Iranian Digital Influence Campaign on Israeli Social Networks

ALMA RESEARCH OCTOBER 28, 2021

By Mayan Sarnat [1]

Much has been said about the cyberwar that has become the main battlefield in recent years in the war between the superpowers and between Israel and Iran. Still, this war has received a version update in the last two years, and foreign elements are encouraging the public to turn on each other and fight from within. Iranian efforts have recently been made in a virtual campaign for influence, fuel hatred and internal strife, encourage polarization, hatred, and despair, and undermine democracy.

Iran has invested significant resources and accumulated vast experience in the conduct of digital influence efforts. These clandestine propaganda efforts have been used to complement Iranian foreign policy operations for the better part of a decade. In pursuit of foreign and domestic information dominance, Iran began operating Facebook and Twitter "sock puppets" (A fictitious online identity created for deception) as early as 2010. As a whole, Iran's digital influence operations represent a continuation of public diplomacy, albeit conducted through misleading websites and social media "sock puppets".

Social networks are one of the most influential factors on our political positions and trust in state institutions. Facebook is the most influential when it comes to political-security issues. According to a survey by the Israeli Channel 13, 50% of the Israeli public claim that "Fake News" prevents them from understanding reality. 45% percent are worried about expressions of hatred online, which Israel's enemies seem eager to exploit.

These days, the "models" network, as defined by the media, operates in Israel – hundreds of fictitious profiles of women, allegedly Israeli, run by a foreign political entity, apparently – Iran, whose goal is to divide, initiate conflict and influence the Israeli public politically. The "models" are very politically active on the net and aim at all directions, participating in discussions and forming groups. The main message is that everything is bad and corrupt, and it cannot be fixed. The "models" entice men primarily to do their bidding online.

They enter influential groups and establish such. Every Friday, they make sure to upload a photo and wish "Shabbat Shalom" (A greeting in Hebrew for the holy day of the Jews beginning on the seventh day of the week). An inquisitive look will identify unauthentic and identical behavior with the same visual characteristics. They wish "Shabbat Shalom" and a good week to all followers to increase interaction with followers and increase a sense of trust, often accompanied by revealing images.

[1] *This article was written by Mayan Sarnat, a research fellow of the Alma Center. She has a master's degree in diplomacy and security from Tel Aviv University. Today, she is a senior analyst in the security field in a company specializing in intelligence research and national security.*

- Noa Moshe from Tel Aviv has more than 2,000 followers and excellent Hebrew. She is very politically active, expresses herself a lot on military issues and on Covid and makes sure to wish Shabbat Shalom and a happy holiday. But everything also angers her, despairs her.

- Noa is actually Madeleine, a model and blogger from Romania. Her identity as well as that of hundreds of other sophisticated profiles of attractive women are part of a 'network of influence' operated by a foreign political entity, by most signs – Iran. They extract the images from porn sites and modify them so that they cannot be traced by Google Photos.

One of the fake profiles, Noa Shamir, posted a cartoon and provocative content against Former Israeli Prime Minister, Benjamin Netanyahu. These photos were uploaded again by Benjamin Netanyahu and his son Yair, blaming the post on 'extreme leftists'., it was not leftists who created and distributed them but the fake profiles. The source for the cartoon was from a competition in Iran in 2016. These profiles operated during the Israeli elections to produce propaganda that will impair, as the propagandists saw it, the ability of the citizens to make conscious and intelligent decisions.

A year ago, the "models" preached keeping distance and wearing a mask and hating the ultra-Orthodox who "spread" the covid virus. In recent months the same profiles have changed attitudes: the covid is a lie and the vaccine is an international conspiracy. They are active daily, responding to hot topics, fueling conspiracy theories and penetrating dozens of political groups, and flooding them with messages such as "everything is broken" "everything is corrupt" "the country is terrible" "everything is collapsing". They not only fit into the political groups, but they also form them, copy content from dubious sites, and mislead the members. They "snatch" groups, set up ones with a similar name, and take the logo. In response join thousands of misguided people who think they have joined the group they wished and are dragged into the inciting discourse.

The "models" try to be active wherever there is social sensitivity and especially in groups of soldiers. The models set up a group that post content about failures in the IDF; "neglecting soldiers, not caring for them, the food is terrible", etc. The purpose of this type of campaign as can be understood is to lower the motivation for recruitment.

As mentioned before, the main suspect in operating this network of fake profiles is Iran, which has recently increased its surveillance and involvement in social media networks in Israel. There are a number of key factors that have led investigators from the "Fake Reporter" NGO that has exposed the network, to suspect Iran as the operator of those pages:

Recurring textual characteristics: space before punctuation, double exclamation marks, re-use of red exclamation mark emoji, bad Hebrew, gender confusion, incorrect translation of words, singular and plural confusion, and reverse question mark use (as in Arabic and Persian).

Recurring visual characteristics: In some of the profiles the pictures have been manipulated; the image has been flipped or the forehead area has been stretched. This is done so that it is not possible to locate the source of the image on the web. A Google search does not locate the image but once more

advanced facial recognition technology is used the source of the profile picture can be traced to a pornographic site and to girls from Russia.

In addition, the same characteristics identified by Fake Reporter were previously identified by the organization in a previous campaign in which it was proven that Iran was involved. In that campaign, which was at the beginning of the first round of the last Israeli elections, Facebook used the analysis of Fake Reporter and classified the profiles as part of an Iranian influence campaign and removed them from the network.

While Iran is at the forefront of digital influence campaigns, no country has used its cyber capabilities as a weapon like Russia. The new version of the cold war is registered in its name. The most talked-about example was Russia's use of social media to influence the 2016 U.S. presidential election. In 2016, Russian trolls created fake accounts and memes that were uploaded to social media and attacked Hillary Clinton. The KGB and its Eastern European metamorphoses also used campaigns of influence through the people recruited in Western countries in the past. Nowadays, the internet has given the campaign a huge boost as there is no longer a need to recruit spies or key personnel in the target country.

The Iranians learned quickly, and both the "Shin Bet" (The Israeli General Security Service) and Facebook have confirmed that in the last Israeli election they identified an influence network in Israel operated by a foreign power. It can be estimated from Iranian activity that in Iran it is believed that at the moment, Israel is weak internally and that this is an opportunity to act and weaken it through tools that deepen the internal dispute.

Before the appearance of social media platforms, terrorist and criminal activities tend, by nature, to be as clandestine and secretive as possible. Accordingly, the methods designed to combat them focus on unearthing data and tying them into evidence of wrongdoing.

One might think that social media platforms – where people cast their preferred persona to the world – are not the places one would intuitively search for terrorists and criminals. Yet in recent years, in light of terrorist organizations' vast use of social media platforms, the discipline of gathering and analyzing intelligence from social media platforms – developed in the business world and colloquially called SOCMINT – has been increasingly useful in tracking terrorist activities.

SOCMINT can be useful in tracing these activities, with the help of WEBINT investigative tools that combine qualitative analysis with Big Data Analytics. Applying these tools can help demonstrate how the activities of different actors, states, and terrorist organizations can be tracked online.

Iranian networks like the Russian ones operate throughout the virtual space, on Twitter, Tiktok, but mostly on Facebook and Instagram. Facebook seems to recognize that this activity at the end of the day increases the company's profitability and cannot be relied upon to forcefully act against it. And so, on the user level, in order to avoid being played by Iranian operatives disguised as models, it is best to be suspicious and make sure the profiles and groups you are communicating with are reliable.