How does Iran Wage its information warfare battle against Israel?

by Ofir Barel **(/experts/ofir-barel)**

Sep 1, 2021
Also available in
العربية (/ar/policy-analysis/kyf-tshnw-ayran-hrbha-alalamyt-dd-asrayyl)

ABOUT THE AUTHORS

Ofir Barel (/experts/ofir-barel)

Ofir Barel is a researcher at Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University. He is also a former researcher at the Institute for National Security Studies (INSS) and at the Center for Political Research at the Israeli Ministry of Foreign Affairs. Barel is a contributor to Fikra Forum.

Brief Analysis

In the face of Iranian influence operations, Israel must adopt a comprehensive national strategy to prevent further infiltration aimed at disrupting social cohesion and political stability.

The Iran-Israel conflict is multidimensional and has been going on for years. At the highest strategic level, Iran has been developing nuclear capabilities, which according to Israel are intended to be used towards its destruction. On the military tactic front, Iran backs the arming efforts of its proxies—Hamas and Hezbollah—against Israel. Iranian hackers also launch numerous cyberattacks against companies and critical infrastructure in Israel.

Over the years, Israel has—at least according to foreign sources— initiated and engaged in numerous operations against the threats mentioned above, as well as its own cyberattacks. Compared to this activity, however, there is one threat that Israel has not concretely engaged with: in recent years, researchers in Israel and abroad have gathered multiple instances of Iranian malicious influence operations, targeting Israeli citizens on social media. This contrasts with the international dissemination of anti-Israel messages that various governmental entities, such as the Israeli Ministry of Foreign Affairs, have worked to combat.

Influence operations may be defined as propagandist actions designed to alter the perceptions and actions of a specific audience to promote the goals of the initiator, which are usually directly contrary to the clear interests of the target audience. This can be achieved primarily through a massive distribution of false information, which is designed to manufacture emotions and distorts the perceptions of the intended recipients. Specifically, the Iranian influence operations described below are intended to erode the political stability and social cohesion within Israel.

The Russian interference in the 2016 U.S. elections, **designed to achieve similar goals (https://www.lawfareblog.com/what-mueller-report-tells-us-about-russian-influence-operations)** , has strengthened the global recognition of the potential harm of these types of campaigns. This is demonstrated, for example, by Robert Mueller’s statement **(https://edition.cnn.com/2019/07/24/politics/robert-mueller-opening-statement-judiciary/index.html)** before Congress in 2017: “I've seen a number of challenges to our democracy. The Russian government's effort to interfere in our election is among the most serious... this deserves the attention of every American.” Iran also recognizes this fact and has adopted this style of influence in its efforts against Israel .

Yet Israel has not implemented an appropriate response to this threat. This manifests not only in the lack of basic data **(https://fs.knesset.gov.il/globaldocs/MMM/88e9ca15-7b54-e911-80e9-00155d0aeebb/2_88e9ca15-7b54-e911-80e9-00155d0aeebb_11_10982.pdf)** regarding foreign electoral involvements, but also in a claim **(https://twitter.com/FakeReporter/status/1410621671157866496)** (raised by an organization dealing with the issue) about the absence of a real-time reaction by the government. Instead, the government should set up national and international mechanisms that can help Israel crystallize systematic policy and quick action plans.

Characteristics of the Iranian information warfare against Israel

These operations can be categorized into two types. The first—and more common —type includes influence campaigns devised to undermine Israeli domestic stability by fueling conflicts regarding controversial issues, similar to the Russian influence actions in 2016. The most notable subversive campaign is the Iranian interference **(https://www.ynetnews.com/articles/0,7340,L-5455991,00.html)** in the April 2019 legislative election, when hundreds of fake accounts tried to stir up public divisions on these issues on social media. The second type contains operations intended to emphasize Iran's supremacy vis-à-vis Western countries. This includes the fabricated news site "Tel Aviv Times", **(https://www.ynet.co.il/articles/0,7340,L-5342357,00.html)** which framed Israel as a weak state by publishing rewritten articles copied from Israeli news sites.

Ongoing and significant delegitimization operations have challenged Israeli democracy since its establishment. However, what makes current Iranian activity a unique threat that requires particular attention is the rapid improvement in its performance. This advance is part of a broader enhancement of the Iranian information warfare against (mainly) Western countries, which has been achieved in a relatively short period of time. While in 2018, cyber security company FireEye described **(https://nypost.com/2018/09/03/iranians-are-bad-at-the-fake-news-game/)** the Iranian campaigns as “sloppy” and “redundant”, by 2020, the American Atlantic Council highlighted **(https://www.cyberscoop.com/iran-disinformation-atlantic-council-2020/)** Iran's vast experience and resources, enabling it to act cunningly against its enemies. This trend is not accidental: according to some intelligence experts **(https://nationalinterest.org/blog/buzz/how-iran-might-fight-war-against-america-thanks-russia-67002)** , Iran carefully applies Russian information war methods that were later turned against western democracies. The results of this study were visible, for example, during the 2018 U.S. elections, when Iran implemented **(https://www.nbcnews.com/tech/tech-news/iran-s-facebook-strategy-had-echoes-russian-playbook-n903091)** intervention methods that mimicked Russian tactics that had been carried out two years earlier.

Regarding Israel, two recent incidents illustrate the intricacy of Iranian influence operations: on the one hand, during Operation Guardian of the Walls, Iran (according to Israeli intelligence sources **(https://www.yediot.co.il/articles/0,7340,L-5938901,00.html?fbclid=IwAR0jc9wFEJOICnIwfLK4DgIqXvfdFR6f7ncLS9ep_K64xSiNcPLWF6SaVnk)**) had operated an extensive network of Twitter accounts designed to demoralize the Israeli public. Those messages reached Israelis and international viewers alike, with estimates suggesting that **(https://twitter.com/FakeReporter/status/1395738544975532032?fbclid=IwAR2h6YE_-gcbhjwqPS-sIVf1X2exN_J8B83GFa_P9TOruQewnELRTRA-994)** over one hundred million people worldwide had been exposed to them. Additionally, Iranian trolls were also suspected to have escalated internal tensions between Jews and Arab citizens during the crisis.

Simultaneously, Iranian activists **infiltrated (https://www.nytimes.com/2021/06/30/technology/disinformation-message-apps.html)** WhatsApp and Telegram groups of the black flag movement—which organized protests against the former prime minister, Benjamin Netanyahu—and shared polarizing messages, exploiting the trust of the group members, whose numbers are sometimes estimated to include just a few dozen. The fact that these two campaigns were carried out roughly at the same time during the first half of 2021 indicates Iran's ability to turn its diverse capabilities against the Israeli civilian population, with little awareness of the entities working to protect Israel from such threats.

What might intensify the Iranian threat to Israel is the possibility of cooperation **(https://www.jpost.com/Arab-Israeli-Conflict/Terrorists-trying-to-use-cyber-to-impact-elections-ICT-579783)** between Iran and its allies, in which Iran could bequeath its experience in cyber warfare and information warfare. Over almost a decade, Hezbollah has used thousands of activists to disseminate manipulative and false messages **(https://www.telegraph.co.uk/news/2020/08/02/exclusive-inside-hezbollahs-fake-news-training-camps-sowing/)** against various targets. It would not be unreasonable to assume that an essential part of the activity of this "troll farm" is based on Iranian methods, which its other proxy—Hamas—might also learn.

What can Israel do?

The absence of a comprehensive governmental strategy for warding off Iranian influence operations targeting Israeli citizens and the potential severe consequences call for the immediate implementation of two organizational measures, which already have been proven as efficient in other contexts.

At the national level, Israel must establish a dedicated center for countering influence operations. Based on the practice of similar bodies in Europe and the United States, this aim can be achieved through a threefold action plan: characterizing the information warfare conducted against the state, guiding non-profit organizations and individuals involved in debunking influence operations, and informing the public regarding the nature of the threats and possible countermeasures. Global experience has proven the effectiveness of the centers in inhibiting foreign influence operations: for instance, according to Jakub Janda **(https://www.thelocal.se/20180914/opinion-how-to-counter-russian-interference-like-a-swede/)**, who has previously advised the Czech government on countering Russian influence operations**,** a similar national task force set up in Sweden before the 2018 general election was one of the important means for defending it from a foreign intervention. It should be noted that in 2019, the Israel Democracy Institute and the Israeli Security Agency suggested **(https://www.jpost.com/Arab-Israeli-Conflict/Terrorists-trying-to-use-cyber-to-impact-elections-ICT-579783)** establishing such an authority dedicated to identifying suspicious activity on Israeli networks. However, as far as is known, no such authority has been founded.

At the international level, Israel should apply for membership of the EU-HYBNET project **(https://euhybnet.eu/)**: a pan-European network for tackling influence operations funded by the Horizon 2020 program, which Israel participates in. By participating in this continental network, Israel will be able to benefit from three remarkable advantages.

First, the initiative is not intended to deal with influence operations per se, but as an aspect of warfare method known as hybrid warfare that involves **(https://foreignpolicy.com/2018/01/18/inside-a-european-center-to-combat-russias-hybrid-warfare/)** the use of military and non-military means for routing the enemy. The execution of a wide-scale de-moralizing operation against the Israeli public during Operation Guardian of the Walls, for example, illustrates the need to develop and refine principles of hybrid warfare as part of thwarting foreign influence operations.

Second, the project brings together military and civilian experts from twenty-two European countries. This is an inexhaustible pool of experience, from which Israel will be able to derive many useful conclusions—especially when a considerable part of them **regularly deal (https://carnegieeurope.eu/strategiceurope/81322)** with Russian influence operations.

Finally, alongside conducting theoretical research on hybrid threats, the center organizes training events during which participants can gain and practice essential skills for successfully stymieing hybrid threats. The lessons learned following the exercises might grant Israel applicable and verified tactics for responding to malicious influence operations in real-time.

So far, Israel has wasted precious time ignoring an existential threat, which has become increasingly elusive and dangerous. The two solutions described above could serve as a base for an overall policy, which may allow Israel to not only be better prepared for future influence operations but also turn public diplomacy into a vital component in curbing Iran's harmful ambitions. ❖

RECOMMENDED

BRIEF ANALYSIS

Saudi Arabia Adjusts Its History, Diminishing the Role of Wahhabism

Feb 11, 2022

◆

Simon Henderson

(/policy-analysis/saudi-arabia-adjusts-its-history-diminishing-role-wahhabism)

ARTICLES & TESTIMONY

Podcast: Breaking Hezbollah's Golden Rule

Feb 9, 2022

◆

Matthew Levitt

(/policy-analysis/podcast-breaking-hezbollahs-golden-rule)

BRIEF ANALYSIS

Targeting the Islamic State: Jihadist Military Threats and the U.S. Response

February 16, 2022, starting at 12:00 p.m. EST (1700 GMT)

◆

Ido Levy,
Craig Whiteside

(/policy-analysis/targeting-islamic-state-jihadist-military-threats-and-us-response)