

A Worldwide Russian Influence Campaign— Implications for Israel

David Siman-Tov and Vera Michlin-Shapir | No. 1901 | October 13, 2024

A recent FBI report reveals a Russian influence campaign targeting several countries, including the United States and Israel. The report highlights Russia's attempts to sway Israeli public opinion, particularly during times of political upheavals, with the aim of encouraging support for its war against Ukraine. For the first time, it was publicly disclosed that the Arab population in Israel was also a target of Russian influence. The campaign utilized digital media and the creation of fake content, which was spread via social networks. To counter these tactics, Israel would benefit from upgrading its digital defense, fostering international cooperation, and enacting relevant legislation and regulation. Additionally, the public should be made aware of the threat.

Beginning in early September 2024, official US agencies, including the FBI, the Treasury Department, and the State Department, took new measures to counter Russian influence among the American public and to protect the US information space from organized Russian interference. Earlier this month, the FBI [filed an indictment](#) against Russian influence agents working for RT, the Kremlin's news network, accusing them of attempting to sway American public opinion through an American subcontractor.

The FBI report includes documents obtained by American intelligence, among them evidence of a Russian conspiracy to influence Israeli public opinion and Jewish communities worldwide. This is part of the “Doppelganger” campaign, which has recently gained attention all over the world, including Israel. Russian influence efforts are also apparent in other European countries, such as Ukraine and Germany, and in Latin America, particularly Mexico. The US State Department and Treasury Department has subsequently [imposed](#) new sanctions on RT, accusing it of being “a de facto arm of Russia's intelligence apparatus.” These actions signal a step up by the American establishment to combat influence campaigns, particularly those linked to Russia, and reflect its determination to defend liberal values in the digital space. The report further highlights operational details of the Doppelganger campaign and reinforces previous concerns about [the intention of parties linked to the Russian government](#) to influence Israeli public opinion. The documents indicate that this operation is well-funded and well-coordinated and directly linked to the Kremlin, with the team working under the direct supervision of Russia's First Deputy Chief of Staff Sergey Kiriyenko.

The section of the report concerning Israel covers the period preceding the war in the Gaza Strip. It highlights Russia's efforts to influence the Israeli public and possibly also to shift the government's stance on the war in Ukraine. The campaign also sought to weaken Israel by intensifying the internal tensions over the proposed judicial reform and to strengthen Prime Minister Benjamin Netanyahu, whom the Kremlin sees as a potential ally for pro-Russian policies. The report asserts that the political and social divide in Israel make it ripe for a significant influence campaign and can serve Russia's goals, with the potential of swaying public opinion within an extremely short time span. It lists the names of prominent Russian agents active in the political field and recommends that their online activity be monitored.

The influence campaign extensively utilized digital media, including paid advertisements, caricatures, and "cooperative ventures" with real or fake Israeli influencers. These efforts were supported by the creation of forums on social networks and Telegram in addition to fake websites that were clones of popular news sources, such as the *Washington Post*, to publish credible-looking content. The campaign team included media, intelligence, and technology experts from companies operated by Russia, such as the Social Design Agency (SDA). These companies were responsible for producing fake content, disseminating it on social networks, and using dashboards to monitor public reactions. These teams also included experts who developed bots and algorithms to amplify the fake content's distribution and target specific audiences.

Journalists Uri Blau and Milan Czerny, of the "[Shomrim](#)" website, have exposed additional documents not included in the US indictment, raising concern about the involvement of a Russian state agency in influencing Israeli public opinion through social media and possibly interfering in Israeli politics. The article broke new ground by drawing attention to Arab society in Israel as a vulnerable target for Russian influence. For example, one document suggested increasing social tension by spraying provocative graffiti in Arab neighborhoods. Blau and Czerny also asserted that the Russian campaign included a plan to create a new political party that would appeal to Russian-speaking Israelis. It is possible that the Russians self-leaked the documents on which the "Shomrim" article was based as a means of boosting their efforts and deterring actions against their interests and capabilities in the information space.

Both the American government report and the "Shomrim" article note that it is difficult to measure the impact of these campaigns on public opinion. Nevertheless, the US Justice Department is determined to penalize the parties behind the Russian influence campaigns for deceiving the American public with misleading information and disinformation. The underlying principle is that citizens in a democracy have a basic right to accurate and reliable information, while those undermining this right should be held accountable, regardless of the campaign's degree of influence.

Implications and Recommendations for Israel

Thomas Rid, a scholar specializing in Russian and Soviet influence operations, highlights the important distinction between the ordinary lies that people tell one another and the disinformation spread by the influence campaigns. While ordinary lies are spread randomly, the spread of disinformation is part of an organized effort by bureaucratic and intelligence establishments. To address the challenges posed by these influence campaigns, countries—including Israel—must establish professional agencies to help protect their digital space and provide reliable information that citizens can use to make informed decisions about political and public life.

The US indictment, based on a comprehensive FBI investigation, contains extensive information showing that the United States has established a nationwide system to counter influence efforts. This system, similar to those in other Western countries, could serve as a model for Israel, despite the differences in both the severity of the threat and the political and strategic cultures of the two countries.

Over the past decade, liberal democracies have gained valuable experience and knowledge in dealing with attempts by hostile entities to exert influence. While Israel has begun initial preparations to respond to these threats, especially in light of recent influence campaigns, its efforts have been slow and deliberate. For example, Israel has not taken basic steps to counter Russian influence campaigns, such as halting the operation of the RT network, which continues to function in Israel unhindered.

The following are key steps that should be taken in Israel, some of which are already in the initial stages:

1. Recognition of foreign interference, particularly Russian activity, as a strategic threat to Israel.
2. Organization of government ministries and the intelligence and cyber effort to provide a continuous response to the challenge. This response should include advanced technological tools to detect foreign disinformation and strengthen international cooperation with Western countries. This organizational effort, in cooperation with civil society, will help create status reports on foreign campaigns targeting Israel during both peacetime and war.
3. Alignment of Israeli legislation and regulation with Europe, the United States, and other Western and Eastern countries (such as Australia and Taiwan) to detect illegitimate influence campaigns on digital platforms. Regulating these companies is essential for coping with this challenge.
4. Involvement of civil society. Civil society organizations play an important role in countering foreign influence campaigns, both through research and by removing foreign networks from cyberspace. The intelligence community face

challenges in monitoring internal public discourse, but civil society organizations can address this issue more freely with fewer obstacles. Their role should be encouraged and supported.

5. Increased public awareness. It is recommended to increase transparency and public awareness of foreign influence campaigns through widespread media publicity and by enlisting influencers in the effort. It is crucial to inform the public as soon as possible after the influence campaign is detected, unlike the delayed release in the FBI's report, which was published more than a year after the events.
6. Educational initiatives. Educational initiatives should be implemented for the various age groups to raise awareness of the foreign influence efforts and their dangers. This will strengthen Israeli society, although these efforts are still in their initial stages compared to the greater awareness of cyber threats.

Dr. Vera Michlin-Shapir is the director of education at the Symposium Institute for Strategic Communications. She was previously a researcher and lecturer at the King's Center for Strategic Communication at King's College London and a researcher at INSS.

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