, including "Palestine has returned and will be victorious."⁴⁵ A few weeks later, thousands of Israelis received text messages, emails, and links to counterfeit news websites designed to spread panic. Messages claimed, for example, that a power plant had been hit by Hamas's rockets, and urged people to take pills for protection against a "chemical incident."⁴⁶ In another case, a fake version of an Israeli news website was created to spread inauthentic headlines, such as "IDF Spokesperson: Chemical Population Alert in Dimona."⁴⁷ Indeed, cybersecurity firms monitoring Israeli websites reported sharp surges in malicious traffic during this period, with some sites experiencing attack volumes that reached into the millions of access requests per second.⁴⁸

But perhaps the most widely recognized component of Hamas's digital influence campaigns targeting the Israeli public involved the strategic release of hostage videos. Beginning within days of the attack, Hamas and its allied group Palestinian Islamic Jihad disseminated videos featuring Israeli hostages. The videos were typically filmed in confined spaces and varied in tone: Some included direct appeals to the Israeli government, while others showed visible signs of duress. Other clips included unverified claims that hostages had been killed during Israeli strikes.⁴⁹ Although the specific triggers for each release remain uncertain, reporting indicates that many videos were issued during moments of heightened political pressure inside Israel, often overlapping with periods of negotiation and public debate over the government's handling of the war.⁵⁰ Figure 6 shows the monthly number of hostage-video releases between October 7, 2023, and September 2025. It illustrates how Hamas sustained a steady stream of such content over nearly two years. These videos received wide coverage in Israeli and international media.⁵¹ The recurring release of these videos contributed to growing public pressure on Israeli leaders to reach a ceasefire with Hamas and became a focal point in debates about the government's priorities and conduct of the war.⁵²

Hamas's ability to disseminate these materials widely was amplified by its rapidly expanding digital footprint. The group's main Telegram channel, for example, more than tripled in followers within days of the attack, reaching over 670,000 subscribers by late October 2023.⁵³ That growth was interrupted on October 26, when Telegram suspended the account for violating its content guidelines.⁵⁴ In response, Hamas relied on a combination of surrogate accounts, reposting networks, and affiliated

media outlets to continue circulating its materials, often with slight modifications designed to evade platform moderation systems. One important node in this broader ecosystem was the Telegram channel Gaza Now, which the Atlantic Council’s DFRLab describes as “ Hamas aligned.” The channel consistently circulated Hamas-produced content throughout the war, including hostages videos filmed by the organization, while also expanding its own reach to more than 1.3 million subscribers. Because channels such as Gaza Now predated the war and presented themselves as news sources covering events in Gaza, they could lend a degree of legitimacy to Hamas-aligned content and help it circulate beyond explicitly branded Hamas channels.⁵⁵

Figure 6: Monthly Releases of Hamas Hostage Videos After October 7, 2023



Toward **international audiences**, Hamas’s digital messaging sought to frame the October 7 attacks as a historic act of resistance and to position the group as a national liberation movement and a disciplined military force confronting an occupying power.⁵⁶ The same first-person footage that alarmed Israeli viewers was used abroad to present the breach of Israeli defenses as a significant tactical achievement. These videos, disseminated across platforms like X, TikTok, and Instagram, were edited to emphasize the success and audacity of the operation and circulated widely due to their scale and graphic content.⁵⁷ The use of live footage, distributed almost immediately after the attacks, marked a shift from past conflicts. It allowed Hamas to seize control of the global narrative before traditional news outlets or Israeli authorities could respond, which may have helped shape how the operation was understood around the world.⁵⁸

Hamas's messaging, in addition to portraying military success, sought to frame the attackers as principled actors adhering to wartime norms. Some clips, for example, depicted Hamas fighters offering water to children or calming civilians, in an apparent attempt to sanitize the violence.⁵⁹ Online networks supporting Hamas sought to humanize the group by portraying the abduction of Israelis to Gaza Strip as a legitimate means of securing the release of Palestinian prisoners from Israeli jails. These claims referenced prior incidents of Israeli violence against worshippers at Al-Aqsa Mosque, framing it as the trigger for Hamas's attack.⁶⁰

As the war progressed and the humanitarian toll in Gaza mounted, Hamas's messaging pivoted toward emphasizing the scale of Israeli military retaliation. Social media channels affiliated with the group amplified images of bombed hospitals, displaced families, and wounded children.⁶¹ This approach built on a long-standing effort to present Hamas's violence internationally as resistance to occupation, and to shift external attention from terrorism to the legality and proportionality of Israel's conduct, including claims about civilian harm and war crimes.⁶² These themes became a dominant component of Hamas's international outreach in the following months, where they appeared consistently across its main Telegram channels and affiliated media accounts.

IRAN'S DIGITAL OPERATIONS

While Hamas focused on overt propaganda and Israel emphasized official narratives aimed at shaping international opinion, Iran often pursued a more covert strategy. Its operations frequently used inauthentic accounts, impersonation, and threatening cyber activity to bolster Hamas's campaign against Israel and position the Iranian regime as the regional vanguard of anti-Israel resistance. After October 2023, these efforts expanded in both scale and coordination, combining messaging from state-run and semi-official outlets with digital operations attributed to cyber actors linked to the Islamic Revolutionary Guard Corps (IRGC).

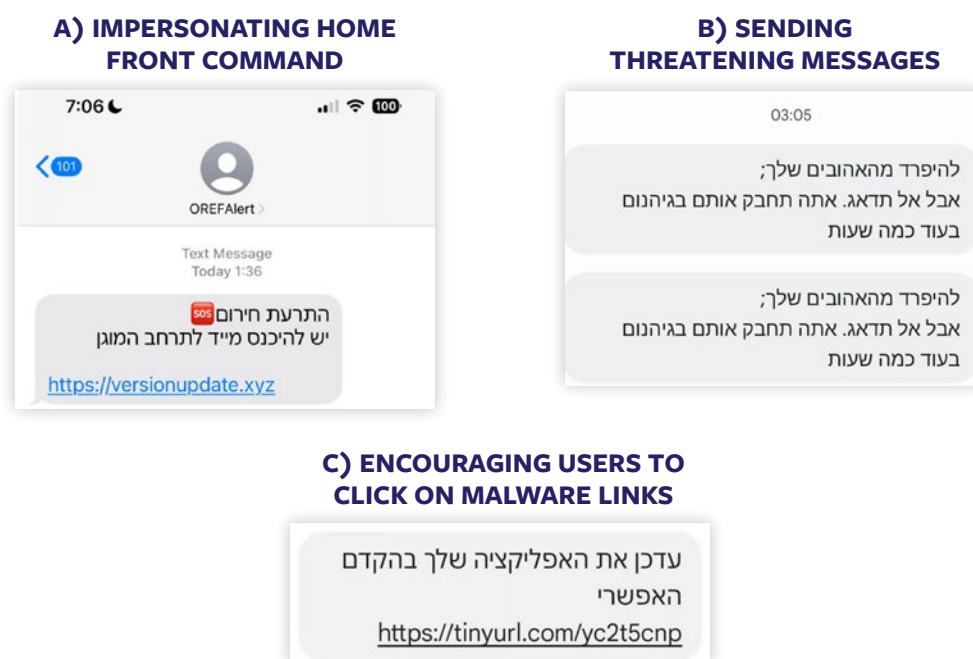
The great majority of Iran's campaigns during this period targeted **Israeli publics**. These campaigns included cyber intrusions, hack-and-leak operations, coordinated text messaging campaigns intended to intimidate, and social media campaigns aimed at sowing division and eroding public confidence in the government. Iran's activity began immediately after the Hamas attack. On October 7, 2023, for example, an IRGC-affiliated media outlet claimed that Iranian cyber actors had disabled an Israeli power plant, resulting in a local outage, though this was not independently verified.⁶³ In another case, an Iranian state broadcaster aired footage it presented as showing Hamas's capture of Israeli commanders. The video, which circulated widely, was later identified as footage from an unrelated incident in Nagorno-Karabakh, involving Azerbaijani forces detaining separatist leaders.⁶⁴ These episodes reflected an effort to amplify perceptions of Hamas's military effectiveness, even when based on misleading or repurposed visual material.

These early efforts soon gave way to more direct targeting of Israeli publics through Hebrew-language messaging. On October 26, 2024, just weeks after the second wave of Iranian missile strikes on Israel, a Hebrew-language account attributed to Supreme Leader Khamenei was launched on X.⁶⁵

The account posted messages in Hebrew declaring that “the Zionist regime made a mistake and miscalculated regarding Iran.”⁶⁶ Around the same time, the regime erected a large billboard in Tehran’s Palestine Square bearing the message: “Another Storm Is Coming,” a phrase widely seen as echoing the October 7 assault, which Hamas named the “Al-Aqsa Flood.”⁶⁷ Messages of this kind, delivered in Hebrew and directed at Israeli audiences, continued over the following weeks and months. They frequently expressed support for Hamas, framed developments as victories over Israel, and appeared designed to intimidate and demoralize.

One particularly notable tactic was the combination of cyberattacks with threatening messages. For instance, in September 2024, Israeli authorities reported that Iran and Hezbollah were behind a mass campaign that sent intimidating text messages to millions of Israeli citizens, using phone numbers obtained through a prior hack.⁶⁸ Some messages impersonated Israel’s Home Front Command (the military unit responsible for civil protection), ordering recipients in broken Hebrew to seek immediate shelter. Others contained explicit threats such as “Say goodbye to your loved ones; don’t worry, you’ll hug them in hell in a few hours,” and included malware links (see Figure 7). In a separate incident in January 2025, an Iran-linked hacker group breached the emergency alert systems of an Israeli security firm and triggered Red Alert sirens—audio warnings for incoming rocket fire—at approximately 20 daycare centers across the country. Through the same system, the hackers also broadcast messages expressing support for anti-Israel militant groups.⁶⁹

Figure 7: Text Messaging Campaigns Targeting the Israeli Public



A: “Emergency Alert [SOS emoji]. You need to enter immediately into a safe shelter,” impersonated as OREFAlert (Home Front Command); B: “Say goodbye to your loved ones; don’t worry, you’ll hug them in hell in a few hours”; C: “Update your app as soon as possible [link to malware]”.⁷⁰

Alongside these intimidation efforts, Iran sought to exacerbate social and political divisions within Israeli society. These campaigns relied on covert networks operating across social media platforms and sought to deepen internal polarization. Rather than pushing a uniform ideological message, Iranian-linked accounts amplified opposing views tailored to different segments of the population. Some posed as left-leaning Israeli activists criticizing the government for abandoning hostages,⁷¹ while others mimicked ultranationalist voices calling for violent retribution and denouncing dissenters as traitors.⁷² The goal seems to have been to fuel discord and weaken the cohesion of the Israeli public—a strategy that echoes tactics seen in covert operations by other actors, such as Russia.⁷³

One prominent example is the network known as “Tears of War,” a covert influence campaign operating across multiple social media platforms that impersonated Israeli activists. Its messaging focused on undermining Prime Minister Netanyahu and amplifying criticism of his wartime leadership, often highlighting the human and economic costs of the conflict as a tool of demoralization. Much of this content circulated through inauthentic accounts that used AI-generated profile images and carefully crafted messages to inflame public anger toward the government. Some posts invoked existential threats—warning of “a second Holocaust,” predicting mass casualties from Iranian missiles, or alleging catastrophic failures of Israel’s defense systems—while others spread fabricated news, including claims that the defense minister had been assassinated.⁷⁴ A notable feature of this campaign is that it sought to exert influence beyond the digital sphere. In some cases, it mobilized Israeli citizens to hang posters inside Israel calling for Prime Minister Netanyahu’s impeachment and to join protests against the government.⁷⁵

In addition to Israeli publics, Iran’s information operations targeted **international audiences**. These messaging efforts sought to shape global perceptions of the war in ways that would delegitimize Israel and increase sympathy for Iran and its allied militant organizations.

Several high-profile operations combined technical breaches with public-facing messaging. In December 2023, for example, Iranian-linked hackers disrupted streaming platforms in Canada, the United Arab Emirates, and the United Kingdom, replacing live broadcasts with segments about the war in Gaza. According to Microsoft Threat Intelligence, the segments featured an AI-generated anchor delivering news-style bulletins about Palestinian casualties and prison conditions, accompanied by graphic imagery.⁷⁶ Viewers in the UAE described being surprised: One reported watching *BBC News* when the screen froze and cut to the fabricated broadcast, while another recalled being unable to shield her children as “every channel we switched to displayed the same content.”⁷⁷

In a related incident, IRGC-affiliated cyber actors exploited vulnerabilities in programmable logic controllers used in water systems, including devices manufactured by Israeli firms and deployed abroad. In one case, attackers defaced control system interfaces with anti-Israel slogans such as “Down with Israel.”⁷⁸ The campaign prompted a joint cybersecurity advisory from the US Cybersecurity and Infrastructure Security Agency, which warned that these actors were targeting critical infrastructure and using public defacements to signal political motivations.⁷⁹

Beyond cyberattacks, Iranian-affiliated networks also deployed covert influence campaigns seeking to support the growing anti-Israel protest movement in various countries, particularly in the United States. According to a statement by the US director of national intelligence, Iranian government actors

posed as activists online to encourage demonstrations, spread inflammatory content, and in some cases tried to offer financial support to protest participants.⁸⁰ As part of this effort, Supreme Leader Khamenei published an open letter in May 2024 addressed to American university students, praising them as “a branch of the Resistance Front” and encouraging their “honorable struggle” against US support for Israel.⁸¹ *Time* magazine later reported that the letter was widely promoted online using hashtags like #LetterFromLeader and #LETTER4U, with signs of coordinated inauthentic behavior among newly created social media accounts.⁸²

INFLUENCE OPERATIONS BY HEZBOLLAH AND THE HOUTHIS

Compared to other actors, Hezbollah and the Houthis operated with smaller digital infrastructures, but both used information campaigns to target various audiences, primarily in Israel. Much of their messaging focused on public threats, claims of military action, and intimidation.

Hezbollah

Hezbollah often relied on speeches by its leader, Hassan Nasrallah, to present the group as a disciplined deterrent force shielding Lebanon from Israeli aggression.⁸³ In these addresses, Nasrallah described Hezbollah’s engagement along the northern border as part of a broader effort to pressure Israel to alter its campaign in Gaza, emphasizing the imposition of military, economic, and societal costs.⁸⁴

Additionally, the group conducted a series of intimidation campaigns directed at the Israeli public, including mass text messages to civilians during escalations that were intended to erode morale and signal the costs of continued fighting. Israeli media reported campaigns targeting border-city mayors with threatening messages that urged them to press the government to end the war.⁸⁵ Hezbollah-affiliated hacktivist groups also claimed responsibility for several cyber operations. These included a reported breach of the Israeli parliament’s website, which was publicized through mass text messages linking to the site, as well as a separate incident in which threatening messages were sent to Haifa Port workers warning of missile strikes and alleged system compromises.⁸⁶

Hezbollah also adopted covert influence tactics similar to those used by Iran, although on a smaller scale. Investigations by Meta and others identified fake social media profiles and fictitious news entities tied to actors in Lebanon, including outlets linked to the pro-Hezbollah Al Mayadeen network.⁸⁷ One such platform, Dofek TV, launched in January 2024, published divisive and demoralizing Hebrew-language content aimed at Israeli audiences. Its messaging focused on deepening internal polarization, spreading anti-government narratives, and weakening public morale by emphasizing battlefield losses and the economic and human costs of the war (see Figure 8).⁸⁸

The Houthis

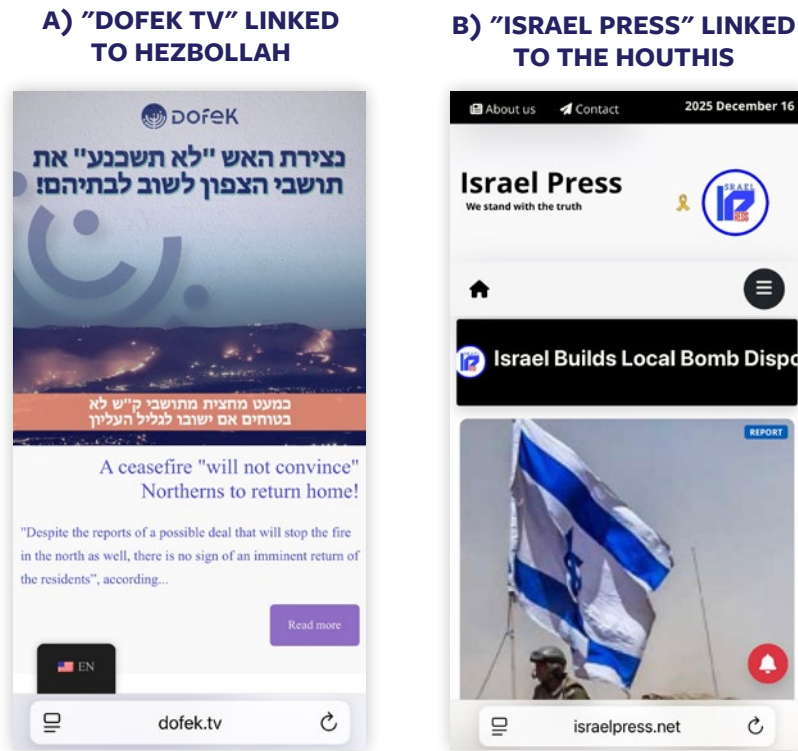
Houthi influence operations during the war centered on public threats and repeated claims of military action tied to developments in Gaza and the Red Sea. To international audiences, the group framed its naval actions as a blockade intended to pressure Israel and as an expression of solidarity with Gaza. This messaging emphasized the Houthis' portrayal of themselves as defenders of the Muslim nation against Israel and its Western allies, and sought to elevate their standing within the regional resistance camp by presenting attacks on commercial shipping vessels as politically justified.⁸⁹

Toward Israeli audiences, Houthi messaging took a more direct and threatening tone. Senior officials increasingly incorporated English- and Hebrew-language messages aimed explicitly at intimidation. Hezam al-Asad, a member of the Houthi political bureau, repeatedly posted short, threatening messages in Hebrew on X, often in awkward or broken phrasing, warning of impending attacks on Israeli cities. In one widely noted instance early in the war, al-Asad posted a single word—"Eilat" (the name of an Israeli town)—shortly after the IDF announced an expansion of ground operations, a message widely interpreted as a direct threat.⁹⁰ Senior Houthi leader Abdul-Malik al-Houthi similarly issued public warnings intended to influence Israeli and US decision-making, threatening missile and drone attacks in response to potential developments in the war, such as the mass displacement of Palestinians from Gaza.⁹¹

Many of these campaigns relied on unverifiable or false claims. On multiple occasions, Houthi spokesmen announced large-scale missile or drone strikes on Israel, asserting that targets had been hit. Israeli officials consistently denied these claims, reporting interceptions or failures.⁹² In other cases, Houthi-affiliated accounts circulated fabricated visual evidence, including video game footage repurposed to depict the downing of US aircraft or attacks on American naval assets.⁹³ One widely circulated message claimed that a Houthi missile strike had sunk the USS *Dwight D. Eisenhower*; the message was accompanied by doctored videos showing an aircraft carrier exploding. US Navy officials publicly refuted these reports.⁹⁴

In addition to overt messaging, the Houthis have reportedly engaged in covert campaigns targeting Israeli publics. These included fake Hebrew-language Facebook pages that redirected users to counter-feit news websites.⁹⁵ According to cybersecurity researchers, the campaign relied on a long-standing infrastructure of inauthentic accounts, Facebook groups, and cloned websites that copied real Israeli news and gossip content and seeded it into large, legitimate community groups.⁹⁶ Figure 8 shows some examples from these campaigns.

Figure 8: Examples of Counterfeit News Sites Linked to Hezbollah and the Houthis



The examination of actors and their operations above highlights the range of tactics and audiences involved in influence operations since the October 7 attack. Viewed in isolation, however, these campaigns make it harder to see how information campaigns unfold over time: how narratives are introduced and taken up as events develop, and how messaging adapts in response to adversaries' communications. To address this limitation, we shift from an actor-by-actor perspective to examining influence activities during a single round of confrontation.

A CASE IN FOCUS: ONLINE INFLUENCE AMID THE ISRAEL–IRAN ESCALATION OF JUNE 2025

The June 13–24, 2025, escalation between Israel and Iran offers an opportunity to observe how wartime influence operations function under conditions of rapid escalation. Over the 18 months following October 7, 2023, online influence activity by regional actors expanded steadily in scale and sophistication. The 12-day Israel–Iran confrontation, however, produced the most intense burst of coordinated information and cyber operations in our dataset, both in the number of campaigns launched and in the volume of content disseminated across platforms (see Figure 3). The concentration of activity into a brief window brings to view the dynamic process in which narratives are introduced and contested alongside developments on the battlefield.

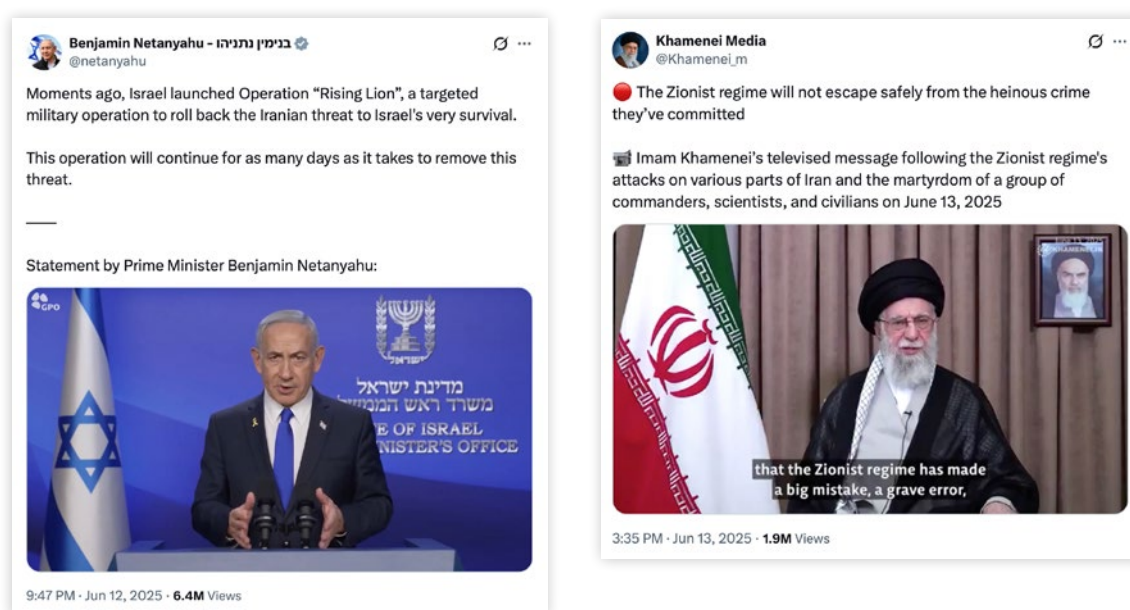
Consistent with the framework we presented earlier, this episode can be understood as a competition over audiences, particularly international publics and the adversary’s population. To reach these audiences, both actors combined official messaging, amplification by networks of affiliated and proxy accounts, and cyber-enabled actions. Below, we trace this competition through three prominent themes in the online campaigns of both sides.

1. COMPETING CLAIMS OF VICTIMHOOD AND LEGITIMACY

The first battle was over the basic moral structure of the escalation: Who is the victim, and who is the aggressor? Israel’s official messaging often framed the June 13 strike as preemptive self-defense against an imminent nuclear threat, emphasizing necessity and urgency. Israeli leaders and official military accounts described Iran as a rapidly escalating threat with implications beyond Israel. In one widely circulated post, for example, the IDF articulated this position in explicitly international terms, warning that “Iran is a global threat” and that Israel was “not the end goal,” and emphasizing that it had “no other choice but to act” before the threat escalated further.⁹⁷

Iran’s response echoed the structure of Israel’s claim, but reversed its moral valence. Iranian officials and state-aligned accounts framed Israel as the aggressor and Iran as the victim exercising legitimate retaliation. In public statements, Iran’s leadership described the June 13 strike as an unprovoked act of aggression and emphasized Iran’s right to respond in self-defense. Ali Khamenei condemned Israel’s actions and warned that Israel would not escape unscathed, while the Foreign Ministry framed Iran’s response as lawful retaliation under international law. Senior political figures reinforced this framing, portraying Iran’s actions as showing restraint and having been undertaken to deter further attacks rather than to escalate the conflict.⁹⁸

Figure 9: Israeli and Iranian Leaders' Statements Legitimizing Military Action

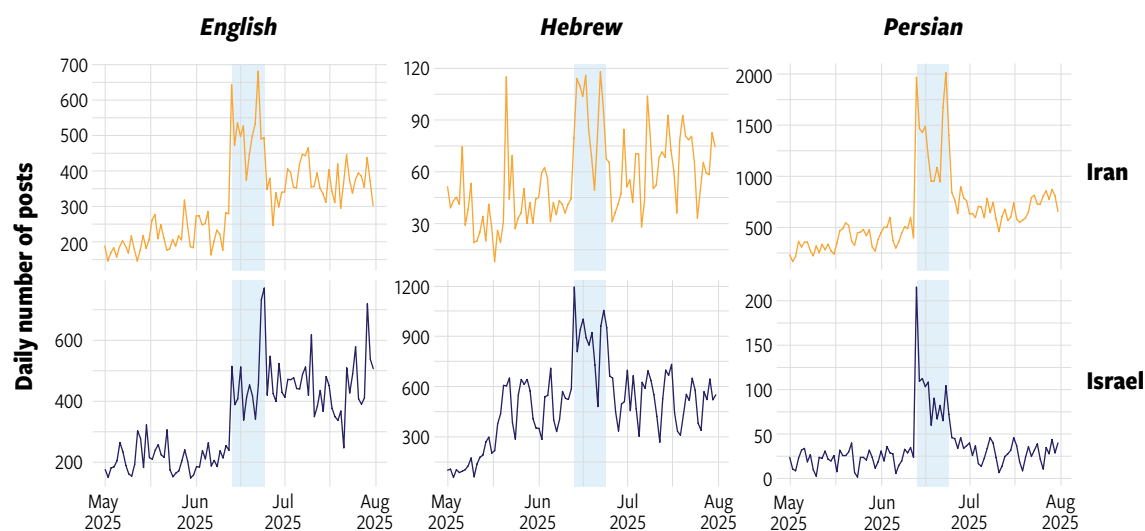


Israel (left): Statement by Israeli Prime Minister Benjamin Netanyahu announcing the launch of a targeted military operation against Iran, framing the action as necessary self-defense to counter an existential threat.⁹⁹ Iran (right): Televised address by Iran's Supreme Leader Ali Khamenei following Israeli strikes, framing Iran as the victim of aggression and emphasizing the need for retaliation.¹⁰⁰

What's interesting is that both sides sought to anchor interpretation early. Benjamin Netanyahu posted a public speech on X less than two hours after the attack, describing it as "a targeted military operation to roll back the Iranian threat to Israel's very survival."¹⁰¹ Ali Khamenei responded shortly afterward, accusing Israel of having "committed a crime in our dear country today at dawn with its satanic, bloodstained hands" (see Figure 9).¹⁰² The speed of these statements signals the strategic value of early framing, for both international audiences, whose reactions can translate into diplomatic constraints, and domestic and enemy publics.

Figure 10 shows the rapid rise in posts during the escalation by Iranian-affiliated and Israeli-affiliated accounts on X, Telegram, Facebook, Instagram, TikTok, and YouTube, across the languages most commonly utilized: English, Persian, and Hebrew. Both sides sharply increased their average daily messaging volume on June 13, the moment the escalation began. English-language posts by Iran-linked accounts rose by 130 percent, while Israeli-affiliated accounts increased their English posting by 123 percent in the days following the start of the war, compared with prior weeks. Targeting of enemy publics was also substantial. Iran's messaging in Hebrew, likely directed at Israeli audiences, rose by 127 percent during the escalation, while Israeli messaging in Persian increased by 343 percent, a sharp change from the levels of the preceding weeks.

Figure 10: Sharp Rise in Posting Activity with the Start of the Iran–Israel War



Note: Posts are from X, Telegram, Facebook, Instagram, TikTok, and YouTube in 2025.
Light blue shading indicates the 12-Day War, June 13–24, 2025.

2. YOUR LEADERSHIP IS AGAINST YOU: OPERATIONS AIMED AT THE ADVERSARY’S PUBLIC

Both Israel and Iran not only made claims of legitimacy targeting international audiences, but targeted the adversary’s population in an effort to undermine trust in leadership and heighten internal unrest.

Israeli-linked Persian-language messaging focusing on Iranian audiences combined ridicule and moral indictment to undermine confidence in the clerical leadership. A prominent strand of this messaging relied on mockery and delegitimation of senior figures, particularly Khamenei. Posts circulated by Israel’s official accounts in Persian portrayed the Iranian regime as weak, absurd, or fraudulent, often using visual satire. One widely shared post, for example, mocked the regime as “the first power in the region—in the field of Photoshop,” pairing the caption with manipulated imagery that cast official Iranian claims of strength as artificial and hollow. Other posts depicted the regime as isolated and fearful, asserting that the Islamic Republic “is much weaker than they think” and “fears its own people.”¹⁰³

Alongside ridicule, Israeli-linked accounts promoted narratives of solidarity with the Iranian people and sought to encourage internal dissent. For example, in an English-language speech translated to Persian targeting the Iranian people, Benjamin Netanyahu framed the attack on Iran as not only preventing a nuclear threat, but also paving the way for the Iranian people to “achieve their freedom” from the oppression of the Iranian regime. In this speech, he used symbols employed by Iranian protesters since 2022, and said, “This is your opportunity to stand up and make your voice heard.”¹⁰⁴

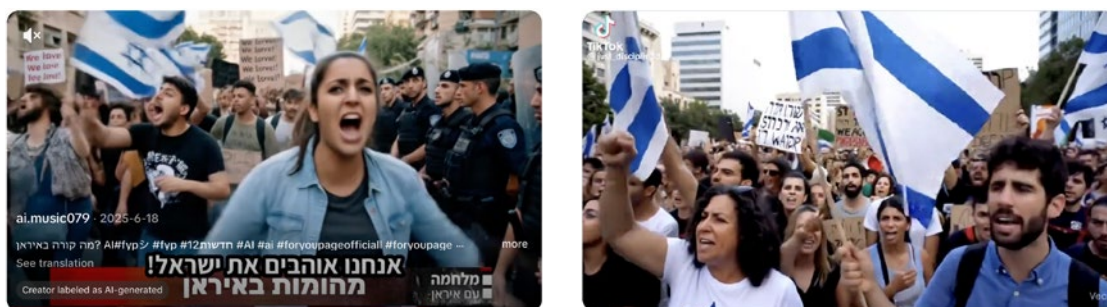
Other official posts by Israeli government accounts emphasized a people–regime divide, accusing Iran’s leaders of having “spent tens of billions of dollars from your youth and your life” on nuclear and

military ambitions, before concluding with messages such as “Do not let them kill your dreams” and “We stand with you,” often accompanied by imagery combining Israeli symbols with pre-revolutionary Iranian motifs associated with the Shah.¹⁰⁵ Other content originating from pro-Israel accounts went further, circulating AI-generated videos purporting to show pro-Israel demonstrations inside Iran, with captions claiming that Iranians were “shouting ‘We love Israel!’ in the streets.” (see Figure 11)¹⁰⁶ One prominent X account presenting itself as the Mossad’s Persian-language spokesperson called on Iranians to revolt, offered financial and medical assistance, and shared AI-generated videos depicting more prosperous lives under a new regime.¹⁰⁷ Similar efforts at mobilizing the Iranian people against the regime were reported around Israel’s strike on Evin prison in Tehran.¹⁰⁸

Iran pursued a similar strategy when targeting the Israeli public. The goal seems to have been to redirect wartime fear and disruption into opposition to the government. A large part of the related content was distributed by unofficial Iranian-affiliated networks that relied heavily on impersonation of Israeli citizens and activists. These accounts adopted Israeli names and symbols, and circulated imagery styled after Israeli newspapers and protest visuals to enhance credibility.¹⁰⁹

Much of this messaging focused on ridiculing Prime Minister Benjamin Netanyahu and framing civilian vulnerability as the direct result of his decisions.¹¹⁰ Some posts mocked his absence during attacks, asking “Where is Netanyahu now? Does he also have no shelter?”¹¹¹ while others depicted crowded shelters and communications breakdowns, warning Israelis that they were being left with “only pain, destruction, and hatred,” and concluding pointedly, “Thank you, Bibi.”¹¹² Other messages also made this attribution explicit, warning Israelis that they were “paying the price for Netanyahu’s stupidity,” urging them to “bring him down,” or describing civilians as “cannon fodder” for a leadership insulated from the consequences of its decisions.¹¹³ Some impersonated content circulated short videos (many of which appeared AI-generated or manipulated) showing dramatic explosions or protest scenes, suggesting that escalation and suffering were inevitable consequences of the government’s actions.¹¹⁴ These efforts appear to have sought to activate existing grievances and channel wartime fear into political opposition against Israel’s leadership.

Figure 11: AI-Generated Videos of Iranian and Israeli Protests



Left: AI-generated video depicting an Iranian protest scene saying “We love Israel,” circulated by impersonating accounts to simulate domestic unrest and amplify perceptions of internal dissent.¹¹⁵ Right: AI-generated video depicting an Israeli protest scene calling for an end to the war with Iran, circulated by social media accounts to amplify perceptions of internal dissent and distrust in Israeli government.¹¹⁶

3. EFFORTS TO INTIMIDATE AND DEMORALIZE

The June 2025 escalation was accompanied by an unusually visible surge in intimidation-oriented activity directed at enemy publics, spanning cyber operations by proxy organizations and official threats. In the opening days of the confrontation, cybersecurity firms and government sources reported a sharp increase in malicious cyber activity linked to both sides.¹¹⁷ Israeli authorities documented a dramatic rise in attempted intrusions, denial-of-service attacks, and disruption campaigns targeting civilian infrastructure, with some estimates suggesting a several-hundred-percent increase in attack volume relative to the levels of prior weeks.¹¹⁸

For example, a cyber hacker group supporting Israel announced that it had attacked Iranian financial institutions. One of the most visible incidents involved Bank Sepah, a state-owned Iranian bank with close ties to the defense sector. In mid-June, pro-Israel cyber accounts claimed responsibility for a cyberattack against Bank Sepah, asserting that the group had destroyed the bank's data and portraying the institution as vulnerable to further cyber action.¹¹⁹ Later reporting noted that Bank Sepah's website was offline and that customers were experiencing difficulties accessing their accounts; Iranian authorities described the outages as temporary disruptions and did not publicly confirm the cause.¹²⁰

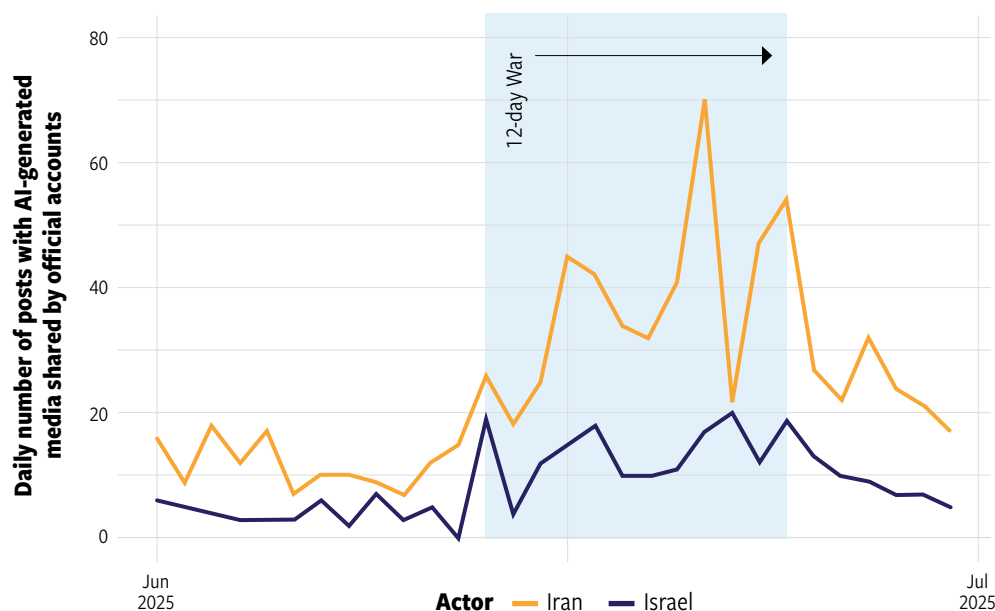
Similarly, pro-Iranian hacker groups announced a series of attacks targeting Israeli civilian and commercial systems. Iranian-aligned collectives publicly claimed responsibility for denial-of-service attacks against Israeli government portals, transportation-related websites, and private companies, framing these operations as retaliation for Israel's military actions.¹²¹ Israeli authorities confirmed the surge, with the Israel National Cyber Directorate warning of widespread social-engineering operations, spoofed emergency alerts, and intrusions into civilian camera systems that officials described as efforts to sow public fear.¹²²

Beyond cyber operations, intimidation became increasingly explicit in official and semi-official messaging. Israeli government and military accounts circulated material emphasizing Israel's operational reach inside Iran and its capacity to strike sensitive targets. Posts attributed to Israeli official channels highlighted intelligence penetration and operational access, sometimes pairing warnings with imagery or language suggesting that Iranian military and security assets were fully exposed.¹²³ Iranian official messaging, by contrast, relied on more direct and overtly threatening language aimed at Israeli publics. Khamenei issued a series of public statements warning that Israel had committed a "grave mistake" and would face a "bitter and painful fate," while English- and Hebrew-language posts from his official accounts warned that attacks on Iran would impose heavy costs.¹²⁴ Posts by channels linked to the Islamic Revolutionary Guard Corps echoed these threats, frequently pairing them with images of missiles and references to future retaliation.¹²⁵

These intimidation messages were often accompanied by dramatic visual depictions using AI-generated media, which increased with the start of the escalation (see Figure 12 and "Detecting AI-Generated Multimedia" in the Appendix). Accounts linked to both sides circulated synthetic or heavily manipulated visuals designed to exaggerate damage and heighten fear.¹²⁶ Iranian state-aligned outlets and affiliated accounts shared fabricated or altered videos depicting large-scale devastation inside Israel, including scenes of explosions, missile strikes, fires, and urban collapse.¹²⁷ Israeli-linked

networks employed similar techniques, circulating AI-generated or heavily stylized visuals portraying strikes inside Iran and emphasizing the vulnerability of the Iranian regime.¹²⁸ The prominence of AI-generated content during the escalation was sufficiently visible to attract widespread public attention.¹²⁹ Some examples from AI-generated media shared by official channels are shown in Figure 13.

Figure 12: The Use of AI-Generated Media Rose During the Escalation



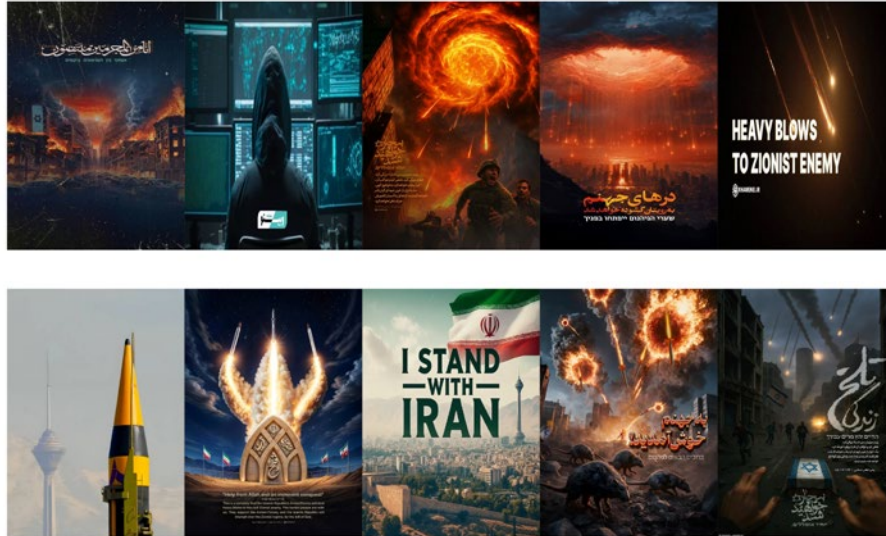
Note: Light blue shading indicates the 12-Day War between Israel and Iran, June 13–24, 2025.

What this episode reveals is how much importance actors believe online influence efforts have during rapid military escalation. The diversity of tactics used—combining cyber operations, official messaging, covert impersonation, and AI-generated content—alongside many efforts to reach key audiences showcases the value both sides placed on shaping perceptions and legitimacy. The fast deployment of these efforts from the first hours of the escalation also signals the premium placed on determining the narrative early. The concentration of activity during this brief window suggests that at least on the information side, a great deal was at stake. What remains an open question is whether these efforts had any effect; we discuss this point more directly in the final section.

The fast deployment of these efforts from the first hours of the escalation also signals the premium placed on determining the narrative early.

Figure 13: AI-Generated Media Shared by Official Iranian and Israeli Accounts

A) IRAN



B) ISRAEL



CONCLUSION: LESSONS FROM THE INFORMATION FRONT

The conflicts that unfolded across the Middle East between 2023 and 2025 make clear that information operations are no longer peripheral to warfare. They have become a regular and often highly visible component of how armed actors pursue strategic goals. Across the campaigns documented in this report, states and non-state actors alike used digital media to shape how conflict events were understood by different publics. They did so to justify violence, erode morale, mobilize supporters, intimidate adversaries, and influence how outside audiences interpreted the war. The information space, in other words, was not merely a venue for wartime commentary. It was itself an active front.

Several broader patterns stand out. First, influence operations in this conflict were often directed at specific audiences, with actors adapting messages across languages and channels depending on which publics they sought to reach and what strategic purpose they hoped to serve. Second, the material examined here shows the value of analyzing these operations in context. Repetition across accounts, coordination across platforms, alignment with military or political developments, and consistent targeting can reveal patterns that are less visible when content is viewed in isolation.

This wider view also helps clarify the relationship between information operations and cyber activity. Although the two remain analytically distinct, the cases examined here suggest that they were often connected in practice. In some instances, cyber activity enabled broader messaging efforts by generating spoofed communications that were then spread through compromised channels. In other instances, strategic messaging around cyberattacks increased their visibility and helped them reach broader audiences. At times, the cyber incident itself appeared to carry a communicative function, serving to intimidate civilians, demoralize adversaries, or project capability. These patterns suggest that the intersection of cyber and influence operations warrants greater scholarly and policy attention than it has so far received. They also point to how wartime information contests are shaped not only by offensive campaigns, but by efforts to expose and counter them.

The intersection of cyber and influence operations warrants greater scholarly and policy attention than it has so far received.

The cases examined here also make clear that once the information space becomes an active front, it becomes a site of response and contestation. Actors across the conflict did not simply launch influence operations; they also sought to contain or discredit the operations of their adversaries. Sometimes this took the form of restricting the flow of information, whether through extensive internet shutdowns and tighter control over communications, as in Iran, or through narrower wartime limits on what could be publicly circulated or discussed.¹³⁰ In other cases, the response was to expose hostile campaigns by identifying fake accounts, spoofed messages, or covert influence efforts and framing

them as manipulation.¹³¹ Elsewhere, actors turned to countermessaging, including public rebuttal and efforts to combat hostile narratives with alternative ones.¹³² These responses varied substantially across settings, and the evidence assembled here is not sufficient to provide a systematic accounting of all such measures across actors and theaters. A fuller understanding of wartime countermeasures, and of the conditions under which they are adopted, would require more focused research.

At the same time, important questions remain about the effects of these campaigns and the responses they provoked. Mapping narratives, tactics, and patterns of coordination is not the same as demonstrating influence. This report shows how actors sought to shape beliefs and behaviors, and how their adversaries sometimes attempted to counter those efforts, but it remains much harder to determine when such operations succeeded, for whom, and under what conditions. Future work should move beyond documentation alone to examine the reach and reception of wartime influence operations, including the role of synthetic media and other emerging tools.

These findings carry several implications for practitioners. The first is institutional. The kind of monitoring called for by this report cannot be built ad hoc during a crisis. It requires standing capacity to collect public data across platforms, preserve evidence before it disappears, work across languages, combine regional and technical expertise, and interpret online campaigns in relation to military and political developments. Yet this public-interest monitoring infrastructure has weakened at precisely the moment when wartime influence operations have become more complex. CrowdTangle, long used by journalists and researchers to monitor public content on Facebook and Instagram, was shut down in August 2024.¹³³ Meta's Content Library and API provide an alternative source of platform data, but access is reviewed and limited to approved academic and public-interest research institutions.¹³⁴ Major academic efforts in the field have also faced legal and political pressure, with Stanford's Internet Observatory reportedly shedding most of its staff and the Election Integrity Partnership concluding its work.¹³⁵

This creates a gap between the scale of the problem and the institutions available to study it. Governments, foundations, universities, and platforms should invest in durable, independent monitoring capacity for conflict-related information operations. This should include emergency data-access arrangements during armed conflict, support for multilingual and regional expertise, legal protections for public-interest researchers, and mechanisms for preserving evidence of coordinated campaigns before accounts or posts are removed. Platforms should not be the only actors able to see crises as they unfold.

The second implication concerns platform governance. Wartime influence operations often cut across platform policy categories, including misinformation, coordinated inauthentic behavior, manipulated media, state-linked activity, and terrorist or militant organization content. The cases examined in this report suggest the need for conflict-specific policies that can be activated during fast-moving crises. These policies should include real-time review capacity for coordinated campaigns during armed conflict; clearer labeling rules for realistic synthetic media that purports to show battlefield events, civilian harm, protests, or military success; stronger systems for identifying cross-platform impersonation and proxy amplification; and publicly articulated standards for how platforms treat official state accounts, semi-official channels, and deniable affiliated networks during war. This is especially urgent for AI-generated media. Meta's Oversight Board recently reached a similar conclusion in a

case involving AI-generated content during the 2025 Israel–Iran War, calling for stronger provenance standards, detection tools, and labeling practices for deceptive AI-generated content in conflicts and crises.¹³⁶

More broadly, responding to wartime influence operations requires more than debunking isolated claims after the fact. It requires the capacity to track campaigns across platforms, interpret them in relation to conflict dynamics, and recognize when seemingly separate informational and cyber incidents form part of the same broader effort. The central challenge is therefore more than identifying false or manipulated content; it's also building the institutional and platform-level infrastructure needed to understand how narrative contests unfold during war.

**[Responding to wartime influence operations]
requires the capacity to track campaigns across
platforms, interpret them in relation to conflict
dynamics, and recognize when seemingly separate
informational and cyber incidents form part of
the same broader effort.**

APPENDIX

DATA COLLECTION METHODOLOGY

This section provides additional detail on the construction of the two datasets used in the analysis. The first is a campaign-level dataset of publicly reported information and cyber operations conducted by the five principal actors examined in the report: Israel, Hamas, Iran, Hezbollah, and the Houthis. The second is a post-level dataset of public social media content disseminated by official and unofficial accounts affiliated with those actors. The two datasets capture different units of analysis. The first records discrete reported campaigns or incidents. The second captures the underlying stream of posts disseminated over the same period.

Campaign-Level Dataset of Reported Operations

The campaign-level dataset was constructed to capture discrete information and cyber operations conducted during the period under study. The dataset includes operations attributed to Israel, Hamas, Iran, Hezbollah, and the Houthis, including both officially attributed campaigns and operations conducted by unofficial actors or groups aligned with their cause. Cases were identified through a multilingual search strategy combining keyword searches and iterative source tracing. We searched in English, Hebrew, Arabic, and Persian, using combinations of actor names, platforms, audiences, and operation types. Searches drew on domestic and international media coverage, OSINT (open source intelligence) investigations, platform transparency materials, cybersecurity reporting, think tank publications, NGO and government reports, and references uncovered through already identified cases.

The unit of observation in the campaign-level dataset is a distinct reported campaign or incident. When the same campaign appeared across multiple reports, we matched cases by actor, platform, type, and date, and sought multiple sources to verify that they referred to the same underlying operation. When one incident spanned multiple platforms, it was coded as a single operation. When an operation unfolded over multiple days or weeks, it was treated as one campaign and dated using the first observed day of the operation.

Inclusion in the campaign-level dataset required that a case match our definition of a discrete information operation or cyber operation and that it could be linked to one of the focal actors, either through official attribution or through a sufficiently clear connection to unofficial actors aligned with that actor's agenda. We excluded cases that could not be verified, unattributed or weakly sourced claims, and campaigns for which no plausible link to one of the focal actors could be established. We also excluded domestic information operations, because the report focuses on campaigns targeting enemy or international audiences.

For each campaign, we coded the date of execution or reporting, the actor responsible, the intended target audience, and the tactics used. Tactic categories were developed through an initial inductive review of the cases and then applied deductively using the project's broader theoretical

framework. Campaigns could receive multiple tactic codes. In the final version used for analysis, the main substantive categories included operations aimed at disrupting systems, stealing information, polarizing or demoralizing audiences, mobilizing against the enemy, intimidating targets, and increasing sympathy. The underlying coding protocol used by the research team also distinguished among broader campaign types and specific methods, including cyber, overt media, and covert operations. The date variable records the first date of the campaign as reported in the sources used for coding. When the execution date could not be identified, we used the date on which the campaign was reported. All cases were reviewed by more than one person, and disagreements were resolved through deliberation and consensus.

Post-Level Social Media Dataset

The second dataset captures public social media content disseminated by official and unofficial accounts affiliated with the same five actors over the same period. It includes content from Facebook, Instagram, YouTube, X, Telegram, and TikTok. All six platforms were covered across the study period, although the amount of available data differed across platforms.

We constructed the account list in two stages. First, we identified official accounts belonging to governments, organizations, or formal actor-linked entities on each platform. Second, we expanded outward to identify unofficial affiliated accounts using information from the campaign-level dataset, outside reporting, and our own platform investigations. This produced a broader set of accounts that included aligned media outlets, cyber units, semi-official channels, and other accounts of influencer-sympathizers that consistently amplified the actor's messaging.

We classified official accounts conservatively. Accounts were coded as official only when direct institutional ownership or control was clear. Accounts that supported an actor's goals but did not clearly belong to the actor institutionally were coded as unofficial. In ambiguous cases, accounts were treated as unofficial, and accounts were removed altogether when the link to the actor was not sufficiently clear. Our analysis distinguishes organized networks from the broader universe of organic supportive posting. Not every sympathetic user was included. Rather, the post-level dataset focuses on accounts that exhibited some degree of coordination, repetition, or strategic intent, or that were identified in secondary reporting as part of a broader actor-linked network.

We collected public posts from these accounts prospectively using a third-party API.¹³⁷ For each post, we retained all available metadata, including account ID, post ID, post text, publication date, engagement measures, and attached media. The dataset includes original posts as well as reposts, retweets, and forwards. Deleted or inaccessible posts were not included, though because we collected data prospectively, it likely captured a substantial amount of content that was later removed. After collection, posts from all platforms were harmonized into a single combined dataset. Table A1 shows the list of accounts by actor and platform.

Detecting AI-Generated Multimedia

We analyzed all visual media in the dataset using Sightengine, a commercial detection system designed to identify AI-generated content. The model analyzes the visual (pixel-level) properties of images and video frames and does not rely on metadata such as Exchangeable Image File Format (EXIF) information. For each image or frame, Sightengine produces a continuous score between 0 and 1, with higher values indicating greater confidence that the content was generated by an AI model. The system was trained on a large corpus of human-created and artificially generated images spanning a wide range of content types, including photography, drawings, artwork, and memes, and is designed to detect images produced by major generative models currently in use, such as Stable Diffusion, Midjourney, Adobe Firefly, Flux, and related systems.¹³⁸ We classified content with a score of 0.9 or higher as AI-generated.

To evaluate the classifier's ability to identify AI-generated media, we assessed its performance using a benchmark dataset of 1,000 synthetic images. These images were generated using a text-to-image model that was publicly available during the study period, with the explicit goal of matching the state of generative image technology as it existed in June 2025. To implement this validation, we generated images programmatically using Flux, drawing on generic, randomly generated prompts rather than conflict-specific content. Applying the same detection threshold used in the main analysis (0.9), the classifier correctly identified 96.8 percent of AI-generated images in this validation set.

Table A1: List of Accounts by Actor and Platform

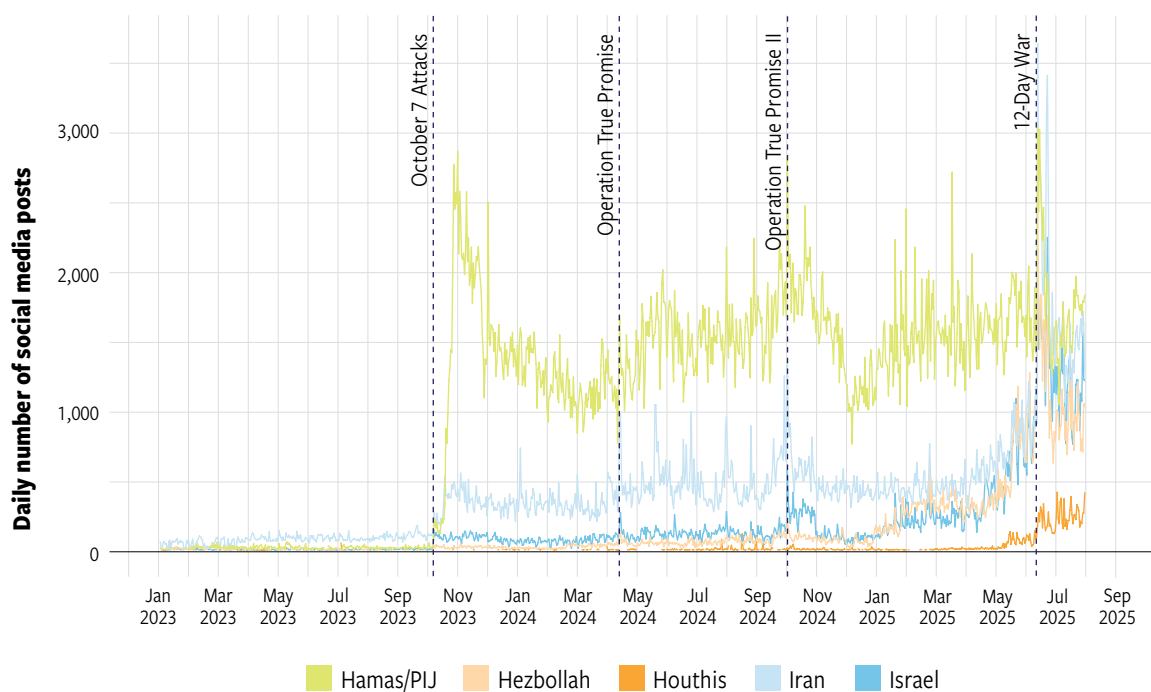
Actor	Platform	Account Names
Iran official	Facebook	Foreign Ministry, Islamic Republic of Iran
Iran official	Instagram	سيد؛ پایگاه اطلاع رسانی دولت؛ شهيد حسين اميرعبداللهيان؛ ابراهيم رئيسی
Iran official	Telegram	کانال اخبار؛ سيد ابراهيم رئيسی؛ سپاه سایبری پاسداران IRGC؛ سپاه سایبری پاسداران IRGC؛ سپاه پاسداران؛ سپاه پاسداران؛ سپاه پاسداران
Iran official	TikTok	Khamenei Quotes
Iran official	Twitter	IRNaghizadeh; Ajaatollah Khamenei; Government of the Islamic Republic of Iran; Government of the Islamic Republic of Iran; H.Amirabdollahian؛ اميرعبداللهيان؛ Iran Defense (unofficial); Iran Defense commentary (unofficial); Iran Defense؛ نيروهای مسلح جمهوری اسلامی ایران؛ Iran Military; IRAN Military; Iran Military (Commentary); Islamic Iran Military; Khamenei Media; Khamenei Site Web; Khamenei TV; Khamenei.ir; KHAMENEI.IR؛ فارسی؛ Khamenei.ir Hebrew; Masoud Pezeshkian; Pars Today English; ParsToday English; Saeed Khatibzadeh؛ علی شمخانی؛ سيد ابراهيم رئيسی؛ سعيد خطيبزاده؛ دفاع و پشتیبانی نیروهای مسلح وزارت؛ محمدباقر قالیباف
Iran unofficial	Facebook	شירה معین؛ نירה لوی؛ نوיה لوی؛ חדשות סלבריטאים؛ SimayAzadi؛ Press TV Highlights
Iran unofficial	Instagram	خبرگزاری فارس؛ خبرگزاری تسنیم؛ خبرگزاری ایرنا؛ IRNA News؛ عکירת ישראלים؛ Press TV؛ Tasnim News Hebrew؛ کار آنلاین؛ رسانه نگار
Iran unofficial	Telegram	مחזירים אותם! Bring Them Home Now؛ אזעקת תקיפה؛ Attack Alarm؛ ללא צנזורה؛ ישראליים פטריוטים؛ אגרון - גוש קטיף-؛ seculars of israel؛ Press TV؛ PressTV؛ פארס טודיי PARS TODAY؛ CAR ONLINE؛ הביתה עכשיו؛ חוזרים הביתה؛ מחאת הדגלים השחורים؛ ישראל השנייה؛ זכותנו؛ דמועות המלחמה؛ אין קול؛ אדוק؛ חוזרים הביתה؛ خبرگزاری؛ صباح العزم؛ کانال گنجشک درنده؛ خبرگزاری فارس؛ خبرگزاری تسنیم؛ ایرنا
Iran unofficial	TikTok	IRANTEHRAN؛ Iran Military؛ Israel.news؛ jewishfist

Hezbollah unofficial	YouTube	Al Mayadeen English; Lebanon On; شخصيات
Houthis official	Twitter	Yahya Sare'e; حزام الأسد; محمد علي الحوثي; نصر الدين عامر; Nasruddin Amer نصر الدين عامر
Houthis unofficial	Facebook	Ofoq Foundation مؤسسة أفي
Houthis unofficial	Instagram	Ofoq Foundation مؤسسة أفي
Houthis unofficial	Telegram	Almasirah English; Yemen Military; Yemeni Army; Yemeni Army Houthis; أعمال تلفزيونية - يحيى الشامي
Houthis unofficial	Twitter	مؤسسة أفي Ofoq Foundation مؤسسة فكرة; قناة المسيرة; ضيف الله الشامي; شاهد المسيرة

Note: Channel names are reported as they appeared in the source data. Some channels used more than one display name over time, including minor variations in punctuation or spelling; these variants are retained to reflect how the accounts presented themselves at collection.

ADDITIONAL RESULTS

Figure C1: Daily Number of Posts by Actor



Note: PIJ = Palestinian Islamic Jihad. Hamas category includes PIJ-linked campaigns.

ENDNOTES

- 1 Maria Petrova and Augustin Tapsoba, “Information and Conflict: From the Role of (Social) Media and Public Opinion to Big Data and Forecasting,” *Economic Policy* 40, no. 124 (2025): 845-878; Henning Lahmann, “Protecting the Global Information Space in Times of Armed Conflict,” *International Review of the Red Cross* 102, no. 915 (2020): 1227-1248; Joseph Levin and US JD, “Lessons on Public-Facing Information Operations in Current Conflicts,” *Military Review* 2 (2025): 20-31; Bailey Ulbricht and Joelle Rizk, “How Harmful Information on Social Media Impacts People Affected by Armed Conflict: A Typology of Harms,” *International Review of the Red Cross* 106, no. 926 (2024): 823-862; Daniel Michaels and Drew Hinshaw, “Why Countries Are Suddenly Broadcasting Their Spies’ Exploits,” *Wall Street Journal*, June 21, 2025, <https://www.wsj.com/world/why-countries-are-suddenly-broadcasting-their-spies-exploits-f455a666>.
- 2 For examples, see Derek B. Johnson, “Israeli Influence Operation Highlights Global Disinformation Industry,” *CyberScoop*, June 5, 2024, <https://web.archive.org/web/20250714150953/https://cyberscoop.com/israel-influence-operations-stoic/>; “Hamas Telegram in the Immediate Wake of Their 7 October Terrorist Attacks—Propaganda Content,” *VoxPol*, November 16, 2023, <https://voxpol.eu/hamas-telegram-in-the-immediate-wake-of-their-7-october-terrorist-attacks-part-2-propaganda-content/>; Ari Ben Am, “A Year of Meming Dangerously: Iranian Influence Operations Targeting Israel Since October 7,” *Foundation for Defense of Democracies*, August 28, 2025, <https://www.fdd.org/analysis/2025/08/28/a-year-of-meming-dangerously-iranian-influence-operations-targeting-israel-since-october-7/>.
- 3 Meta, *Threat Report: The State of Influence Operations 2017–2020* (Menlo Park, CA: Meta Platforms, 2021), <https://about.fb.com/wp-content/uploads/2021/05/IO-Threat-Report-May-20-2021.pdf>; Princeton University, *Trends in Online Influence Efforts* (Princeton, NJ: Empirical Studies of Conflict Project, 2024), <https://esoc.princeton.edu/publications/trends-online-influence-efforts/>; Javier Pastor-Galindo et al., “Influence Operations in Social Networks,” *arXiv* (2025), <https://arxiv.org/abs/2502.11827>; James Pamment and Darejan Tsurtsumia, *Beyond Operation Doppelgänger: A Capability Assessment of the Social Design Agency* (Lund: Lund University, Centre for Psychological Defence, 2025), <https://www.psychologicaldefence.lu.se/sites/psychologicaldefence.lu.se/files/2025-05/Beyond%20Operation%20Doppelgänger.pdf>.
- 4 Sara-Jayne Terp and Pablo Breuer, “DISARM: A Framework for Analysis of Disinformation Campaigns,” in *2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)* (IEEE, 2022), 1-8; Camille François, “Actors, Behaviors, Content: A Disinformation ABC: Highlighting Three Vectors of Viral Deception to Guide Industry & Regulatory Responses,” working paper, Transatlantic High Level Working Group on Content Moderation Online and Freedom of Expression (Annenberg Public Policy Center, September 20, 2019); James Pamment, “The ABCDE Framework,” in *The EU’s Role in Fighting Disinformation: Crafting a Disinformation Framework* (Washington, DC: Carnegie Endowment for International Peace, 2020), <https://www.jstor.org/stable/resrep26180.6>.
- 5 Barbara F. Walter and Gregoire Phillips, “Who Uses Internet Propaganda in Civil Wars and Why?” *Journal of Peace Research* 62, no. 3 (2025): 550-563; Benjamin T. Jones and Eleonora Mattiacci, “A Manifesto, in 140 Characters or Fewer: Social Media as a Tool of Rebel Diplomacy,” *British Journal of Political Science* 49, no. 2 (2019): 739-761; Keir Giles, “Russian Cyber and Information Warfare in Practice,” *Chatham House* 14 (2023).
- 6 Filipe N. Ribeiro, Koustuv Saha, Mahmoudreza Babaei, Lucas Henrique, Johnnatan Messias, Fabricio Benevenuto, Oana Goga, Krishna P. Gummadi, and Elissa M. Redmiles, “On Microtargeting Socially Divisive Ads: A Case Study of Russia-Linked Ad Campaigns on Facebook,” in *Proceedings of the Conference on Fairness, Accountability, and Transparency* (2019), 140-149; Eric K. Clemons, Maximilian Schreieck, and Ravi V. Waran, “Managing Disinformation on Social Media Platforms,” *Electronic Markets* 35, no. 1 (2025): 52; Eric V. Larson, Richard E. Darilek, Daniel Gibran, Brian Nichiporuk, Amy Richardson, Lowell H. Schwartz, and Cathryn Q. Thurston, *Foundations of Effective Influence Operations: A Framework for Enhancing Army Capabilities* (RAND Corporation, 2009); Tamar Mitts, Grégoire Phillips, and Barbara F. Walter, “Studying the Impact of ISIS Propaganda Campaigns,” *Journal of Politics* 84, no. 2 (2022): 1220-1225.
- 7 Renée DiResta and Josh A. Goldstein, “Full-Spectrum Propaganda in the Social Media Era,” *Security Studies* 34, no. 4 (2025): 714-750.
- 8 Fernando Maymí, Robert Bixler, Randolph Jones, and Scott Lathrop, “Towards a Definition of Cyberspace Tactics, Techniques and Procedures,” in *2017 IEEE International Conference on Big Data (Big Data)* (IEEE, 2017), 4674-4679.
- 9 Erica D. Borghard and Shawn W. Loneragan, “The Logic of Coercion in Cyberspace,” *Security Studies* 26, no. 3 (2017): 452-481.
- 10 All-Party Parliamentary Group on UK-Israel, *7 October Parliamentary Commission Report (The Roberts Report)* (London, 2025), <https://static1.squarespace.com/static/67bf0490d422da027d74c55c/t/6836f4a448ca2f538893b1e5/1748432053794/7+October+Parliamentary+Commission+Report++The+Roberts+Report.pdf>.

- 11 Zeina Jamaluddine, Hanan Abukmail, Sarah Aly, Oona M. R. Campbell, and Francesco Checchi, "Traumatic Injury Mortality in the Gaza Strip from Oct 7, 2023, to June 30, 2024: A Capture–Recapture Analysis," *The Lancet* 405 (February 8, 2025): 469–77, <https://www.thelancet.com/action/showPdf?pii=S0140-6736%2824%2902678-3>; Yaniv Kubovich and Nir Hasson, "IDF Accepts Gaza Health Ministry Death Toll of Over 71,000 Palestinians Killed During the War," *Haaretz*, January 29, 2026, <https://www.haaretz.com/israel-news/2026-01-29/ty-article/.premium/idf-accepts-gaza-health-ministry-estimate-of-over-70-000-palestinians-killed-in-the-war/0000019c-0918-dec4-adfd-fd5dde830000>.
- 12 We draw on definitions by the US Department of Defense and NATO, which state that influence operations are the coordinated use of capabilities—such as cyber operations, psychological operations, and military deception—to influence adversary perceptions and behavior. These doctrines highlight the strategic intent behind influence operations: They are designed to achieve concrete effects by shaping how information is received and acted upon. US Department of Defense and NATO definitions are summarized in Congressional Research Service, *Defense Primer: Information Operations*, CRS Report IF10771 (2022), <https://crsreports.congress.gov/product/pdf/IF/IF10771>; NATO Standardization Office, *Allied Joint Doctrine for Information Operations (AJP-10.1)* (2023), https://assets.publishing.service.gov.uk/media/650c03bf52e73c000d9425bb/AJP_10_1_Info_Ops_UK_web.pdf.
- 13 We include with Hamas also campaigns launched by the Palestinian Islamic Jihad (PIJ). PIJ is a Palestinian militant organization that operates in Gaza, other parts of the Palestinian territories, and abroad. It rejects political compromise with Israel, positions itself as part of the broader Islamist resistance front, and maintains close ties with Iran. While smaller than Hamas in membership and political capacity, PIJ has carried out frequent attacks against Israel and was an active participant in the October 7 assault.
- 14 Liraz Margalit, "זירת המלחמה האמיתית: ישראל פועלת לפי חוקים חדשים ומנהלת קמפיין תודעה אפקטיבי," ["The Real Battlefield: Israel Operates under New Rules and Runs an Effective Influence Campaign"], *Maariv*, October 12, 2024, <https://web.archive.org/web/20250220071846/https://www.maariv.co.il/journalists/article-1139627>; Israel Ministry of Foreign Affairs (@IsraelMFA), post on X, April 8, 2023, <https://x.com/IsraelMFA/status/1644692813672579074>; Israel (@Israel), post on X, February 11, 2023, <https://x.com/Israel/status/1624296163036872704>; Israel Defense Forces (@IDF), post on X, September 10, 2023, <https://x.com/IDF/status/1700892803276964176>.
- 15 Josh Rottenberg, "Inside the Museum of Tolerance's Screening of Hamas Attack Footage," *Los Angeles Times*, November 8, 2023, <https://web.archive.org/web/20250329182735/https://www.latimes.com/entertainment-arts/story/2023-11-08/israel-hamas-oct-7-terror-attack-footage-museum-of-tolerance-bearing-witness>.
- 16 Guy Finnes, "#HamasIsSIS?: Assessing the Campaign Comparing Proscribed Groups," *Institute for Strategic Dialogue*, November 28, 2023, https://web.archive.org/web/20250919141320/https://www.isdglobal.org/digital_dispatches/hamasisis-assessing-the-campaign-comparing-proscribed-groups/.
- 17 Israel (@Israel), post on X, August 7, 2024, <https://x.com/Israel/status/1953401185072746829>; Shannon Bond, "Civilian Deaths Are Being Dismissed as 'Crisis Actors' in Gaza and Israel," *NPR*, Morning Edition, November 27, 2023, <https://web.archive.org/web/20251017215149/https://www.npr.org/2023/11/27/1214451419/civilian-deaths-are-being-dismissed-as-crisis-actors-in-gaza-and-israel>; Marc Owen Jones, "Evidencing Alethocide: Israel's War on Truth in Gaza," *Third World Quarterly* (2025): 1–18.
- 18 Israel Defense Forces (@IDF), post on X, November 12, 2023, <https://x.com/IDF/status/1723665392525021439>.
- 19 Jorge Fitz-Gibbon, "Arabic Copy of Adolf Hitler's Mein Kampf Found Inside Child's Room in Gaza," *New York Post*, November 12, 2023, <https://web.archive.org/web/20250724211744/https://nypost.com/2023/11/12/news/arabic-copy-of-adolf-hitlers-mein-kampf-found-inside-childs-room-in-gaza/>; Itamar Eichner, "הרצוג חשף: ספרו של היטלר נמצא בחדר ילדים ששימש כבסיס טרור בעזה" ["Herzog Reveals: Hitler's Book Found in a Child's Room Used as a Terror Base in Gaza"], *Ynet*, November 12, 2023, <https://web.archive.org/web/20250318151137/https://www.ynet.co.il/news/article/bj0kvfaq6>.
- 20 Leonard Rubenstein, "Israel's Rewriting of the Law of War," *Just Security*, December 21, 2023, <https://web.archive.org/web/20250906185136/https://www.justsecurity.org/90789/israels-rewriting-of-the-law-of-war/>.
- 21 Israel (@Israel), post on X, November 8, 2023, <https://x.com/Israel/status/1722323218428551235>.
- 22 Emanuel Fabian and *Times of Israel* Staff, "Hamas's Main Operations Base Is Under Shifa Hospital in Gaza City, Says IDF," *Times of Israel*, October 27, 2023, <https://web.archive.org/web/20251010083957/https://www.timesofisrael.com/hamass-main-operations-base-is-under-shifa-hospital-in-gaza-city-says-idf/>; Israel Defense Forces (@IDF), post on X, October 27, 2023, <https://x.com/IDF/status/1717911686026268831>.
- 23 Israel Defense Forces, "Prevention of Large-Scale Hezbollah Attack," IDF website, n.d., archived October 7, 2024, <https://web.archive.org/web/20241007094450/https://www.idf.il/en/mini-sites/prevention-of-large-scale-hezbollah-attack/>; Israel Defense Forces (@IDF), post on X, August 21, 2024, <https://x.com/IDF/status/1826268507585028292>.
- 24 Avichay Adraee (@AvichayAdraee), post on X, October 9, 2023, <https://x.com/AvichayAdraee/status/1711326563004723314>.
- 25 Israel Defense Forces, "Hamas Continues to Use the Residents of Gaza as Human Shields," IDF website, October 26, 2023, <https://www.idf.il/en/mini-sites/israel-at-war/war-on-hamas-2023-resources/hamas-continues-to-use-the-residents-of-the-gaza-as-human-shields/>.

- 26 Derek B. Johnson, "Israeli Influence Operation Highlights Global Disinformation Industry," *CyberScoop*, June 5, 2024, <https://web.archive.org/web/20250714150953/https://cyberscoop.com/israel-influence-operations-stoic/>.
- 27 Meta, *Adversarial Threat Report: First Quarter*, by Margarita Franklin, Lindsay Hundley, Mike Torrey, David Agranovich, and Mike Dvilyanski (Meta, 2024), <https://web.archive.org/web/20251011000214/https://md.teyit.org/file/meta-threat-report.pdf>; Fake Reporter, Pro-Israeli Influence Network, November 2023–March 2024 (Fake Reporter, March 19, 2024), <https://web.archive.org/web/20251023014942/https://img.haarets.co.il/bs/0000018e-6fde-ddf4-a3de-6ffe56380000/0a/34/69bc45d64be4a21a215531725951/pro-israeli-influence-network-report-march-2024.pdf>.
- 28 Sheera Frenkel, "Israel Secretly Targets U.S. Lawmakers With Influence Campaign on Gaza War," *New York Times*, June 5, 2024, <https://web.archive.org/web/20251022201840/https://www.nytimes.com/2024/06/05/technology/israel-campaign-gaza-social-media.html>.
- 29 Avichay Adraee (@AvichayAdraee), posts on X, October 17, 2024, and June 1, 2025, <https://x.com/AvichayAdraee/status/1847009876465115376>; <https://x.com/AvichayAdraee/status/1929094550607352025>.
- 30 Associated Press, "Hamas Claims Military Chief Survived Israeli Strike," *Politico*, July 14, 2024, <https://web.archive.org/web/20240715024504/https://www.politico.com/news/2024/07/14/hamas-military-chief-israeli-strike-00168106>.
- 31 Eugenia Yosef, "Israel's Netanyahu Acknowledges Pager Attack, Says He Sees 'Eye-to-Eye' with Trump on Iran," CNN, November 10, 2024, <https://web.archive.org/web/20250202123456/https://www.cnn.com/2024/11/10/middleeast/israel-netanyahu-pager-trump-intl-latam>; Sheera Frenkel and Ronen Bergman, "Israel Planted Explosives in Pagers Sold to Hezbollah, Officials Say," *New York Times*, September 17, 2024, <https://web.archive.org/web/20251022031403/https://www.nytimes.com/2024/09/17/world/middleeast/israel-hezbollah-pagers-explosives.html>; Ynet News, "Retired Mossad Agents to Reveal Secrets of Hezbollah Pager Operation in U.S. Interview," Ynet, December 19, 2024, <https://web.archive.org/web/20250906080426/https://www.ynetnews.com/article/s1tom6wbjg>.
- 32 Charbel Mallo, Tamara Qiblawi, Jeremy Diamond, Lauren Kent, Rob Picheta, Christian Edwards, and Helen Regan, "Israel Behind Deadly Pager Explosions That Targeted Hezbollah and Injured Thousands in Lebanon," CNN, September 17, 2024, <https://web.archive.org/web/20250321161226/https://edition.cnn.com/2024/09/17/middleeast/lebanon-hezbollah-pagers-explosions-intl>; "Hezbollah Blames Israel after Pager Explosions Kill Nine and Injure Thousands in Lebanon," *BBC News*, September 18, 2024, <https://web.archive.org/web/20251015071928/https://www.bbc.com/news/articles/cd7xnelvpepo>; Laila Bassam and Tom Perry, "Pager Attack Throws Hezbollah into Disarray," Reuters, September 18, 2024, <https://www.reuters.com/world/middle-east/pager-attack-throws-hezbollah-into-disarray-2024-09-18/>.
- 33 Amal Chmouny, "The Impact of Israeli Cyber Operations on Hezbollah," *Arab Center Washington DC*, April 2, 2025, <https://web.archive.org/web/20250825083409/https://arabcenterdc.org/resource/the-impact-of-israeli-cyber-operations-on-hezbollah/>.
- 34 Israeli Prime Minister (Farsi) (@israelipm_farsi), post on X, June 1, 2023, https://x.com/israelipm_farsi/status/1664331795729358852; Hananya Naftali (@hananyanaftali), video on TikTok, March 10, 2023, <https://vm.tiktok.com/ZMSBNonrJ/>.
- 35 Original in Persian: Israel in Farsi (@IsraelinFarsi), post in Persian on Instagram, June 12, 2025, <https://www.instagram.com/p/DK0sjUionbO/>; Israel in Farsi (@IsraelinFarsi), post on Telegram, August 8, 2025, <https://t.me/IsraelinFarsi/9804>.
- 36 State of Israel (@israel), videos on TikTok, <https://www.tiktok.com/@israel/video/7280237773662080274>; <https://www.tiktok.com/@israel/video/7186705426124213505>; Israel Katz (@Israel_katz), post on X, August 14, 2024, https://x.com/Israel_katz/status/1823685918932238629.
- 37 Original in Persian: Israel in Persian (@IsraelPersian), post on X, October 4, 2024, <https://x.com/IsraelPersian/status/1842169011292794927>; Israel Katz (@Israel_katz), post on X, August 14, 2024, https://x.com/Israel_katz/status/1823685918932238629.
- 38 "Israel Ramps Up Psychological Warfare on Lebanon with Drone Broadcasts," *New Arab*, August 9, 2024, <https://web.archive.org/web/20250520185648/https://www.newarab.com/news/israel-ramps-psychological-warfare-lebanon-broadcasts>.
- 39 "Here Are the Propaganda Leaflets Israel Is Currently Dropping over Gaza," *Drop Site News*, January 8, 2025, <https://web.archive.org/web/20250905114659/https://www.dropsitenews.com/p/here-are-the-propaganda-leaflets>; Jason Burke, "Israel Drops Leaflets in Gaza Offering Reward for Hostage Information," *Guardian*, October 24, 2023, <https://web.archive.org/web/20250803065824/https://www.theguardian.com/world/2023/oct/24/israel-drops-leaflets-in-gaza-offering-reward-for-hostage-information>.
- 40 "Here Are the Propaganda Leaflets Israel Is Currently Dropping over Gaza," *Drop Site News*.
- 41 Richard Sanders and Al Jazeera Investigative Unit, "October 7: Forensic Analysis Shows Hamas Abuses, Many False Israeli Claims," Al Jazeera, March 21, 2024, <https://www.aljazeera.com/news/2024/3/21/october-7-forensic-analysis-shows-hamas-abuses-many-false-israeli-claims>; Casey Tolan, Audrey Ash, Isabelle Chapman, and Curt Merrill, "Slain Hamas Militants' Body Camera Videos Show the Preparation and Tactics Behind Their Terror Attack on Israel," CNN, October 26, 2023, <https://web.archive.org/web/20240621025519/https://www.cnn.com/interactive/2023/middleeast/hamas-attack-body-cam-videos-invs-dg/>.

- 42 Li Cohen, "Israeli Woman Learned of Grandmother's Killing on Facebook—After Militant Uploaded a Video of Her Body," *CBS News*, October 11, 2023, <https://www.cbsnews.com/news/mor-bayder-grandmother-killed-hamas-attack-facebook-video/>; Sheera Frenkel and Tiffany Hsu, " Hamas Took Hostages. Social Media Spread Their Stories," *New York Times*, October 17, 2023, <https://web.archive.org/web/20231018000000/https://www.nytimes.com/2023/10/17/technology/hamas-hostages-social-media.html>.
- 43 Human Rights Watch, *Israel/Palestine: Videos of Hamas-Led Attacks Verified* (October 18, 2023), <https://www.hrw.org/news/2023/10/18/israel/palestine-videos-hamas-led-attacks-verified>; " Hamas Telegram in the Immediate Wake of Their 7 October Terrorist Attacks—Propaganda Content," *VoxPol*, November 16, 2023, <https://voxpoleu/hamas-telegram-in-the-immediate-wake-of-their-7-october-terrorist-attacks-part-2-propaganda-content/>; Despoina Antonakaki and Sotiris Ioannidis, *Israel-Hamas War through Telegram, Reddit and Twitter*, arXiv (January 30, 2025), <https://arxiv.org/abs/2502.00060>.
- 44 Israel Wullman, "Head of the National Cyber Directorate: 'We Are Working to Prevent Harm to IDF Capabilities and to Protect Critical Infrastructure,'" Mamon (*Ynet*), October 24, 2023, <https://web.archive.org/web/20231024150530/https://www.ynet.co.il/digital/article/yokra13644424>; " Hamas Supporters Hack Maccabi Tel Aviv Basketball Club Website," *Ynet Sports*, November 6, 2023, <https://www.ynet.co.il/sport/israelibasketball/article/syjtbgp7t>.
- 45 Wullman, "Head of the National Cyber Directorate."
- 46 Raphael Kahan, " Hamas Hackers Are Trying to Scare Israelis with Fake SMS Messages and News Sites," *Ynetnews*, October 25, 2023, <https://www.ynetnews.com/business/article/hjoy4f8mp>.
- 47 Raphael Kahan, "Fake SMS Messages and Websites: Hackers in the Service of Hamas Attempt to Scare Israelis," *Ynet* (Digital/Tech News), October 24, 2023, <https://www.ynet.co.il/digital/technews/article/hyjiwssfa>.
- 48 Omer Yoachimik and Jorge Pacheco, "Cyber Attacks in the Israel–Hamas War," *Cloudflare Blog*, October 23, 2023, <https://blog.cloudflare.com/cyber-attacks-in-the-israel-hamas-war/>.
- 49 Andrew Carey, Lianne Kolirin, and Tara John, " Hamas Says Two Israeli Hostages Are Dead, as IDF Calls Videos 'Psychological Torment' of Captives' Families," *CNN*, January 16, 2024, <https://www.cnn.com/2024/01/16/middleeast/israel-hamas-hostages-video-psychological-torment-intl>; Mike Schwartz and Sophie Tanno, "Israel Investigating after Hamas Releases Photos Purportedly Showing Body of Female Hostage," *CNN*, November 24, 2024, <https://www.cnn.com/2024/11/24/middleeast/israel-hamas-says-hostage-dead-intl-latam>.
- 50 Rami Amichay and Lili Bayer, "Israelis Stage Nationwide Protests to Demand End to Gaza War and Release of Hostages," *Reuters*, August 17, 2025, <https://www.reuters.com/world/middle-east/israelis-stage-nationwide-protests-demand-end-gaza-war-release-hostages-2025-08-17/>.
- 51 Anna Foster, "Keith Siegel and Omri Miran: Video Shows U.S. and Israeli Hostages Alive in Gaza," *BBC News*, April 27, 2024, <https://www.bbc.com/news/world-middle-east-68913568>; *Times of Israel* Staff, " Hamas Hostage Video Shows Maxim Herkin and Bar Kuperstein, in First Signs of Life," *Times of Israel*, April 5, 2025, <https://www.timesofisrael.com/hamas-hostage-video-shows-maxim-herkin-and-bar-kupershtein-in-first-signs-of-life/>; *Agence France-Presse*, " Hamas Releases Video Showing Israeli-American Hostage Alive," *Arab News*, April 12, 2025, <https://www.arabnews.com/node/2596806/middle-east>.
- 52 Avi Ashkenazi, " Hamas Releases Hostage Videos: The Goal Is to Pressure Netanyahu into a Comprehensive Deal," *Maariv*, December 7, 2024, <https://www.maariv.co.il/news/military/article-1154306>; Dan Raban, Lihi Gordon, Hagar Kochavi, Gaia Zohar, Einav Halabi, and Itamar Eichner, "Sign of Life: Hamas Publishes Video of Abducted Soldier Edan Alexander," *Ynet*, April 12, 2025, <https://www.ynet.co.il/news/article/r1oeuy00cyx>; Melanie Lidman, "A Father's Agony over Video of His Emaciated Son, a Hostage in Gaza, Adds Pressure for a Ceasefire," *Associated Press*, August 4, 2025, <https://apnews.com/article/israel-palestinians-gaza-hamas-hostages-hunger-videos-c9951a33a7f8d47d4ad77705d1267fbd>; Luc Bronner, "Macabre Video of the Last Hostages Held by Hamas Shocks Israel," *Le Monde*, August 4, 2025, https://www.lemonde.fr/en/international/article/2025/08/04/macabre-video-of-the-last-hostages-held-by-hamas-shocks-israel_6744051_4.html.
- 53 Darren Loucaides, "How Telegram Became a Terrifying Weapon in the Israel–Hamas War," *Wired*, October 31, 2023, <https://www.wired.com/story/telegram-hamas-israel-conflict/>.
- 54 Clare Duffy and Brian Fung, "Messaging App Telegram Restricts Access to Some Hamas-Run Channels," *CNN*, October 26, 2023, <https://www.cnn.com/2023/10/26/tech/telegram-blocking-hamas-accounts>.
- 55 Darren Loucaides, "How Telegram Became a Terrifying Weapon in the Israel–Hamas War," *Wired*, October 31, 2023, <https://www.wired.com/story/telegram-hamas-israel-conflict/>; Gaza Now—Arabic, Telegram channel, <https://t.me/s/gazaalannet/65484>.
- 56 " Hamas Says October 7 Attack Was a 'Necessary Step,' Admits to 'Some Faults,'" *Al Jazeera*, January 21, 2024, <https://www.aljazeera.com/news/2024/1/21/hamas-says-october-7-attack-was-a-necessary-step-admits-to-some-faults>; Menachem Klein, " Hamas's Narrative of 7 October and the Impossibility of Ignoring It," *Istituto Affari Internazionali (IAI)*, February 9, 2024, <https://www.iai.it/en/publications/c05/hamass-narrative-7-october-and-impossibility-ignoring-it>.
- 57 Max Zahn, "Israel-Hamas War: Tech Platforms Under Scrutiny over Spread of False, Graphic Posts," *ABC News*, October 16, 2023, <https://abcnews.com/Business/israel-hamas-war-tech-platforms-scrutiny-spread-false/story?id=103954236>.

- 58 *Disinformation— Hamas-Israel War*, Cyabra, October 24, 2023, <https://cyabra.com/reports/disinformation-hamas-israel-war/>; David D. Kirkpatrick and Adam Rasgon, “The Hamas Propaganda War: Across the Arab World, the Group Is Successfully Selling Its Narrative of Resistance,” *New Yorker*, October 30, 2023, <https://www.newyorker.com/news/news-desk/the-hamas-propaganda-war>; Eric Cortellessa, “The Oct. 7 Massacre Revealed a New Hamas Social Media Strategy,” *Time*, October 31, 2023, <https://time.com/6330005/the-oct-7-massacre-revealed-a-new-hamas-social-media-strategy/>.
- 59 Cyabra, *Disinformation— Hamas-Israel War*; David D. Kirkpatrick and Adam Rasgon, “The Hamas Propaganda War”; Eric Cortellessa, “The Oct. 7 Massacre Revealed a New Hamas Social Media Strategy.”
- 60 Rotem Baruchin, “1 in 4 Profiles Are Pro-Hamas Fake Accounts: The Online Battlefield,” *Cyabra Blog*, October 11, 2023, <https://cyabra.com/blog/1-of-4-pro-hamas-profiles-are-fake-the-online-battlefront>.
- 61 Drew Harwell and Elizabeth Dwoskin, “Hamas Turns to Social Media to Get Its Message Out—and to Spread Fear,” *Washington Post*, October 18, 2023, <https://www.washingtonpost.com/technology/2023/10/18/hamas-social-media-terror/>; Matt Berg, “NYT Admits Error in Gaza Hospital Report,” *Politico*, October 23, 2023, <https://www.politico.com/news/2023/10/23/gaza-hospital-new-york-times-00122986>.
- 62 Hamas, “Hamas: A Document of General Principles and Policies” (May 1, 2017), <https://israeled.org/hamas-a-document-of-general-principles-policies/>; “Hamas New Policy Document 010517” (PDF), esp. sections framing the struggle as anti-occupation/anti-colonial and calling for prosecution of “war criminals,” <https://palwatch.org/storage/documents/hamas%20new%20policy%20document%20010517.pdf>; “Doctrine of Hamas,” Wilson Center, October 20, 2023, <https://www.wilsoncenter.org/article/doctrine-hamas>; Shibley Telhami, “The Nationalist Versus the Religious: Implications for Peace with Hamas,” *Brookings*, March 18, 2014, <https://www.brookings.edu/articles/the-nationalist-versus-the-religious-implications-for-peace-with-hamas/>; Devorah Margolin, “A Major Pivot in Hamas Strategy,” *Washington Institute for Near East Policy*, October 16, 2023, <https://www.washingtoninstitute.org/policy-analysis/major-pivot-hamas-strategy>.
- 63 Tasnim News Agency (Persian) (@tasnimnews_fa), post on X, October 7, 2023, https://x.com/tasnimnews_fa/status/1710641145363972499.
- 64 Reuters Fact Check, “Fact Check: Handcuffed Men in Video Are Karabakh Ex-Leaders, Not Israeli Generals,” *Reuters*, October 11, 2023, <https://www.reuters.com/fact-check/handcuffed-men-video-are-karabakh-ex-leaders-not-israeli-generals-2023-10-11/>.
- 65 Ali Khamenei (Hebrew-language account) (@Khamenei_Heb), profile on X, https://x.com/Khamenei_Heb.
- 66 Ali Khamenei (Hebrew-language account) (@Khamenei_Heb), post in Hebrew on X, October 27, 2024, https://x.com/Khamenei_Heb/status/1850596556661248131.
- 67 Dov Gil-Har, “Khamenei Opened a Hebrew-Language X Account and Posted His First Tweet—Israelis Were Quick to Respond,” *KAN News*, October 26, 2024, <https://www.kan.org.il/content/kan-news/global/816809/>.
- 68 Raphael Kahan, “Foreign Hacktivists Pretend to Be Home Front Command to Infiltrate Israeli Phones,” *Ynetnews*, October 29, 2024, <https://www.ynetnews.com/business/article/hjnwgo0l1g>.
- 69 Omer Benjakob, “Israel Says Hezbollah, Iran Sent Millions of Messages to Israelis in Bid to Cause Panic,” *Haaretz*, September 19, 2024, <https://www.haaretz.com/israel-news/security-aviation/2024-09-19/ty-article/.premium/israelis-receive-threatening-messages-with-virus-laden-links-from-fraudulent-sources/00000192-09c8-db47-a7bf-e9d8c2550000>.
- 70 Omer Benjakob, “Israel Says Hezbollah, Iran Sent Millions of Messages to Israelis in Bid to Cause Panic,” *Haaretz*, September 19, 2024, <https://www.haaretz.com/israel-news/security-aviation/2024-09-19/ty-article/.premium/israelis-receive-threatening-messages-with-virus-laden-links-from-fraudulent-sources/00000192-09c8-db47-a7bf-e9d8c2550000>; Raphael Kahan, “National Cyber Directorate Confirms: Malicious SMS Campaign Originated from Iran and Hezbollah,” *Ynet* (Digital/Tech News), September 19, 2024, <https://www.ynet.co.il/digital/technews/article/hkh2snkar>.
- 71 Fake Reporter (@FakeReporter), post on X, November 26, 2023, <https://x.com/FakeReporter/status/1728768973670338563>; Omri Barak, “An Incitement Campaign Exploiting the Pain of Hostages’ Families—Originating Abroad,” *Mako*, November 24, 2023, <https://www.mako.co.il/news-military/6361323ddea5a810/Article-59c4d2a4fedfb81026.htm>.
- 72 Ari Ben Am, “A Year of Meming Dangerously: Iranian Influence Operations Targeting Israel Since October 7,” *Foundation for Defense of Democracies*, August 28, 2025, <https://www.fdd.org/analysis/2025/08/28/a-year-of-meming-dangerously-iranian-influence-operations-targeting-israel-since-october-7/>.
- 73 Cardiff University, *The Internet Research Agency in Europe, 2014–2016*, n.d., https://www.cardiff.ac.uk/_data/assets/pdf_file/0007/2733325/The-Internet-Research-Agency-In-Europe-2014-2016.pdf.
- 74 Fake Reporter (@FakeReporter), post on X, June 13, 2025, <https://x.com/FakeReporter/status/1944362834193768515>.
- 75 Fake Reporter (@FakeReporter), post on X, November 26, 2023, <https://x.com/FakeReporter/status/1728768973670338563>.
- 76 Microsoft Threat Intelligence, “Iran Surges Cyber-Enabled Influence Operations in Support of Hamas,” *Microsoft Security Insider*, February 26, 2024, <https://www.microsoft.com/en-us/security/security-insider/threat-landscape/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas/>.

- 77 Mazhar Farooqui, "UAE: Cyberattack Disrupts TV Services, Rattles Some Residents with Graphic Content from Gaza," *Khaleej Times*, December 11, 2023, <https://www.khaleejtimes.com/uae/uae-cyberattack-disrupts-tv-services-rattles-some-residents-with-graphic-content-from-gaza>.
- 78 Microsoft Threat Intelligence, "Exposed and Vulnerable: Recent Attacks Highlight Critical Need to Protect Internet-Exposed OT Devices," *Microsoft Security Blog*, May 30, 2024, <https://www.microsoft.com/en-us/security/blog/2024/05/30/exposed-and-vulnerable-recent-attacks-highlight-critical-need-to-protect-internet-exposed-ot-devices/>.
- 79 Cybersecurity and Infrastructure Security Agency (CISA), "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities," December 18, 2024, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>.
- 80 Office of the Director of National Intelligence (ODNI), "Statement from Director of National Intelligence Avril Haines on Recent Iranian Influence Efforts," press release no. 17-24, July 9, 2024, <https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2024/3842-statement-from-director-of-national-intelligence-avril-haines-on-recent-iranian-influence-efforts>.
- 81 Ali Khamenei, "As the Page of History Is Turning, You Are Standing on the Right Side of It," English-language website of the Office of the Supreme Leader of Iran, May 30, 2024, <https://english.khamenei.ir/news/10823/As-the-page-of-history-is-turning-you-are-standing-on-the-right>.
- 82 Farhad Souzanchi, "Iran's Futile but Revealing Attempts to Influence U.S. Campus Protests," *Time*, September 9, 2024, <https://time.com/7010673/irans-footprint-in-university-protests-is-light-but-revealing/>.
- 83 Daniel Byman and Emma McCaleb, "Understanding Hamas's and Hezbollah's Uses of Information Technology," brief, Center for Strategic and International Studies, n.d., <https://www.csis.org/analysis/understanding-hamass-and-hezbollahs-uses-information-technology>; A. Monnier, "Hezbollah's Use of Social Media: Communication Strategy and Impact on Public Opinion," *Hermès, La Revue* 94, no. 2 (2024): 217–22, <https://shs.cairn.info/journal-hermes-la-revue-2024-2-page-217?lang=en>.
- 84 David Daoud, "After a Failed Attack, Hezbollah's Propaganda Seeks to Prevent a Wider War with Israel," *Atlantic Council*, August 25, 2024, <https://www.atlanticcouncil.org/blogs/menasource/hezbollah-shukur-israel-preemptive-strike/>.
- 85 Yair Kraus, "Hezbollah Journalist's Threat Against the Head of the Moshav: 'The Donkey Is More Precious than Pearls,'" *Ynet*, January 27, 2024, <https://www.ynet.co.il/news/article/bk5ryxqca>.
- 86 Raphael Kahan, "Hezbollah Attempted to Run an Intimidation Campaign Against Israelis on Telegram," *Ynet*, August 25, 2024, <https://www.ynet.co.il/digital/technews/article/sywjwudi0>; Shaked Sadeh, "'We Have Hacked the Port of Haifa, You Have Little Time to Leave': Iran and Hezbollah Deliver an Unusual Message to Israel," *Maariv*, October 21, 2024, <https://www.maariv.co.il/news/military/article-1141834>; Reuters, "Lebanon's Hezbollah Publishes Drone Footage Claiming to Show Surveillance of Israel's Haifa," Reuters, June 18, 2024, <https://www.reuters.com/world/middle-east/lebanons-hezbollah-publishes-drone-footage-claiming-show-surveillance-israels-2024-06-18/>.
- 87 Ari Ben Am, "Meta Dismantles Iranian and Hezbollah Influence Operations Targeting Israel," Policy Brief, *Foundation for Defense of Democracies*, December 18, 2024, <https://www.fdd.org/analysis/2024/12/18/meta-dismantles-iranian-and-hezbollah-influence-operations-targeting-israel/>; Meta, *Third Quarter Meta Adversarial Threat Report*, by Margarita Franklin and Mike Torrey, Q3 2024, <https://transparency.meta.com/sr/Q3-2024-Adversarial-threat-report/>.
- 88 Shlomi Heller and Bini Ashkenasy, "Lebanon-Linked Operators Run Fake Israeli 'News Site,' Spread Anti-Israel Sentiments—Exclusive," *Jerusalem Post*, April 18, 2024, <https://www.jpost.com/israel-news/article-797725>.
- 89 Nadwa Al-Dawsari, "Armed Groups in Context: The Houthis—From Local Insurgency to Regional (Non-State) Powerhouse Shaping Middle East Dynamics," *Armed Groups and International Law*, January 14, 2025, <https://www.armedgroups-internationalallaw.org/2025/01/14/the-houthis-from-local-insurgency-to-regional-non-state-powerhouse-shaping-middle-east-dynamics/>.
- 90 Hezam al-Asad (@hezamalasad), post on X, October 27, 2023, <https://x.com/hezamalasad/status/1717986495808544969>; "'Eilat': The Houthis' Threat After the Interception of Drones from Yemen, in a Single Word," *Ynet*, October 27, 2023, <https://www.ynet.co.il/news/article/ryiqe6tzip>.
- 91 Reuters, "Yemen's Houthis Say They Will Attack if U.S. and Israel Try to Displace Gazans," Reuters, February 13, 2025, <https://www.reuters.com/world/middle-east/yemens-houthis-say-they-will-attack-if-us-israel-try-displace-gazans-2025-02-13/>.
- 92 "Houthis Launch Large Number of Drones at Targets in Israel," *Middle East Monitor*, November 2, 2023, <https://www.middleeastmonitor.com/20231102-houthis-launch-large-number-of-drones-at-targets-in-israel/>; "Israel Says It Thwarted Aerial Attacks by Yemen's Houthis near Red Sea," *Saudi Gazette*, November 1, 2023, <https://saudigazette.com.sa/article/637270/World/Mena/Israel-says-it-thwarted-aerial-attacks-by-Yemens-Houthis-near-Red-Sea>.
- 93 Reuters Fact Check, "Fact Check: Video Game Footage Mislabeled as Showing Houthis Striking U.S. Fighter Jet," Reuters, January 17, 2024, <https://www.reuters.com/fact-check/video-game-footage-mislabeled-showing-houthis-striking-us-fighter-jet-2024-01-17/>.
- 94 "Houthi Claims of Attack on U.S. Aircraft Carrier Are False, U.S. Officials Say," CNBC, June 23, 2024, <https://www.cnbc.com/2024/06/23/houthi-claims-of-attack-on-us-aircraft-carrier-are-false-us-officials-say.html>.

- 95 “Celebrity News” (חדשות סלבריטאים), Facebook page, accessed January 24, 2026, <https://www.facebook.com/people/חדשות-סלבריטאים/61571412401564/> [account removed by Meta].
- 96 ClearSky Cyber Security, *Houthi-Yemeni Influence Campaign*, April 2025, <https://www.clearskysec.com/wp-content/uploads/2025/04/Houthi-Influence-Campaign-april-2025.pdf>.
- 97 See posts by @IDF, @netanyahu, and @Israel during June 2025: <https://x.com/IDF/status/1933506910155571331>, <https://x.com/IDF/status/1936743187340521933>, <https://x.com/IDF/status/1935656241935655240>, <https://x.com/IDF/status/1934063573040525765>, <https://x.com/netanyahu/status/1933340443343008068>, <https://x.com/Israel/status/1933831563155775577>, <https://x.com/Israel/status/1934604041012883518>, <https://x.com/Israel/status/1934166230367178892>, <https://x.com/IDF/status/1841167289984397726>, <https://x.com/netanyahu/status/1933922050319515656>, <https://x.com/IDF/status/1934151460079423867>.
- 98 Ali Khamenei (@khamenei_ir); Iranian Ministry of Foreign Affairs (@IRIMFA_EN); Masoud Pezeshkian (@drpezheshkian): https://x.com/khamenei_ir/status/1933364668581531876, https://x.com/khamenei_ir/status/1938317802085011526, https://x.com/khamenei_ir/status/1933366210072064505, https://x.com/IRIMFA_EN/status/1935988334637007336, <https://x.com/drpezheshkian/status/1942235569796334060>, <https://x.com/drpezheshkian/status/1942235572434559089>, <https://x.com/drpezheshkian/status/1942235581259382884>, <https://x.com/drpezheshkian/status/1942235585693012222>.
- 99 Benjamin Netanyahu, “Moments ago, Israel launched Operation ‘Rising Lion’...,” X, June 12, 2025, <https://x.com/netanyahu/status/1933340443343008068>.
- 100 Khamenei Media (@Khamenei_m), “The Zionist regime will not escape safely from the heinous crime they’ve committed,” X, June 13, 2025, https://x.com/Khamenei_m/status/1933609273914704173.
- 101 Benjamin Netanyahu (@netanyahu), post on X, June 12, 2025, <https://x.com/netanyahu/status/1933340443343008068>.
- 102 Ali Khamenei (@khamenei_ir), post on X, June 12, 2025, https://x.com/khamenei_ir/status/1933364668581531876; Ali Khamenei (@khamenei_ir), post on X, June 13, 2025, https://x.com/Khamenei_m/status/1933609273914704173.
- 103 Israel Persian (@IsraelPersian), post on X, June 17, 2025, <https://x.com/IsraelPersian/status/1935040122350711195>.
- 104 Benjamin Netanyahu (@netanyahu), post on X, June 13, 2025, <https://x.com/netanyahu/status/1933626898242056488>.
- 105 Israel Persian (@IsraelPersian), post on X, June 22, 2025, <https://x.com/IsraelPersian/status/1936714390512046370>.
- 106 The Voice Truth (@thevoicetruth1), post on X, June 18, 2025, <https://x.com/thevoicetruth1/status/1935352391232049340>; “Israel Is Giving the Iranian People Hope for Freedom After 46 Years of Oppression,” video posted on Facebook, June 19, 2025, <https://www.facebook.com/61572988572963/videos/israel-is-giving-the-iranian-people-hope-for-freedom-after-46-years-of-oppression/621813590923342/>.
- 107 Steven Lee Myers, Natan Odenheimer, and Erika Solomon, “Israel and Iran Usher In New Era of Psychological Warfare,” *New York Times*, July 15, 2025, <https://www.nytimes.com/2025/07/15/technology/israel-iran-psychological-warfare.html>; Islamic Republic News Agency (IRNA), “جاسوسی و تخلیه اطلاعاتی موساد با ترفند ارائه مشاوره پزشکی,” July 10, 2025, <https://www.irna.ir/news/85884713/>; Mossad Farsi (@MossadSpokesman), post on X, June 26, 2025, <https://x.com/MossadSpokesman/status/1938143332057641029>; Mossad Farsi (@MossadSpokesman), post on X, July 25, 2025, <https://x.com/MossadSpokesman/status/1948762030426513786>; Mossad Farsi (@MossadSpokesman), post on X, July 27, 2025, <https://x.com/MossadSpokesman/status/1949505874784813167>.
- 108 Mahsa Alimardani and Sam Gregory, “Iran–Israel AI War Propaganda Is a Warning to the World,” *Carnegie Endowment for International Peace*, July 28, 2025, <https://carnegieendowment.org/research/2025/07/iran-israel-ai-war-propaganda-is-a-warning-to-the-world?lang=en>; Steven Lee Myers, Natan Odenheimer, and Erika Solomon, “Israel and Iran Usher In New Era of Psychological Warfare,” *New York Times*, July 15, 2025, <https://www.nytimes.com/2025/07/15/technology/israel-iran-psychological-warfare.html>.
- 109 Raphael Kahan, “How Iran Is Trying to Break Israel—Without Firing a Single Bullet,” *Ynet*, July 8, 2025, <https://www.ynet.co.il/digital/technology/article/sjc9kfcsee>.
- 110 A. Akhundpur (@AAkhundpur), post on X, June 19, 2025, <https://x.com/AAkhundpur/status/1935766714199031903>.
- 111 Attack Alarm (@Attack_Alarm), post on Telegram, June 15, 2025, https://t.me/Attack_Alarm/463.
- 112 Our Right IL+ (@Ourright_ILPlus), post on Telegram, June 21, 2025, https://t.me/Ourright_ILPlus/1758; Car Online X (@caronlineX), post on X, June 17, 2025, <https://x.com/caronlineX/status/1936282659635802262>.
- 113 SEPAH Cybery (@SEPAHCYBERY), post on Telegram, June 14, 2025, <https://t.me/SEPAHCYBERY/118725>; Israel News 134 (@israel.news134), photo post on TikTok, June 15, 2025, <https://www.tiktok.com/@israel.news134/photo/7516103917235621125>.
- 114 Car Online X (@caronlineX), posts on X, <https://x.com/caronlineX/status/1935667147155341762>; <https://x.com/caronlineX/status/1935466341835694406>.
- 115 CryptoLiftX, “We Love Israel!,” video post, X, June 18, 2025, <https://x.com/CryptoLiftX/status/1935352391232049340>.
- 116 Kathrin Wesolowski and Adnan Sidibe, “Fact Check: Protests Against the Israel-Iran Conflict?” *Deutsche Welle*, June 20, 2025, <https://www.dw.com/en/fact-check-protests-against-the-israel-iran-conflict/a-72985421>.

- 117 Nikita Shah, "What the Israel–Iran Conflict Revealed about Wartime Cyber Operations," *Atlantic Council*, July 30, 2025, <https://www.atlanticcouncil.org/blogs/new-atlanticist/what-the-israel-iran-conflict-revealed-about-wartime-cyber-operations/>.
- 118 Yonah Jeremy Bob, "Iran Has Attacked Every Israeli Citizen Multiple Times, New Cyber Chief Yossi Karadi Says," *Jerusalem Post*, December 9, 2025, <https://www.jpost.com/israel-news/defense-news/article-879689>; Joanna England, "Iranian Cyberthreats Increase by 700%: Will Shift Towards Israel, Says Google Expert," *Intelligent CISO*, June 16, 2025, <https://www.intelligentciso.com/2025/06/16/iranian-cyberthreats-increase-by-700-will-shift-towards-israel-says-google-expert/>.
- 119 Gonjeshke Darand (@GonjeshkeDarand), posts on X, <https://x.com/GonjeshkeDarand/status/1934883811327705166>; <https://x.com/GonjeshkeDarand/status/1935231054249435607>.
- 120 Michael Doran and Zineb Riboua, "Predatory Sparrow Hacks Iran's Financial System," *Wall Street Journal*, July 20, 2025, <https://www.wsj.com/opinion/predatory-sparrow-hacks-irans-financial-system-attack-stablecoins-ad6e79b5>; A. J. Vicens and James Pearson, "Suspected Israeli Hackers Claim to Destroy Data at Iran's Bank Sepah," *Reuters*, June 17, 2025, <https://www.reuters.com/world/middle-east/suspected-israeli-hackers-claim-destroy-data-irans-bank-sepah-2025-06-17/>.
- 121 Radware, "Hybrid Warfare Unfolded: Cyberattacks, Hacktivism and Disinformation in the 2025 Israel–Iran War," June 18, 2025, <https://www.radware.com/security/threat-advisories-and-attack-reports/cyberattacks-hacktivism-and-disinformation-in-the-2025-israel-iran-war/>; The New Arab Staff, "Iran-Linked Hackers Launch Wave of Cyberattacks on Israel," *New Arab*, June 16, 2025, <https://www.newarab.com/news/iran-linked-hackers-launch-wave-cyberattacks-israel/>; NSFOCUS, "The Hacktivist Cyber Attacks in the Iran–Israel Conflict," June 26, 2025, <https://nsfocusglobal.com/the-hacktivist-cyber-attacks-in-the-iran-israel-conflict/>.
- 122 *Jerusalem Post* Staff, "Israelis Receive Fake Terror Attack Warning to Trick Them into Staying Out of Bomb Shelters," *Jerusalem Post*, June 16, 2025, <https://www.jpost.com/israel-news/article-857969>; Yonah Jeremy Bob, "Iran Has Attacked Every Israeli Citizen Multiple Times, New Cyber Chief Yossi Karadi Says," *Jerusalem Post*, December 9, 2025, <https://www.jpost.com/israel-news/defense-news/article-879689>.
- 123 "Footage Released by the Mossad Claims to Show Israeli Agents in Iran—Video," *Guardian*, June 13, 2025, sourced from Reuters, <https://www.theguardian.com/world/video/2025/jun/13/footage-released-by-the-mossad-claims-to-show-israeli-agents-in-iran-video>; Dov Lieber and Andrew Dowell, "How Israel's Mossad Smuggled Drone Parts to Attack Iran From Within," *Wall Street Journal*, June 15, 2025, <https://www.wsj.com/world/middle-east/how-israels-mossad-smuggled-drone-parts-to-attack-iran-from-within-633516a9>; Israel (@Israel), post on X, April 14, 2024, <https://x.com/Israel/status/1779516650288460131>.
- 124 Ali Khamenei (@Khamenei_fa; @Khamenei_ir; @Khamenei_Heb), posts on X (Persian-, English-, and Hebrew-language accounts), https://x.com/Khamenei_fa/status/1933980263111139363; https://x.com/Khamenei_fa/status/1934698541210910816; https://x.com/Khamenei_ir/status/1938317802085011526; https://x.com/Khamenei_ir/status/1933366210072064505; https://x.com/Khamenei_ir/status/1935303824325108208; https://x.com/Khamenei_ir/status/1935315636835475632; https://x.com/Khamenei_Heb/status/1935137873939796024; https://x.com/Khamenei_Heb/status/1933612476303880219; https://x.com/Khamenei_Heb/status/193339772377764303.
- 125 SEPAH Cybery (@SEPAHCYBERY), posts on Telegram, <https://t.me/SEPAHCYBERY/117651>; <https://t.me/SEPAHCYBERY/118352>; <https://t.me/SEPAHCYBERY/118932>; <https://t.me/SEPAHCYBERY/119187>.
- 126 Myers, Odenheimer, and Solomon, "Israel and Iran Usher In New Era of Psychological Warfare"; Alimardani and Gregory, "Iran–Israel AI War Propaganda Is a Warning to the World."
- 127 *Tehran Times* (@TehranTimes79), Defa News (@Defanews_ir), and Ali Khamenei (@Khamenei_m), posts on X, <https://x.com/TehranTimes79/status/1933850991599767749>; https://x.com/Defanews_ir/status/1933842989337465341; https://x.com/Defanews_ir/status/1934538403057377718; https://x.com/Khamenei_m/status/1936060719587352591.
- 128 Israel Persian (@IsraelPersian), posts on X, <https://x.com/IsraelPersian/status/1934704021182267743>; <https://x.com/IsraelPersian/status/1934970430835527732>; <https://x.com/IsraelPersian/status/1935040122350711195>; <https://www.tiktok.com/@israel/video/7516926464726420743>.
- 129 Steven Lee Myers, Natan Odenheimer, and Erika Solomon, "Israel and Iran Usher In New Era of Psychological Warfare," *New York Times*, July 15, 2025, <https://www.nytimes.com/2025/07/15/technology/israel-iran-psychological-warfare.html>; Matt Murphy, Olga Robinson, and Shayan Sardarizadeh, "Israel–Iran Conflict Unleashes Wave of AI Disinformation," *BBC News*, June 20, 2025, <https://www.bbc.com/news/articles/c0k78715enxo>.
- 130 Arash Aryapour, "Iran's Stealth Internet Blackout: A New Model of Censorship," arXiv:2507.14183 (2025); Tia Goldenberg and Jon Gambrell, "Israel Orders Al Jazeera to Close Its Local Operation and Seizes Some of Its Equipment," *Associated Press*, May 5, 2024, <https://apnews.com/article/israel-aljazeera-amas-gaza-war-eba9416aea82f505ab908ee60d1de5e4>.
- 131 Peter Beaumont, "Network of Israeli Citizens Arrested After Spying for Iran, Police Say," *Guardian*, October 21, 2024, <https://www.theguardian.com/world/2024/oct/21/israeli-citizens-arrested-spying-for-iran-police-say>; Israel Wullman, "Fake Missiles, Phantom Pilots and Spoofed Alerts: Israel's War Against Iranian Fake News," *Ynetnews*, June 17, 2025, <https://www.ynetnews.com/tech-and-digital/article/b1pvowynce>.

- 132 Christy Cooney and Paul Adams, “Israel’s Netanyahu Condemns ‘Cruel’ Hamas Video of Israeli Hostages,” *BBC News*, October 30, 2023, <https://www.bbc.com/news/world-middle-east-67265915>; Ali Khamenei, “Message to the Iranian Nation Following Israeli Attacks,” official website of the Supreme Leader of Iran, June 13, 2025, <https://english.khamenei.ir/service/Speeches>; Yusuf Can, “Narrative Warfare: How Disinformation Shapes the Israeli-Hamas Conflict—and Millions of Minds,” *Bulletin of the Atomic Scientists*, November 27, 2023, <https://thebulletin.org/2023/11/narrative-warfare-how-disinformation-shapes-the-israeli-hamas-conflict-and-millions-of-minds/>.
- 133 See <https://transparency.meta.com/researchtools/other-data-catalogue/crowdtangle/>.
- 134 Meta, “New Tools to Support Independent Research,” Meta Newsroom, November 21, 2023, updated March 14, 2024, <https://about.fb.com/news/2023/11/new-tools-to-support-independent-research/>; Meta, “Meta Content Library and API,” Meta Transparency Center, updated April 30, 2026, <https://transparency.meta.com/researchtools/meta-content-library/>.
- 135 Joseph Menn, “Stanford’s Top Disinformation Research Group Collapses under Pressure,” *Washington Post*, June 14, 2024, <https://www.washingtonpost.com/technology/2024/06/14/stanford-internet-observatory-disinformation-research-lawsuits-politics/>; Election Integrity Partnership, “Home,” accessed May 20, 2026, <https://www.eipartnership.net/>.
- 136 Oversight Board, “AI-Generated Video in Israel-Iran Conflict,” March 10, 2026, <https://www.oversightboard.com/decision/fb-46usuh23/>.
- 137 See <https://docs.junkipedia.org>.
- 138 For more information, see <https://sightengine.com/docs/ai-generated-image-detection>.

ABOUT THE AUTHORS

TAMAR MITTS

Tamar Mitts is an Associate Professor of International and Public Affairs at Columbia University's School of International and Public Affairs and Director of the Emerging Technologies and International Security Initiative at the Institute of Global Politics. She is also affiliated with the Saltzman Institute of War and Peace Studies and the Data Science Institute. Her research examines the political consequences of information and technology, with a focus on democracy and international security. She studies how digital platforms, AI-generated media, and online information environments affect public trust, collective action, political violence, and conflict. Across this work, she combines computational methods, original data, and rigorous social science research to study politics in a rapidly changing media environment. Her work has appeared in the *American Political Science Review*, *International Organization*, *Journal of Politics*, *Proceedings of the National Academy of Sciences*, and *Science Advances*, among other outlets. She is the author of *Safe Havens for Hate: The Challenge of Moderating Online Extremism* (Princeton University Press, 2025), which received the 2026 Best Book Award in Information Technology and Politics from the American Political Science Association. At Columbia, she teaches courses on democracy and democratic erosion in the AI era, data science and public policy, and quantitative text analysis.

EDEN KADURI

Eden Kaduri is a Middle East security and peacebuilding specialist whose work focuses on information operations, regional conflict, and the strategic dynamics of the MENA region. She served as a Research Assistant at Columbia University's Saltzman Institute of War and Peace Studies and has held research roles at the Institute for National Security Studies and the Jewish Institute for National Security of America. Her experience also includes serving as an intelligence analyst and team leader in the Israel Defense Forces and advising a member of the Israeli Knesset on foreign affairs and national security. She is a Council of Women World Leaders Fellow at King's College London and has participated in regional peacebuilding initiatives through EcoPeace Middle East and Encompass Dialogue. Eden holds an MPA in Data Science for Policy from Columbia University, where she was an International Fellows Program and Institute of Global Politics Scholar, and an MA in Security and Diplomacy from Tel Aviv University, where she graduated with honors.



IGP Institute of
Global Politics

International Affairs Building
420 West 118th Street
New York, NY 10027

212-853-4720
igp.sipa.columbia.edu
igp@sipa.columbia.edu