Special Publication

Ahead of the 2026 Elections: A Report on Foreign Interference in Israeli Social Media Discourse*

David Siman-Tov, Danny Citrinowicz, Amit Cohen, Reut David, Amit Sharon, Gitit Bar-On[1] | November 1, 2026

Several foreign actors are targeting Israeli social media, particularly ahead of the October 27 Knesset elections. The most prominent actors are Iran; the Isnad network, which operates from Turkey and is associated with the Muslim Brotherhood; and the Russian influence operation Doppelgänger. They differ in their resources, structure, and motives.

The various actors are believed to share a common goal: eroding public trust in state institutions and the electoral process, as well as trust between different segments of society. Securing a victory for a particular camp or changing voting patterns is, at most, a secondary objective. Furthermore, although there is no evidence that they coordinate in Israel, they all exploit existing divisions in Israeli society—such as disagreements over the failures that led to the October 7 disaster, Haredi (ultra-Orthodox) conscription, religion and state, foreign relations, and trust in the leadership—and aim to amplify them. They target diverse audiences and sometimes contradict one another, but suspicion and despair recur throughout.

It is important to distinguish between exploiting the election period to intensify existing influence efforts and trying to interfere directly in the elections themselves. Most of the activity identified falls into the first category: it seeks to undermine Israeli public trust and social resilience over time. The election cycle serves as a window of opportunity to intensify existing influence efforts by exploiting more heated political discourse, sharper social divisions, and greater public attention to political issues.

---

[1] Dr. Gitit Bar-On is the Deputy Director of the FakeReporter research initiative. Amit Sharon is a researcher at the initiative.

Internal disagreement is a normal and legitimate component of democratic discourse. The problem arises when a hostile foreign actor impersonates Israelis, radicalizes these disagreements, and injects its voice into domestic debate, making it hard to discern who is really behind the claims and where they originate.

Iran is a well-known actor operating in social media discourse during the previous Knesset elections, in 2022. For Iran, division within Israeli society is an achievement in its own right, regardless of which side wins the election, so it targets audiences with opposing views at the same time. Indeed, Iran-linked networks have also been documented disseminating messages about voting, but these point in contradictory directions. Isnad, a volunteer Islamist network with no known state-actor involvement in its operation, focuses on sowing despair and demoralization. According to Alethea (a threat-intelligence company that detects digital deception, disinformation, and social manipulation), the Russian influence operation Doppelgänger treated the Israeli election as one arena alongside the elections in the United States and France. In Israel, no activity involving parties or candidates was identified; instead, its content sought to erode trust in the relationship between Israel and the United States.

Different actors employ similar tactics: accounts that pose as Israelis and attempt to insert themselves into conversation threads involving accounts with large followings and prominent voices in public discourse. The use of impersonator accounts and amplification via authentic users obscures the source of the content, making it harder to distinguish foreign activity from local political debate. In most cases, the content reaches a broad audience only when real Israelis share it, usually without knowing its origin.

About the Report[2]

This report is based on monitoring of the Isnad network on X, conducted by the Institute for National Security Studies (INSS) using data collection tools provided by Xpoz; documentation by FakeReporter; and research by three commercial firms: the OSINT firms Golden Owl and Alethea, and the cybersecurity firm ClearSky. The data is current as of mid-October 2026.

The report addresses covert interference by foreign actors who conceal their identities or impersonate Israelis. It excludes public statements by foreign leaders intended to sway the elections, such as President Trump's explicit call to back Prime Minister Benjamin Netanyahu. It also excludes the artificial amplification of domestic political discourse through fake accounts, networks, or synthetic content—a practice that can intensify polarization and create a false impression of the level of support for certain positions, even without the involvement of a foreign actor.

[2] Golden Owl, "HaKav HaHaredi" (The Haredi Line) and Avi Almog assisted in preparing this report.

Threats of Foreign Interference in the Elections

The foreign accounts identified can be divided into two categories: states and a non-state ideological network. They differ considerably in their resources, structure, and degree of involvement in the elections. For all of them, however, the election campaign serves primarily as an opportunity to intensify efforts already underway to undermine trust in democratic institutions and deepen polarization—efforts likely to continue after the elections.

Iran: A State Campaign to Weaken Israel from Within

Iran's influence efforts ahead of the elections should be viewed as part of the broader strategic campaign it is waging against Israel, alongside its military, intelligence, and diplomatic efforts. For the regime in Tehran, deepening divisions in Israeli society is an achievement in itself, regardless of which side wins the elections. Against the backdrop of military confrontations between the two countries in recent years, it is reasonable to assume that Iran's leadership views deepening divisions in Israel as a means of eroding national resilience and weakening public trust in Israel's political and security leadership.

A society whose constituent groups view one another with suspicion struggles to build consensus regarding security threats and the costs of confronting them. In Tehran's view, such a society should be especially vulnerable. Iran therefore calculates that a divided Israel will struggle to muster public and political support for another military campaign, narrowing the room for maneuver available to its decision-makers.

Achieving this goal does not require favoring one side over another. It is enough to deepen mutual suspicion, undermine trust in the integrity of the democratic process, and turn political disagreements, an essential part of democracy, into social rifts. Nor is there a need to create new divisions. After years of political, social, and security tensions in Israel, amplifying existing ones is sufficient. From Iran's perspective, a significant achievement would be a situation in which political blocs refuse to recognize the legitimacy of the election results and public trust in state institutions continues to erode, regardless of the election outcome.

FakeReporter documented, for example, a network with strong ties to Iran: its accounts are linked through an Iranian app store, and location data points to Iran. The network targets a range of audiences with divisive and contradictory content to destabilize Israeli society and politics. Golden Owl describes a broad network on X (formerly Twitter) of Hebrew-language personas posing as Israelis. According to account information displayed by X, approximately 150 of these personas are linked to Iran, based on their listed location in Iran or their use of the Iranian version of the app. Golden Owl reports that some of these personas were created during Operation "Rising Lion" in June 2025. Some of the infrastructure used during that war is believed to be active again today, ahead of the Knesset elections.

In recent months, messaging has been tailored to different segments of Israeli society, often targeting groups with opposing views. Messages about how to vote have also differed from one audience to another, sometimes contradicting one another. For example, a network documented by FakeReporter simultaneously pushed messages supporting the Haredi struggle

against conscription and messages opposing the Haredi public. These contradictions suggest a lack of commitment to any ideological position: each audience is fed messages that may intensify its grievances. Another possible explanation is a lack of coordination among several different operators.

Iran's attempts to exploit election periods are not new. Suspect accounts were identified as early as the 2022 elections. They operated before and during the elections, as well as after the results were announced, spreading claims intended to cast doubt on the integrity of the process. Iran's capabilities have likely grown since then. Tehran has gained experience engaging with Israeli society and learned more about its internal divisions. In addition, AI tools enable it to produce seemingly credible content quickly and tailor it to different audiences.

The possibility of cyberattacks combined with influence operations should be considered in the days remaining before the elections and in their aftermath. Iran may seek to obtain sensitive information by hacking and leaking documents or correspondence belonging to political or security figures. The material could be authentic, fabricated, or manipulated, and then circulated in a coordinated manner through influence networks. Such an operation could serve both to deepen polarization and undermine trust in institutions, as well as attempt to alter voter preferences and election results. Even a hack with limited technological success could have a significant public impact, casting doubt on the integrity of the election without actually disrupting electoral systems. The risk of undermining public confidence in the electoral process and its results may intensify in the interval between the closing of polling stations and the announcement of the final results. That being said, this represents a potential scenario rather than evidence of a concrete Iranian plan of this kind for the upcoming elections.

Isnad: An Ideological Network Affiliated with the Muslim Brotherhood

Isnad is an Islamist social influence network that began operating in late 2023. It is affiliated with the Muslim Brotherhood and is led by an Egyptian opposition activist based in Turkey. The network is volunteer-based, and it is not known whether a state actor is involved in its operation. A previous INSS publication described its structure, which includes influence, support, and defense units, as well as its transition to a strategy its operators term "sociological warfare": namely, the sustained erosion of Israeli society from within.

The network's leader publicly describes its activity as a long-term campaign that will continue after the elections. Ahead of the vote, he urged network activists to take action and described the vote as a particularly important campaign. In recent months, he has repeatedly called for the recruitment of hundreds of volunteers. It is not known how many actually joined, and no increase in the reach of the network's content was identified as the elections approached. The network was not active during the previous elections, so there is no baseline for comparison.

The INSS monitoring covered approximately 100 accounts impersonating Israelis, which published around 25,000 posts between August 1 and October 13, 2026. The posts included messages questioning the legitimacy of government institutions and the integrity of the elections. In most cases, the network responded to news events within a day or two and

incorporated references to them into its messaging. It operates personas on both sides of the political spectrum, fueling confrontations among users.

Isnad's content relies mainly on genuine divisions at the heart of Israeli public discourse, allowing it to blend in without inventing false information or new disputes. One prominent narrative expresses despair about the future of life in Israel and encourages emigration. Another undermines trust in the electoral process and its results (portraying the elections as a rigged game and a futile effort) and appears aimed at the legitimacy of the process itself rather than at mobilizing voters. The network also circulates messages portraying different groups in Israeli society as threats to one another.

The immediate threat posed by the network is likely limited, but its potential for long-term harm is more substantial. This assessment is based on the gap between the network's capacity to publish and organize and the low reach of most of its posts, as well as its ability to remain active over time and reach audiences through authentic users.

Russia: Israel as Part of a Broader Campaign

According to Alethea, the Russian influence operation Doppelgänger, which the United States and EU member states have attributed to Russia, also targeted Israel's October 2026 elections, alongside its operations aimed at the elections in the United States and France. ClearSky reported that the campaign's activity in Israel resumed in October 2026 after a pause of about two months that began in August. The campaign focused on narratives about the United States distancing itself from Israel, a possible confrontation with Turkey, an economic crisis, and emigration from Israel. The company assessed that the renewed activity may have been linked to an effort to influence Israeli public opinion ahead of the elections.

Alethea found that the operation used dozens of accounts to post content and more than a thousand accounts to amplify it. The Israeli component consisted primarily of a website impersonating a well-known Israeli news site and featuring fabricated articles in Hebrew. The website domain was registered in May 2025 and remained online for about a year and a half, until several weeks before the elections. Its content focused on eroding trust in relations between Israel and the United States; no content about specific Israeli parties or candidates was documented. Russia's interest appears to extend beyond the elections themselves and to concern the relationship between Israel and the United States.

A review conducted by the INSS confirmed the existence of this activity. As of October 19, all of the accounts reviewed that had spread the content were suspended, and no follow-up wave or dedicated Hebrew-language activity was identified. A review of other networks associated with Russia and of comment threads on prominent political posts also yielded no positive findings.

Modus Operandi

X was the primary platform on which the activity was documented. Activity was also identified on Facebook, Instagram, TikTok, and Telegram. In some cases, the same operator was active on several platforms at once, moving content between them. On X, the personas latch onto existing conversations about politicians, journalists, and accounts with large followings.

The common basis for all the actors is the use of personas posing as Israelis, with Hebrew names and stolen or AI-generated photos. Some accounts were created shortly before the elections; others were dormant or established accounts converted for this purpose. One account, for example, posted in Persian until April 2026, then began presenting itself as Israeli and posting in Hebrew. When an account is suspended, it is replaced by one prepared in advance. Some of the accounts documented, including older ones, have already been suspended.

Most of the personas have no following of their own. They seed replies in conversations involving large accounts ("reply seeding") and rely on real Israelis to share their content ("borrowed amplification"), usually without knowing its origin. Sometimes the accounts share one another's content to increase its reach. Networks of accounts that share one another's posts create the illusion of broad consensus. In the Isnad network, for example, seven accounts were documented circulating messages with a common core over two days—messages that did not appear in the authentic Israeli discourse reviewed. However, Israeli campaigns also coordinate replies, so coordination alone does not necessarily indicate a foreign source.

Some of the activity relies on conspiracy theories, "exposés" attributed to confidential sources, and "documents" with no basis in reality, circulated by sources claiming to be authentic. The content is not always false, however. Sometimes it consists of accurate information or legitimate criticism; suspicion of foreign interference centers on who is disseminating it and how.

From Online Influence to Real-World Engagement: a particularly concerning trend is the attempt to move from disseminating content to engaging directly with Israelis. Documented efforts include contacting political activists, offering to prepare posters for them, organizing competitions with prizes, requesting documentation of their activities, and attempting to contact journalists through a WhatsApp group. In one instance, an Iran- linked persona offered Israeli users "well-paying work," a pattern that security authorities explicitly warn against in the context of recruitment attempts.

Summary: What Else Can We Expect in the Upcoming Elections?

For all the actors, the main aim is not to influence the vote itself but to deepen suspicion, portray the country as being steeped in crisis, and undermine confidence in the integrity of the process.

Given the patterns of Iranian activity uncovered during the 2022 elections, it is important to prepare not only for the period leading up to the elections, but also for Election Day and the days after the results are announced. Influence actors, including those operating from Tehran, may seek to exploit isolated incidents, problems at polling stations, rumors of fraud, videos shown out of context, or delays in announcing the results to cast doubt on the integrity of the democratic process and heighten a sense of chaos and suspicion among the public. They may do so, perhaps, by using "dormant" accounts that become active only on Election Day.

When it comes to the elections themselves, the risk identified in the findings concerns trust in the process more than the outcome. In the eyes of foreign actors, chief among them Iran, a

scenario in which political factions refuse to recognize the legitimacy of the election results, the political system is paralyzed, and trust in national institutions continues to erode would represent a far greater achievement than any shift in the distribution of parliamentary seats. Beyond the disinformation itself, the risk lies in covert networks' ability to blend into local discourse, reach mass audiences through authentic users, and create the appearance of broad public support—regardless of the specific message.

Monitoring of hostile foreign entities seeking to exploit the elections for foreign interference is ongoing, and updates will be issued as developments and needs warrant.

Practical Tools for Identifying Suspicious Influence Activity on Social Media

Foreign influence operations on social media often rely on impersonating domestic users, amplifying messaging via inauthentic accounts, and exploiting public trust in content presented as the authentic views of citizens. Such accounts may look like ordinary Israeli profiles, engage in political debates, comment on current events, and even initiate direct contact with users and social activists. Identifying suspicious activity therefore requires looking beyond the content of posts to examine the account's characteristics, activity history, and behavioral patterns.

Key warning signs that can be checked independently include:

- **Account identity and profile credibility:** On X, Instagram, and Facebook pages, users can view "Account Information" or "Page Transparency" to see when the account or page was created, its location, and any username changes. Check when the account was opened, whether it has a consistent history of activity, and whether its personal details are consistent. An account opened recently that presents itself as a longstanding public figure, a profile that has changed its name unusually, or one with almost no personal information may warrant further scrutiny. Searching the username across other platforms can also determine whether supporting footprints of that identity exist elsewhere online.
- **Profile picture:** Suspicious accounts may use stolen photos, stock images, or AI-generated personas. A reverse image search via Google Lens can reveal whether the photo appears across unrelated profiles or under different names (though a lack of results does not guarantee authenticity). Users can test whether an image was created or altered using artificial intelligence via verification platforms such as SynthID (synthid.com), where images can be uploaded for inspection. Note that the tool does not detect every type of AI-generated content, so a negative result does not necessarily mean the content is authentic.
- **Language and phrasing:** Repeated errors in Hebrew, confusion between masculine and feminine forms, expressions uncommon in spoken Hebrew, writing that appears to be machine-translated, or unusual punctuation may raise suspicion, especially when an account presents itself as Israeli and Hebrew-speaking. However, language errors alone do not indicate foreign activity; they are also common among new immigrants and

Arabic speakers who write in Hebrew. Highly polished Hebrew that appears to have been generated by AI can also be a warning sign, but it is not proof. The use of hashtags, particularly on platforms such as X and Facebook, may also indicate a foreign account, since hashtags are not commonly used by Israelis. Sometimes the hashtags used by foreign accounts are not directly related to the content of the post.

- **Posting and response patterns:** Check whether the account shares personal, original content or focuses almost entirely on spreading political messages, repeatedly sharing content, and replying to other accounts. An unusually high posting frequency, repeated copying of the same messages, or identical replies appearing in several different discussions may indicate automated or coordinated activity.
- **Connections between accounts:** When several accounts post identical or very similar wording, regularly reply to one another, or share the same links within a short period, they may be engaged in coordinated activity intended to artificially increase the visibility of their messages. In such cases, look at the accounts' shared activity patterns rather than relying on the characteristics of a single account.
- **Content credibility and sources:** Exercise caution regarding posts framed as exclusive exposés, reports based on confidential sources, or content provoking a strong emotional response without providing evidence. Look for the story in independent, reliable sources, and check whether the site linked in the post is the media outlet's official site or an impersonating lookalike domain. Using a familiar name, a media outlet's logo, or an authentic photograph does not guarantee that the content itself is reliable.
- **Direct messages and calls to action:** Heightened vigilance is warranted when an unfamiliar account reaches out requesting to spread political messages, join groups, photograph events, provide information, or perform tasks in exchange for payment or another reward. Such requests warrant checking the identity of the person making them and the purpose of the request, even when they are presented as protest initiatives or legitimate civic activity.
- **Suspicious content and narratives:** Influence operations may involve the systematic spread of messages intended to heighten public fear, despair, and distrust. In the Israeli context, such messages may portray Israel as weak and helpless in the face of Iran, exaggerate the scale of destruction and damage during wars, or paint an especially bleak picture of life in Israel, including its economic and social conditions. Warning signs may include the repeated use of unsubstantiated claims, old photographs presented as if they were taken during recent events, information taken out of context, and the coordinated spread of the same messages through different accounts. Political criticism, descriptions of genuine hardships, and expressions of pessimism are not in themselves evidence of foreign activity. Suspicion is warranted when such content is accompanied by deception, impersonation, or inauthentic patterns of dissemination.

- **Impersonation of organizations, groups, and local initiatives:** Influence operations may also use pages and groups that impersonate civic initiatives, local communities, or protest organizations. Check who is behind the page or group, whether it provides reliable contact information, and whether there is evidence of real-world activity. Caution is especially warranted when an entity portraying itself as a local civic organization asks users to provide personal information, join closed groups, or take part in an activity whose organizers cannot be identified.

None of these warning signs on its own proves that an account is fake or operated by a foreign actor. The more independent indicators accumulate, the greater the need for professional verification. A fake account, coordinated inauthentic activity, and activity attributable to a foreign state actor are distinct categories; attributing activity to a state requires additional evidence.

When inauthentic activity is suspected, avoid sharing personal information, amplifying unverified content, or complying with unusual requests. Suspicious profiles can be documented via profile links, screenshots, and examples of suspicious posts, and reported directly to the platform, to Fake Reporter, or to the Israel Internet Association.

**** The article was originally published in Hebrew on October 22, ahead of Israel's October 27, 2026, Knesset elections. The English version, published following the elections, reflects the article as originally published.***