INSS Insight No. 1129, January 16, 2019

Foreign Influence on Political Discourse: A New Strategic Challenge

Itai Brun and David Siman-Tov

The warning by Nadav Argaman, head of the Israel Security Agency, that a foreign nation could potentially interfere in the forthcoming Knesset elections has aroused much debate in Israel. Prime Minister Benjamin Netanyahu declared that Israel is prepared to thwart any cybernetic interference in the election. However, while the technological infrastructure used for the election process may be bolstered by known cyber defense tools, influence operations targeting the political debate during elections are a completely different issue. The experience of electoral processes in Western nations in recent years shows that democratic countries are hard-pressed to confront influence operations. To be prepared to stymie foreign influences in the coming elections, an integrated task force must be formed that combines the efforts of governments, civil society, political parties, the media, and large platforms.

Foreign Influence on Political Discourse

In the past year, Israel's Central Elections Committee joined the list of institutions and organizations that receive guidelines from the National Cyber Directorate. However, these guidelines deal primarily with defense against threats to the technological infrastructure (IT) of the electoral process (voter lists, notifications to voters, and the recording, reporting, and publication of results). However, hidden interventions intended to implant ideas and messages in the political debate through various tools and thereby affect the topics of discussion during the election period are a different threat. This form of influence may disrupt the democratic process, even if the technological infrastructure for the electoral process operates correctly.

Elections present a convenient opportunity for influence operations. During this period, political polarization and other rifts are at their peak, the public pays particular attention to unfolding developments, and the demand for news is liable to lead media and private elements to spread information that is not necessarily verified. Interventions in the issues under political debate may lead to two types of influence:

a. Regarding the election results themselves – the election of a particular candidate in the party primaries, or the election of a preferred party (or preferred political bloc) in the Knesset elections.

b. Use of the elections as a key event to deepen polarization in Israeli society and damage public faith in the democratic process and its underpinning ideas (including the credibility of election results).

Lessons from the US 2016 Elections

Russian involvement in the United States 2016 presidential elections offers an example of a strategic influence operation affecting the topics of the political discourse. The objective of Russian interference was broader than the election of Donald Trump as president: it was intended to exploit rifts in American society, and in deepening polarization, cause the American public to lose faith in democracy and in the electoral process. Russia did not necessarily intend for the American public to believe the messages it spread, but rather to spark doubt, weaken the ability to believe in facts, and encourage revulsion at the political system, to the point of creating a lack of desire to vote.

At issue was not only fake news, but also a comprehensive campaign that included thefts, editing, and publication of embarrassing real data in media, and echoes through a vast army of virtual entities ("bots" and "trolls").

The actual extent of the influence of the Russian campaign on the election results is unknown, and it is doubtful it will ever be entirely clear. However, the campaign exposed America's organizational lapses in cyberspace, despite major investments over many years. Russia did not attack the secret core of the American system or its critical infrastructures (which the American defenses protected); instead, Russia contrived to influence the understanding and behavior of millions of voters. In this sense, what happened in the 2016 United States elections was a "cyber Pearl Harbor" – a jolting strategic surprise in the information era. The American intelligence community detected the Russian operations and was able to describe most of the tactics, but it is clear today that it did not correctly understand the essence of the Russian operations, their purpose, or their implications.

Moreover, it appears that there was no element in the United States that felt responsible for thwarting the Russian campaign or was institutionally, legally, conceptually, and technologically capable of managing such a preventive effort. Thus, a chief difficulty when countering operations that seek to influence the political debate is the absence of a holistic viewpoint that examines both external interventions and their actual influence on political discourse. Likewise necessary is an understanding of the technological means and the contents involved.

Following the presidential elections in the US, influence efforts were observed in election campaigns and other incidents in Europe (including in Germany, England, France, and the Ukraine.)

Influence Efforts by Iran and Additional Elements

Various elements in the Middle East have also developed doctrines vis-à-vis influence operations that target political debate. These operations were previously conducted in a variety of ways and in recent years primarily in the digital space, with an emphasis on social media networks. Thus, for example, in recent months a widespread Iranian influence operation was detected, aiming primarily to exacerbate internal divisions in the United States between different social groups. In this framework, sensitive, socially-loaded content designed to provoke the public, radicalize positions, and fan a vehement debate was disseminated in the United States. To run this campaign, Iran built up a widespread, synchronized network of seemingly reliable fake news sites and fake social media entities over the course of several years, created an online discourse around them, and paid to publicize them.

A similar attempt, albeit of more limited scope, was detected in Israel in 2018. This campaign sought to cause the Israeli public to second-guess Israeli policies and the decision making process for security issues.

The Difficulty in Countering the Threat

Lessons from elections in recent years show that various elements make it difficult for democratic nations to confront influence operations. The desire to "clean" the discourse from illegitimate content creates pressure vis-à-vis fundamental principles of the democratic system, primarily defense of the right to free expression. Determining the boundaries of legitimacy - what is acceptable and what is not in influence campaigns - is also problematic. The justified fear of many elements, of entrusting a specific element with the responsibility for content turns out to be a central hindrance when preparing for this phenomenon. Additional difficulties are related to the need for an understanding of the technological means and the contents involved.

An additional difficulty when confronting hostile influences on political discourse is the multiplicity of elements that may be involved in such influence campaigns, both at home and abroad (making it difficult to distinguish between external and domestic influence attempts): states and organizations launching influence operations in order to weaken the state and intensify polarization; internal political elements that spread disinformation (and are liable to echo, unknowingly, messages from foreign influences); apolitical organizations that disseminate false, mistaken, or distorted news for various agendas; and commercial elements that profit from the great popularity of false information. It is very difficult to differentiate between elements and operations that operate in the same space and use the same platforms.

Counter Efforts

Hostile interventions in political debate constitute a new type of strategic threat to democracies, including in Israel. Indeed, political rifts and social polarization make Israel a ready candidate for influence operations, and the warning by Nadav Argaman, head of the Israel Security Agency, that a foreign nation could potentially interfere in the forthcoming Knesset elections is no surprise. Dealing with this threat is a complex, multidimensional challenge that must be faced systematically both in routine times and during the elections themselves. In advance of the April 2019 elections, the following measures should be taken immediately:

a. Create an integrated, inter-organizational taskforce (including civil society elements) to coordinate and direct preparedness and all efforts by various bodies to stymie foreign influences on the political debate. This team will also be responsible for warning the public.

b. Run a simulation with all relevant elements that will pinpoint the gaps in existing readiness and highlight current understanding of the threat, examine possible means of influence, clarify the respective responsibilities and the relative strengths of various elements, and support the development of countermeasures.

c. Reach agreement between the political parties that the protection of the democratic process is a shared interest and therefore steps must be taken to clearly mark political advertisements, refrain from using fake accounts and deceptive and false information, and improve information security (experience shows that parties, politicians, and electoral committees are a major target for attacks).

d. Encourage large platforms (social media and Google) to continue to work to identify and uncover hostile influence operations.

e. Encourage social media to take responsibility to investigate thoroughly information they spread (using comprehensive fact-checking methods and sensitive detection of the possibility of hostile influence).

f. Explain both the phenomenon and ways to counter it to the public.