INSS Insight

Cyber Challenges and Foreign Influence in the Upcoming Knesset Elections

David Siman-Tov, Tamir Hayman, and Amos Hervitz | No. 1622 | July 21, 2022

The Central Elections Committee in Israel and relevant security agencies are poised to combat cyber threats to the election campaign. In a recent report, the State Comptroller asserted that there were deficiencies in preparations for handling cyber threats in the context of the upcoming elections. Publication of the report was followed by public discussion of the threats to the election process and the response to them. The State Comptroller focuses on technological disruption of the election process, and the report ignores possible subversive influence on political discourse by hostile entities, such as Iran. Such malign foreign influence mandates a systemic response involving the recruitment of civil organizations to heighten awareness and thwart external attempts to influence the political discourse in the election campaign. This joins the need for ongoing comprehensive preparation by the relevant state agencies for dealing with the threat to election processes.

In recent years, elections in democratic regimes have become a target for foreign influence and interference. The campaign period, when political tension peaks, is prime time for influence operations. Influence-related goals can range from distorting the election results to taking advantage of the high-tension period to aggravate polarization in society and undermine public trust in the democratic process.

For the sake of conceptual uniformity, it is important to define the threat of foreign influence on democratic processes in the Western world. Discussion of the threat initially focused on computer network attacks (CNA), technological attacks on the voting process and on information systems relevant to the election campaign. With time and experience, attention shifted to include other channels of influence on public discourse, trust, and cognition. Such acts can occur with disinformation or fraudulent content spread in social media and cyberattacks for cognitive purposes, for example, computer network influence (CNI) attacks, which include the theft and publication of information.

In Israel, former Israel Security Agency (ISA) Director Nadav Argaman warned about foreign interference in the election process as early as 2019 (it is unclear whether he meant a technological attack on information and cyber systems only, or whether he was also referring to interference in political discourse on the social networks, and whether his intention was to warn about the threat, or also to deter an effort to influence the election process). In February 2019, former Knesset Central Elections Committee Chairman and Supreme Court Justice (emeritus) Hanan Melcer likewise referred to an attempt at foreign influence and the possibility of influence on the results of election polls. On March 9, 2022, the State Comptroller published a report about information and cyber systems in the Knesset elections, and in late June, publicly criticized the Central Elections Committee's preparedness for cyber threats.

According to the State Comptroller, the findings of the audit shows "an alarming state of preparedness regarding cyber threats, and a lack of alertness on the part of public agencies in their duty to protect the information in their possession." The report cites a number of deficiencies in the response to cyber threats, among them the absence of a document presenting an overall concept and the lack of activity by a public committee for considering the various issues pertaining to prevention of interference in election processes. The State Comptroller also emphasized the need for action to combat cyber threats in ordinary times, i.e., between election campaigns. The report further emphasizes the tension between the Central Elections Committee's need to remain independent and the need for action, such as the strict regulations governing the defense of critical infrastructure (water and electricity), which are the subject of detailed guidance from the National Cyber Directorate. The Committee's independence gives it autonomy in establishing rules and freedom of action to consult with experts and professional bodies. The report emphasizes, however, that the Committee itself and the election processes are not classified as critical state infrastructure, despite their importance to Israeli democracy. In this context, the State Comptroller cites the United

States as an example of a country that has declared its elections to be critical state infrastructure.

In response to the report, the Central Elections Committee claimed that the four recent election campaigns proved its preparedness and ability to handle cyber defense successfully, and that the many deficiencies pointed out by the State Comptroller have already been rectified. In addition, Central Elections Committee director general Adv. Orly Adas noted that the Committee, recognizing that it needed guidance in cyber defense, was in touch with the Ministry of Defense and experts of international renown. The Committee members stated that while it was not an organization supervised by the National Cyber Directorate, it nevertheless received close guidance from it, albeit on a voluntary basis. Furthermore, a "special elections team" was assembled in advance of the elections to the 21st Knesset with participation from the National Cyber Directorate, intelligence agencies, and the Ministry of Justice, which has assisted the Committee in countering the various cyber threats liable to disrupt the process.

The Gray Area: Cyberattacks for Cognitive Purposes and Foreign Interference in Political Discourse

Of the three cyber threats – attacks for purposes of disruption, attacks for purposes of cognitive influence, and manipulation of the content of public discourse on the social media – the State Comptroller addressed only the first one. There are indeed hostile entities, first and foremost Iran, eager to interfere in the Israeli elections process and influence the country’s democratic processes. In the past two years, for example, FakeReporter, an Israeli nonprofit organization, detected malign networks suspected of being under foreign control that were interfering in internal discourse on both the right and left of the political map in Israel, with an emphasis on demonstrations on both sides (for example, exacerbating rifts, encouraging demonstrations, and fabricating incidents of violence).

The threat to election campaigns, as recognized in the West, spans various spheres and is not confined to disruption of the voting systems. The threat to the elections in Israel can indeed be executed using cyberattacks on the voting systems, but also by influencing the content of political discourse via inserting fraudulent content for the purpose of intensifying existing internal tensions in Israel (between Jews and Arabs, right and left, and Sephardim and Ashkenazim). It can also combine these two channels of action.

As a lesson from the Russian interference in the 2016 United States elections, a team was assembled in 2018 in the US National Cybersecurity and Infrastructure Security Agency (CISA) for dealing with the content of political discourse. The team was formed to examine the severity, scope, and influence of the threat to discourse and the elections for the purpose of informing the public, and to cooperate with other relevant agencies in combating this threat.

The experience accumulated in the West with interference by foreign entities in elections highlights the need to connect agencies from the cyber and content spheres, and to integrate them to devise and implement a response to the threat. In an interview with Army Radio in February 2022, however, former National Cyber Directorate Director General Yigal Unna noted that his Directorate had no need to deal with content, and that the ISA was responsible for this aspect, even though he did recognize that the use of content to influence the election results was dangerous and easy to execute. Making the ISA responsible for thwarting subversion seems natural, but while the ISA specializes in countering malign activity in covert areas, it is largely inactive in public social media areas.

One of the reasons for the difficulty experienced by intelligence agencies in countering illegitimate foreign influence on political discourse is that such subversive activity is necessarily a part of political messages delivered in the internal arena – over which a democratic regime has no authority or interest in exercising supervision. This means that there is a gray area that enjoys immunity, while it nevertheless requires a response, where hostile entities are liable to take advantage of it.

Recommendations

The State Comptroller's report on the information and cyber systems under the responsibility of the Central Elections Committee's raises a number of issues that the relevant organizations, above all the Committee, the National Cyber Bureau, and the intelligence organizations, must address. First, there is a need for integrated and ongoing action to thwart foreign efforts to damage the election process between election campaigns and from a long-term perspective. Second, the report highlights the tension between the need to maintain the Elections Committee's independence and the possibility of classifying it as critical infrastructure. Such a classification has a price, and the existing situation, in which the Committee voluntarily accepts guidance, appears reasonable.

The State Comptroller's report naturally focuses on the state's responsibility for key processes related to the election campaign. Nevertheless, because the political parties and their leaders are a target for cyberattacks and influence, this requires an organized effort to increase awareness on their part as well.

The report reflects a conception – which also exists in part of the Israeli security establishment – of the perceived threats to democratic processes, above all election campaigns. According to this conception, strict observance of information security and cyber protection rules of the CNA-type attacks is sufficient for defending these processes. In reality, the enemy is also interested in influencing the election processes in other ways aimed at undermining the elections' credibility, exploiting the elections to inflame societal divisions, and undermining public trust in the democratic process.

The primary lapse, which is also discernable in the report, lies in the focus on technical aspects of disrupting the functions of the information systems, while ignoring the possibility of malign foreign influence through manipulation of content on social networks, including the dissemination of false information or publication of information stolen in cyberattacks. It is clear that monitoring internal political discourse by state security organizations, especially in public spheres, is restricted in a democratic regime, and is sometimes incompatible with the definition of some of the relevant agencies' responsibility. It appears, however, that the possibility of hostile entities attempting to exploit the election campaign to pollute political discourse and damage the democratic process and its authenticity makes this a necessity.

A democratic country must develop tools for preventing foreign subversive entities from harming it by taking advantage of the democratic rules of the game. This requires a definition of the threat, relevant intelligence, multidisciplinary preparation, and an examination of the rules of behavior on social media (in cooperation with the social media companies). In addition, direct involvement of civil organizations (including non-profit organizations, research institutes, and fact-checking agencies) to raise awareness of the threat of foreign interference in public discourse during the election campaign and strengthen resistance to it are recommended.

Editors of the series: Anat Kurtz, Eldad Shavit and Judith Rosen