The Threat of Foreign Interference in the 2019 Elections in Israel and Ways of Handling it

Pnina Shuker and Gabi Siboni

In recent years, foreign countries has increased their attempts to influence democratic processes in rival countries. The aim is to damage the electoral process via cyberattacks on computerized systems or to try and affect the outcomes. Examining the electoral process in Israel makes it possible to identify such attempts and propose ways of dealing with them. This article suggests the need to distinguish between foreign attempts to influence the elections and domestic ones, which are part of the democratic process, and outlines directions for action to improve efforts to counter foreign interference in the elections.

Keywords: Elections, influence, cyber, democratic process, social media

Introduction

The possibility that a foreign country would try to influence the democratic process in Israel sparked intensive activity leading up to the elections to the twenty-first Knesset. In July 2017, Lt. Gen. Gadi Eisenkot, then the chief of staff, raised the possibility of foreign interference in Israel's democracy, which he described as a vital challenge. In a debate in the Knesset, Eisenkot

Pnina Shuker is a Neubauer research associate at INSS and a doctoral student in the Political Science Department at Bar Ilan University. Prof. Gabi Siboni is the director of the Cyber Security Program at INSS.

mentioned two related phenomena: attempts to interfere with the outcome of the elections by hacking into and damaging the computer-support systems and attempts to influence voters through mass manipulation, by means of posts and ads on social media and internet sites.[1]

Following the announcement that the elections would be brought forward to 2019, senior political and defense figures in Israel expressed many warnings about possible foreign interference. In December 2018, at the Dov Lautman Conference on Educational Policy, Israel's President Rivlin said that "interested parties want to divert attention from the facts to speculation and defamation . . . In the world of 'fake news' we must safeguard the right of citizens to have access to facts without distortion."[2] The president did not clarify whether he was referring to foreign interference or to the political debate within the country. In early January 2019, the head of the General Security Services (GSS), Nadav Argaman, warned that a foreign country was planning to intervene in the elections in Israel, and that the attack could be cyber-based.[3] At the end of that month, at the Cybertech Conference, Prime Minister Netanyahu also declared that Iran was trying to sway the elections in Israel by means of fake network accounts, and it was conducting cyberattacks against Israel "on a daily basis."[4] According to State Comptroller Yosef Shapiro, "foreign intervention that damages the reliability of the systems and of the results would have a drastic effect on public trust in the authorities."[5]

These statements reflected the considerable anxiety among senior politicians and military/security personnel in Israel over the possibility of foreign interference in the Knesset elections, which, for the first time in the state's history, were held in the shadow of this fear. Given this background, this article examines the danger of foreign interference in the 2019 elections and the efforts to address the threat. This article does not consider attempts to

1 Amos Harel, "The Cyber Authority Prepares a Plan of Defense against Foreign Interference in Israel's Elections, *Haaretz*, July 13, 2017.

2 "State President at Dov Lautman Conference: 'Change from Identity Politics to Ideas Politics,'" *Ynet,* December 27, 2018.

3 Amir Buchbut and Yaki Adamker, "Head of the GSS Warns: A Foreign Country is Planning to Interfere in the Elections in Israel," *Walla*, January 8, 2019.

4 Itai Shickman, "Iranian Cyberattacks are Constantly Monitored," *Ynet*, January 29, 2019.

5 Buchbut and Adamker, "Head of the GSS Warns."

influence and manipulate perceptions within the framework of the political and democratic debate within Israel, which are part of Israel's freedom of expression and which Israeli democracy can and should accept.

The first part of the article surveys the phenomenon and characteristics of foreign interference in elections globally across electoral systems. The second part describes the ways in which Israel has prepared to deal with this problem. Finally, the article examines ways of improving how Israel handles similar challenges.

The Phenomenon of Foreign Interference in Democratic Elections

In recent years, foreign elements (governments and non-governmental) have used digital techniques to damage the democratic process in rival countries. They engage in cyberattacks on computerized systems supporting the electoral process in those countries (databases, software, communications systems) in order to damage or steal data, or to interfere with the operating of these systems. In addition, various methods involving large-scale campaigns to subliminally influence voters have also been exposed. These attempts have a range of objectives, from undermining public faith in the democratic process to affecting the support for specific parties and candidates. Sometimes the goal is to dissuade people from participating in the elections on their basis of their identity or socioeconomic status.[6] These efforts have made extensive use of social media.

Contrary to the perception that social media exposes people to a wide variety of views and opinions, it is clear that Facebook—the most popular social network—actually creates closed spaces of users with homogenous views. These closed spaces occur as a result of users' actions, such as blocking friends or removing them from the list of followers, or attacking anyone who expresses different political opinions, particularly in the case of network members whose links are weak. Thus, Facebook can create separation, even polarization and extremism, in the case of political views, instead of encouraging moderation and tolerance of a wide range of opinions.

6 Chris Tenove, Joran Buffie, Spencer McKay, and David Moscrop, *Digital Threats to Democratic Elections: How Foreign Actors Use Digital Techniques to Undermine Democracy* (Vancouver: Center for the Study of Democratic Institutions, University of British Columbia, 2018), p. 26.

In addition, the network's software, which, among other things, collects data about users and their friends' lists, shares specific information with each user based on their personal preferences. This is another factor contributing to a homogenous social environment,[7] due to the human tendency to connect with others who share similarities—ethnic, geographic, ideological—a phenomenon known as homophilia. This tendency, leading to the "herd" mentality on social media, is reinforced by the social media search engines, which generate results that match the user's attitudes.

The problem is that many people still regard what they see on the internet as a true representation of world events, even though it is, in fact, a subjective display tailored to the user and the user's location, economic and social status, relationships and so on. In the context of the elections in Israel, Karine Nahon notes that, in the elections to the twentieth Knesset, many left-wing internet users assumed that the left would win the elections, on the basis of what they saw on Facebook. The flow of information has extensive influence, so that if we examine this case, for example, the assumption that "the left is going to win" could perhaps cause some left-wing voters not to bother voting, since "in any case we're winning."[8]

Efforts to manipulate public opinion or to distribute information on networks are carried out partly by "bots." A bot, short for robot, is a software agent designed for a range of uses. The principle use in this context is the creation of user profiles on social media or software tools to increase the spread of specific posts. Sometimes, the software is able to handle a large number of entities simultaneously. In this way it is possible to distribute a wide range of content aimed at specific interests—commercial, political, or criminal—with the potential for various kinds of abuse, but the common denominator is the use of automation technologies to influence the flow and spread of information.[9]

It is possible to create and distribute disinformation that is focused on reinforcing existing controversies, such as conflicts between parties, in order

7 Nicholas A. John and Shira Dvir-Gvirsman, "'I Don't Like You Any More': Facebook Unfriending by Israelis During the Israel–Gaza Conflict of 2014," *Journal of Communication* 65, no. 6 (2010): 953–974.

8 Roi Goldschmidt, "Distributing False Information on the Internet and Cyberattacks Intended to Influence Elections," Knesset Research & Information Center, June 2017 [in Hebrew].

9 Ibid.

to drive a wedge between allies and undermine shared norms of democratic debate. For example, Russia used social media platforms in the 2016 US presidential elections, spreading messages that purported to show Muslim support of Hillary Clinton. In this context, they purchased advertising space on Facebook where they ran messages such as "Support Hillary; save American Muslims." The purpose was to link political Islam to Clinton.[10] In addition, there was a great deal of activity intended to encourage black Americans to participate in demonstrations and disrupt public order.[11]

Disinformation can also be used to deter people from participating in polls. Research on elections shows that election posters only occasionally seek to persuade people to change their voting intentions, and that they can be more effective in raising or lowering voting rates and influencing the vote in favor of less well-known candidates. In addition, it is possible to harm democratic participation by using digital techniques in order to extort, threaten, or harass candidates.[12]

According to Karine Nahon, the problem of erroneous or distorted information is particularly troublesome during events such as war or elections where the demand for information is greater than usual, and the media tends to spread information quickly, often without sufficient, in-depth fact checking. As a result, the public do not "check the facts" but rather adopt positions based on false information, or when beliefs that they already hold are reinforced. Nahon states that social media and viral items on the internet provide much greater possibilities for using disinformation as a means of influencing people during elections.[13]

To sum up, the ability to vote and influence—the most basic form of political participation—is currently under threat from foreign digital interference. As stated above, this interference can be achieved through cyberattacks on

10 David Siman Tov and Yotam Rosner, "Conscious Undermining: Russia in the US Presidential elections as a New Threat to the West," *INSS Insight* no.1031 (Tel Aviv: Institute for National Security Studies), March 8, 2018.

11 Leonid Nevezlin, "The World's Most Dangerous Troll," *Liberal,* February 2019 [in Hebrew].

12 Tenove and others, *Digital Threats to Democratic Elections*.

13 Goldschmidt, "Distributing False Information on the Internet and Cyberattacks in Order to Influence Elections."

computerized-support systems in order to disrupt *the electoral process*, or through disinformation campaigns intended to affect *the election results*.[14]

Attempts to Influence Elections Worldwide

In recent years, there have been numerous cases of countries intervening in the electoral processes of other countries using internet-based technology. Over the last decade, Russia has been particularly prominent (although it is not alone) among the countries that have used cyber means to influence elections. It attempted to interfere in the elections in Ukraine (2014), in the United States (2016), France, Germany and Holland (2017), and in referenda in Britain, Holland, Italy, and Spain (2017).[15]

The most striking recent example of interference in elections, whose results continue to affect the United States as well as the entire world, is the case of Russian intervention in the US presidential elections in 2016. In early January 2017, the American intelligence community published its assessment that Russia had interfered in the elections using a range of means in order to damage the chances of the Democratic candidate Hillary Clinton and promote the election of Donald Trump.[16] The report states that Russia's efforts included cyber campaigns on social media, in which they used bots, trolls, and hackers to simultaneously spread disinformation regarding a number of competing narratives, in order to exacerbate existing conflicts within American society and undermine trust in western institutions and the democratic process in general.[17]

In February and July 2017, Special Prosecutor Robert Mueller submitted detailed indictments against twenty Russian citizens for interference in the US presidential elections. Nevertheless, no clear explanation has been given of how this interference actually affected the election campaign or the outcome. Even the most prominent research on this subject does not state unequivocally that Russian attempts to exert influence bore fruit but rather

14 Tenove and others, *Digital Threats to Democratic Elections.*

15 Eli Bechar and Ron Shamir, "Cyber Attacks on Electoral Systems: How to Deal with Them?," *Policy Research* (Jerusalem: Israeli Institute for Democracy and Research Program on Cyber Defense) 136 (2019): 9–10 [in Hebrew].

16 Office of the Director of National Intelligence, "Assessing Russian Activities and Intentions in Recent US Elections," January 2017.

17 Andrew Radin and Elina Treyger, "Countering Russian Social Media Influence," *RAND Corporation*, November 2018.

assumes that this is highly probable, based on the circumstantial overlap between Russian efforts and changes in the public and media debate and the surprising results of the elections.[18] It is worth noting that at the end of March 2019, Mueller published his final conclusions, which, in fact, confirmed the conclusions of the Senate Intelligence Committee report of 2017, that Russia had conducted a campaign of hacking into computer systems and spreading disinformation designed to deepen rifts in American society and influence the 2016 elections. Mueller identified two arms of the Kremlin's campaign: the dissemination of false information run by an organization known as the Internet Research Agency and hacking of computer systems by Russian intelligence bodies that worked against the Democratic party.[19]

It is clear, however, that not only Russia has interfered in democratic elections. China did the same in the 2018 elections in Cambodia,[20] while an increasing number of reports have pointed to Chinese efforts to interfere in the US elections, which led President Trump to announce that China was seeking to influence the November 2018 mid-term elections to the US Congress and other institutions.[21] At the end of January 2019, Facebook and Twitter both announced that they had exposed an Iranian secret attempt to exert cyber influence on Israel. It included content that was designed to reinforce the Iranian narrative regarding developments in the Middle East and on the Israel-Palestine conflict, as well as criticism of Prime Minister Netanyahu, his policy, and his family, apparently in an attempt to sway Israeli public opinion before the Knesset elections. The link, however, is circumstantial and it is not clear whether the moves attributed to Iran were indeed intended to affect the elections in Israel.[22]

---

18 Kathleen Hall Jamieson, *Cyber-War: How Russian Hackers and Trolls Helped Elect a President* (Oxford: Oxford University Press, 2018).

19 US Department of Justice, Special Counsel Robert S. Mueller, "Report on the Investigation into Russian Interference in the 2016 Presidential Election," March 2019.

20 Scott Henderson, Steve Miller, Dan Perez, Marcin Siedlarz, Ben Wilson, and Ben Read, "Chinese Espionage Group TEMP.Periscope Targets Cambodia Ahead of July 2018 Elections and Reveals Broad Operations Globally," *FireEye*, July 10, 2018.

21 Abigail Grace, "China's Influence Operations are Pinpointing America's Weaknesses," *FP*, October 4, 2018.

22 Hagar Buchbut, "Facebook Removes Hundreds of Pages Containing Iranian Fake News," *Ynet,* January 31, 2019 [in Hebrew].

At the time of writing, it is not clear to what extent the 2019 elections in Israel were a target for foreign interference and to what degree (if at all) such interference succeeded. Whatever the case, the State of Israel implemented protective efforts before and during the elections.

Efforts to Protect against Foreign Intervention in the 2019 Israeli Elections

There are three possible types of cyberattacks in the context of the Israeli elections. The first is the "classic" cyberattack designed to interfere with the electoral system and the democratic process, including attacks on computerized systems and databases that support the electoral process, or that are related to political parties and polling companies.[23] The second is an attack on political parties and candidates in various ways, such as theft of personal and political data to be published at the most damaging opportunity, disruption of party preparations for the elections, and more. The third includes attempts to subliminally influence public opinion through social media.

Responding to these threats is a complex challenge, and it is important to distinguish between efforts by political parties themselves—a legitimate process that every democratic society must allow—and efforts by foreign elements. Any response may involve an infringement of privacy as a result of monitoring social media. The "classic" cyber threat requires defensive efforts by the interested parties, such as the Central Election Committee (CEC), the parties, polling companies, and other elements that could be exposed to these attacks. The National Cyber Directorate (NCD) has undertaken to provide assistance to all relevant bodies and is working with the Central Election Committee to combat the threat.

National preparations for the elections to the twenty-first Knesset included the establishment of a special elections team led by the NCD, with members from the defense establishment and the Ministry of Justice. The team met regularly, and its activities were based on learning from the experiences of other countries and carrying out exercises with the relevant bodies—the CEC and others in the political and civil systems (such as polling companies). This signified a substantial advance in national readiness in dealing with threats to the democratic process, although at this stage it is only in the context of

23 This is in contrast to efforts to influence the outcomes by means of activity on social media or harmful revelations about candidates and parties.

the elections, with emphasis on technological readiness. Meanwhile the team has not addressed the other threats described above, nor has it involved civil society in the response, as other countries (such as Denmark) have done.[24]

In February 2019, the NCD sent all the political parties in Israel a special document intended to help them protect themselves against various cyber threats. The document specifies procedures and guidelines for strengthening their systems, websites, means of communication, and other virtual infrastructures, and addresses the protection of personal computers, the parties' internal networks, email, mobile phones, smart watches, and telephone exchanges. A particularly long section of the document is devoted to the protection of party websites, including details of what is required.[25]

Notwithstanding this activity, officials linked to the NCD clarified that this body is not obliged to deal with content relating to the elections system and does not intend to focus on frustrating campaigns intended to influence attitudes. However, in a debate in the Knesset in October 2018, just before the local authority elections, the NCD presented a cooperative initiative with Facebook to remove fake profiles.[26] Representatives of the Israeli Internet Association criticized this move, however, arguing that the NCD was not qualified to deal with this subject, even indirectly.[27]

When the date of the Israeli elections was published, Facebook announced that it was setting up a situation room in order to monitor information from a range of sources, including political parties and individual users, regarding posts and campaigns that breach its terms of use. The situation room was supposed to respond quickly to any violations of the rules. For this purpose, Facebook employed a censorship team, which used an artificial intelligence tool to highlight suspicious content. Another tool used by the team involved pushing back problematic campaigns, even if they were funded, in order to

---

24 "Summary of a Simulation Discussion on the Illegitimate Influence on Public and Political Debate by Digital Means, toward the 2019 Elections in Israel," Institute of National Security Studies, Israeli Institute of Democracy, and the Israeli Internet Association, February 26, 2019 [in Hebrew].

25 Ran Bar-Zik, "The Cyber Directorate Issues a Guide to Protection for Parties: Will They Learn the Lesson?" *Haaretz,* February 20, 2019 [in Hebrew].

26 Tal Shahaf, "The National Cyber Directorate: We Worked with Facebook and Twitter to Remove Thousands of Fake Accounts," *Globes*, October 15, 2018 [in Hebrew].

27 Omer Kabir, "Thousands of Fake News Accounts Exposed, which Tried to Influence the Municipal Elections in Israel," *Calcalist,* October 15, 2018 [in Hebrew].

diminish their appeal. Facebook also provided training for Knesset members and their parliamentary assistants who wanted to know how they could avoid misusing the platform, even giving advice on how to protect political accounts from hackers who could break in and issue false announcements from them.[28]

In mid-February 2019, Facebook announced it was increasing its efforts to avoid influencing the elections in Israel, including a "clean up" of followers of politicians. In this campaign, fake and bot accounts were removed from the network and also removed from the profiles of parties and candidates. Facebook even offered media personnel a tool for reporting networks of fake users.[29] Moreover, in mid-March 2019, the Facebook transparency tool for political announcements came into force in Israel, and thus Israel became the fifth country in the world to use this tool, which is intended to combat the threat of foreign interference and anonymous propaganda.[30]

At the beginning of January 2019, a number of lawyers submitted a petition to the Central Elections Committee, asking it to extend the laws of election propaganda to include propaganda on the internet. The petition included a request to the chairperson of the committee to issue an injunction forbidding the parties participating in the elections, or entities acting for them—whether or not for payment—from publishing any announcement, notice, response, "talkback," or "like" that did not carry the name of the party or the candidate on whose behalf it was published. In addition, the petition asked for an injunction forbidding the parties to pay any entity that did so on their behalf or in their name and to apply the injunction to all ads and posts on social media, SMS, and instant messaging programs.[31] The chairperson of the Central Election Committee accepted the petition and at the end of February 2019 set a precedent by issuing an order that required parties to identify themselves on any kind of propaganda on the internet and

28 Uri Berkowitz, Oshrit Gan El, and Tal Shahaf, "Bots, Fake News or Stories: What Will Determine the Fate of the Next Elections?" *Globes*, December 27, 2018.

29 Anat Bein-Leibowitz, "Facebook Embarks on a Campaign to Remove Fake Accounts In Israel; in its Sights – The Bots of Netanyahu and Gabbay," *Globes*, February 20, 2019 [in Hebrew].

30 Hagar Buchbut, "Just before the Elections: A Fast Form for Reporting Bots and the Facebook Transparency Tool," *Ynet,* March 14, 2019 [in Hebrew].

31 Yasmin Yablonka and Tal Shahaf, "An Ancient Law and Netanyahu's Objection: Is it Possible to Supervise Propaganda on the Internet?" *Globes*, January 8, 2019 [in Hebrew].

social media. On the grounds for this decision, the committee's chairperson stressed that, apart from the legal obligation, anonymous propaganda makes it difficult for the security forces to dispel suspicions of foreign intervention in the Knesset elections.[32]

At the end of February 2019, several internet and data security experts asked the Central Elections Committee to take steps prior to the Israeli elections to identify attempts to create fake online identities, particularly on social media. The experts expressed fears that foreign elements might try to interfere in the elections by using social media to spread fake information and manipulate users in other ways and called for the appointment of an official to coordinate reports of fake accounts designed to influence the election process. The model they wished to create is similar to the model that Israel has used against incitement on social media.

Currently, the state has no legal authority to force networks such as Facebook or Twitter to remove posts. There is, however, an interface enabling users to report and request the removal of posts that amount to incitement or breaches of the law: The Cyber Department of the office of the state attorney contacts the relevant network and asks for such material to be taken down. According to the state attorney's data, in about 85 percent of cases, the networks have responded positively to the request.[33]

Apart from the above, citizens held several initiatives to mark propaganda in a clear and consistent way, to avoid the use of fake accounts, and to indicate bots. In this framework, they pledged not to make use of any personal information in order to manipulate individuals emotionally and to secure campaign information, including by means of encrypting personal messages and securing databases.[34] A special online form was created enabling social media users to submit quick and effective reports about bots, suspicious accounts, and anonymous election propaganda, thus facilitating more effective handling of the problem on the various platforms.[35]

---

32 Daniel Dolev, "The End of Anonymous Propaganda: Parties Must Identify Themselves in Online Advertising," *Walla*, February 27, 2019 [in Hebrew].

33 Daniel Dolev, "Request to the Chairman of The Elections Committee: Act Against Online Attempts to Influence the Elections," *Walla*, February 25, 2019 [in Hebrew].

34 Guy Luria and Tehilla Shwartz-Altshuler, "Committing to Fair Elections Online," Israel Institute for Democracy, February 16, 2019 [in Hebrew].

35 Buchbut, "Just Before The Elections: A Fast Form for Reporting Bots and the Facebook Transparency Tool."

Most efforts to defend against foreign interference in the elections clearly were civilian initiatives, and we do not know about specific state preparations for such defense, notwithstanding the announcement by the GSS that "the security system is able to ensure the process of free, democratic elections."[36] The Central Election Committee also announced that "together with security personnel, the Committee has studied what happened in other countries and is formulating an outline of action."[37]As of the time of this writing, it is not clear if there were any foreign attempts to influence the elections to the twenty-first Knesset, or whether efforts to stop such attempts (if they existed) were successful.

It can be noted marginally that early in 2019, the state comptroller announced that he had instructed his staff to prepare for an audit of social media and for cyberspace and to examine the readiness of the authorities to protect themselves against cyberattacks on the computerized systems required for holding elections.[38]

Conclusion

The purpose of this article was to survey the steps taken to protect against the possibility of foreign interference in the Knesset elections in 2019, given similar attempts in other democratic countries in recent years. Until now, hardly any such attempts have been exposed to the Israeli public although the use of unidentified accounts or fictitious accounts in the framework of the internal political debate have been revealed.

The public's focus on the internal debate highlights the need to regulate the use of networks during election campaigns in particular and in terms of the democratic process in general. First, it is necessary to distinguish between various aspects of the phenomenon, and, above all, the use of bots, as political parties may operate or hire the services of companies who operate bots in order to promote their positions or to harm rival candidates. The use of bots should be deemed legitimate, providing it complies with the instructions of the head of the Central Elections Committee regarding

36 Amnon Abramowitz, "The GSS: 'We Have the Tools to Frustrate Foreign Attempts to Influence the Elections," *News 12,* January 8, 2019 [in Hebrew].

37 Dafna Liel, "Elections 2019: Preparing Action against Foreign Interference," *News 12,* January 9, 2019 [in Hebrew].

38 Buchbut and Adamker, "Head of the GSS Warns: A Foreign Country Is Planning to Interfere in the Elections in Israel."

the need to publish the name of the party or candidates in whose name the material is distributed.

Second, with respect to the publication of fake information, it is hard to envisage a fast and relevant mechanism (not a legal process) that would be able to determine which information is fake and which is genuine. The distance between such a mechanism and the risk of serious damage to freedom of expression is quite small. Therefore, it is suggested to allow the publishing of any information, even if some would define it as fake information, as a legitimate part of the democratic debate. Any person or organization who feel themselves injured by such publication can implement their right to seek redress from the legal system with a libel case or claim for damages.

Finally, regarding the use of unidentified profiles by individuals (not by parties), Twitter allows users to have anonymous accounts. Such an account is very important, as it permits people who are not able or willing to expose their identity (for example: state employees) to participate in the political debate and thus realize their right to express their views freely. The situation is quite different regarding the activity of foreign elements seeking to influence the democratic process; this kind of foreign activity amounts to blatant meddling in Israel's democratic process, which should be seen as illegitimate and must be opposed.

The best defense against foreign attempts to interfere in the 2019 Knesset elections clearly came from measures to protect against classic cyberattacks. As of yet, the Israeli public have not learned of any organized, methodical ability (if it even exists) to protect against attempts by foreign elements to exert influence. Defense against such attempts should include a number of basic components. First is intelligence, with the aim of collecting information from a range of sources, both overt and covert. Second, it is also vital to be able to research and analyze the data in order to build a picture of the situation and identify foreign and hostile efforts to influence the democratic process. This includes being able to distinguish between the domestic (legitimate) debate and the external debate, which should be prevented.

We can list a number of ways to thwart foreign attempts. First, the campaign should be exposed to the public, all while maintaining the confidentiality of sources, if necessary. Such exposure can remove the sting from a campaign and minimize its effect on the public. Second, it is possible to contact the media companies concerned, show them the information and demand its

removal, while also blocking the relevant user accounts. Finally, it is possible to proactively engage with the elements behind the campaign in order to thwart their plans.

Achieving this requires cooperation between organizations and technologies. The proposal is to set up a special task force to coordinate activity, based on the abilities of all the defense organizations in Israel. Due to the subject's sensitivity, the team should be directly subordinate to the Central Elections Committee or another apolitical entity. The special task force must acquire—and, if necessary, define and develop—technological tools to help it achieve its objectives.

Over the next two years, more than twenty election campaigns will take place in Europe and North America. We can assume that other countries will have strong interests in the outcomes of these elections, and there are even indications that attempts to interfere in them will occur.[39] Therefore, any lessons learned about the efficacy of steps to defeat foreign meddling in elections in Israel could have great importance for other countries expecting to hold elections.

39 Michael Chertoff and Anders Fogh Rasmussen, "The Unhackable Election: What it Takes to Defend Democracy," *Foreign Affairs* 98, no. 1 (2019): 157.