Russian Influence Campaign Against Israel: Strategic and Cognitive Implications

Milàn Czerny, Vera Michlin-Shapir, David Siman-Tov | No. 1852 | May 1, 2024

Since the October 7th massacre, Russia has stepped up its semi-covert disinformation attacks against Israel, as part of its global Doppelganger influence campaign, which began in 2022. These attacks align with Russia's official stance, which has remained hostile to Israel in recent months. They signal a strategic shift in the Kremlin's approach, by grouping Israel with countries it perceives as enemies. A policy shift by the Israeli government should reflect these dynamics and address the new risks to Israel posed by an increasingly antagonistic Russia.

For at least two years, Russia has been running a global disinformation campaign that has targeted Ukrainian, French, German, and Israeli audiences. The campaign targeting Israelis mimics similar campaigns directed at European states and Ukraine in recent years by spreading fake media articles on social media. In the weeks following the October 7th massacre, the perpetrators have increased the scope and scale of attacks against Israel. Russia has also increased efforts to tailor the political messaging to target Israeli audiences. While in the past, this Doppelganger disinformation campaign against Israel focused on dissuading Israel from supporting Ukraine, the current iteration of the campaign addresses domestic Israeli issues (see figure 1).

Figure 1. A fake copy of "Walla," an Israeli media site, as distributed by the Doppelganger disinformation campaign. The headline reads, "Shifa Hospital [in Gaza] as another defeat in the information war."

The disinformation campaign against Israel is mostly active on X (formerly known as Twitter) and Facebook. Accounts are created in "waves" and publish links to fake websites that are clones of Israeli media sites at an artificially high rate. For instance, on the night of November 20–21, 2023, over 2,000 accounts on X posted nearly 3,000 links to disinformation articles that were shared on clones of Walla and Liberal websites (see figure 2). Simultaneously, clones of Ukrainian, German, and French media are promoted in even greater numbers than the Hebrew clones. Additionally, the Doppelganger disinformation campaign in Hebrew on Facebook redirects users to the same fake content promoted on X, demonstrating a cross-platform effort to maximize exposure.

The pace of the disinformation campaign has remained fairly consistent throughout the war, indicating a bureaucratic effort behind the campaign. Those responsible for the campaign create and post around two to four fake news items every two days or so, which are, in turn, are then promoted by thousands of fake accounts on X.

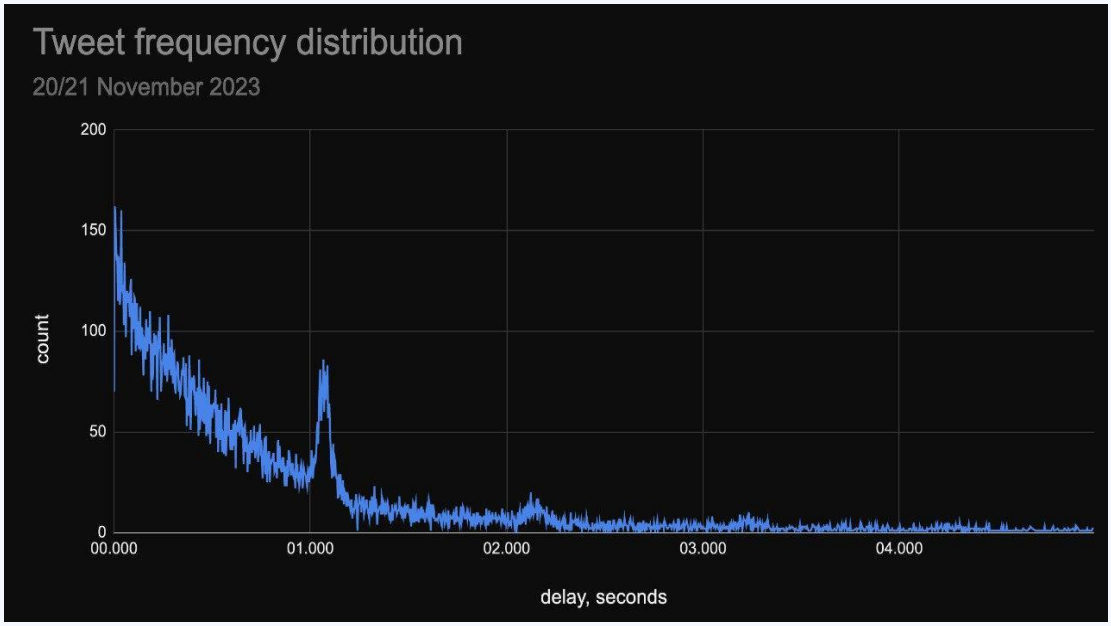

Figure 2. Tweets posted by Doppelganger accounts on November 20–21, 2023 | *Source*: The disinformation team @antibot4navalny, a well-known anti-disinformation initiative often quoted in international media, shared with the authors by the head of this team.

Disturbingly for Israel, the current iteration of the campaign is diligently orchestrated, demonstrating an increased level of attention and investment of time and effort from the perpetrators in targeting Israeli audiences. Posts are quickly adapted to specific events. For instance, during South Africa's case against Israel at The Hague, Doppelganger accounts shared fake news articles in Hebrew related to the topic. Similarly, the Doppelganger campaign used the US strikes against the Houthis to claim that "the US bombing of Yemen is not helping Israel, it's just opening up another front against the IDF," highlighting the perpetrators' growing interest in the Israeli segment of the global Doppelganger disinformation campaign (see also figure 3). Such flexibility in the campaign, which takes advantage of current events to convey a general message, requires both human and computational resources.

Figure 3. A screenshot of a disinformation post distributed on Facebook by Doppelganger-affiliated accounts. The post claims that "The current US administration is sacrificing Israel's security for its own interests."

In the past two years, the Doppelganger campaign has been attributed to different Russian state-linked actors. In December 2022, Meta indicated that two Russian companies, Structura National Technologies, an IT company, and Social Design Agency, a PR firm, were behind the fake sites. The Social Design Agency admitted on its website that it had worked for state entities, such as the Russian Ministry of Internal Affairs. In 2023, the European Union imposed sanctions on both Structura National Technologies and Social Design Agency "for the creation of fake websites impersonating government organizations and legitimate media in Europe (primarily Germany, France, Italy, Ukraine and the United Kingdom)." In addition, cybersecurity researchers found similarities in the code strings of the websites of the Doppelgangers campaign and a previous campaign attributed to APT28, a cyber threat group linked to Russia's military intelligence service (GRU), suggesting a possible connection between the Doppelganger campaign and APT28.

In terms of the audience's receptiveness to the campaign, authentic engagement with the fake articles of the Doppelganger campaign is rare. However, some well-positioned posts have been picked up by popular Israeli Telegram channels, and mainstream media. For instance, one fake message promoted by a Doppelganger account warned Israelis that the 2024 Olympic Games in Paris could become a repeat of the massacre at the 1972 Olympics in Munich. This message was shared by "Carmel News," a channel for Russian-speaking Israelis on Telegram, as well as by "Sdarotali," one of the largest Israeli channels on Telegram with over 300,000 subscribers. In late October, the anchorperson of the Israeli public broadcast KAN11 claimed that Ukrainian weapons had ended up in Hamas's hands, a claim that was widely promoted by the Doppelganger campaign immediately after the October 7th massacre (see figure 4). These incidents suggest that if the campaign gains pace by increasing its scope, scale, and content agility, the Israeli media could potentially believe the Doppelganger fakes and report on them as if they were real, authentic news items.

Figure 4. A screenshot of a disinformation post distributed on Facebook by Doppelganger-affiliated accounts. The post falsely claims that Ukraine is selling weapons to Hamas.

Conclusion

The Doppelganger campaign poses three significant threats to Israel's national security. First, the campaign indicates heightened interest in Israel by Russia's state-backed disinformation actors. While we can currently disregard these efforts as having a marginal effect, we should take seriously unwelcome attention from competent and vicious disinformation campaigns. In 2016 during the American presidential elections, Moscow's influence campaigns involved a wide range of actions, including cyber activities, "state-funded media, third party intermediaries, and paid social media users or trolls." This disinformation activity was largely disregarded at the time as it was perceived as ineffective; however, this changed significantly when Russia's intelligence

agencies hacked into the Democratic National Convention emails with devastating effects on the media environment.

Second, the perpetrators of these campaigns are still learning. They are gaining competency in operating within Israel's already existing polarized media environment. The fake posts are systematically and methodically melting boundaries between truth and lies and finding various ways into the Israeli media space, which will give those behind these campaigns exposure to a much larger audience. The widespread circulation of these fake news items and their appearance from time to time in mainstream and popular Israeli channels undermines trust in the media and induces a sense of chaos and an uncontrolled information environment. As the perpetrators of these campaigns gain more experience with the Israeli media space, their ability to penetrate additional social discourses will increase.

Last, this disinformation campaign aligns with Russia's broader strategic objective of fueling the war in the Middle East and spreading tensions to distract attention from its own war against Ukraine. These were most likely the objectives behind the current iteration of the Doppelganger campaign targeting Israel. As such, this campaign should be seen as a signal of Russia's growing interest in Israel, as an attractive target for hostile Russian activities and further destabilization. This heightened interest in Israel increases the possibility of additional Russian campaigns in the information space and/or interventions in physical space.

To effectively address this threat, the following measures are recommended:

1. Security Perspective—Recognize the operation as a strategic threat with the potential to expand and intensify. Israel should align itself with the policies adopted in NATO-allied countries, aiming to limit the reach of Russian state-backed actors in the information space.
2. Media Engagement in Israel—Exercise caution when engaging with entities aligning themselves with the Russian position. Some may function as agents of influence or unwitting collaborators.
3. Public Awareness—Enhance public awareness regarding Russia's interference in Israeli media and social networks and help to remove harmful content by reporting it to platform administrators.

Editors of the series: Anat Kurtz, Eldad Shavit and Ela Greenberg