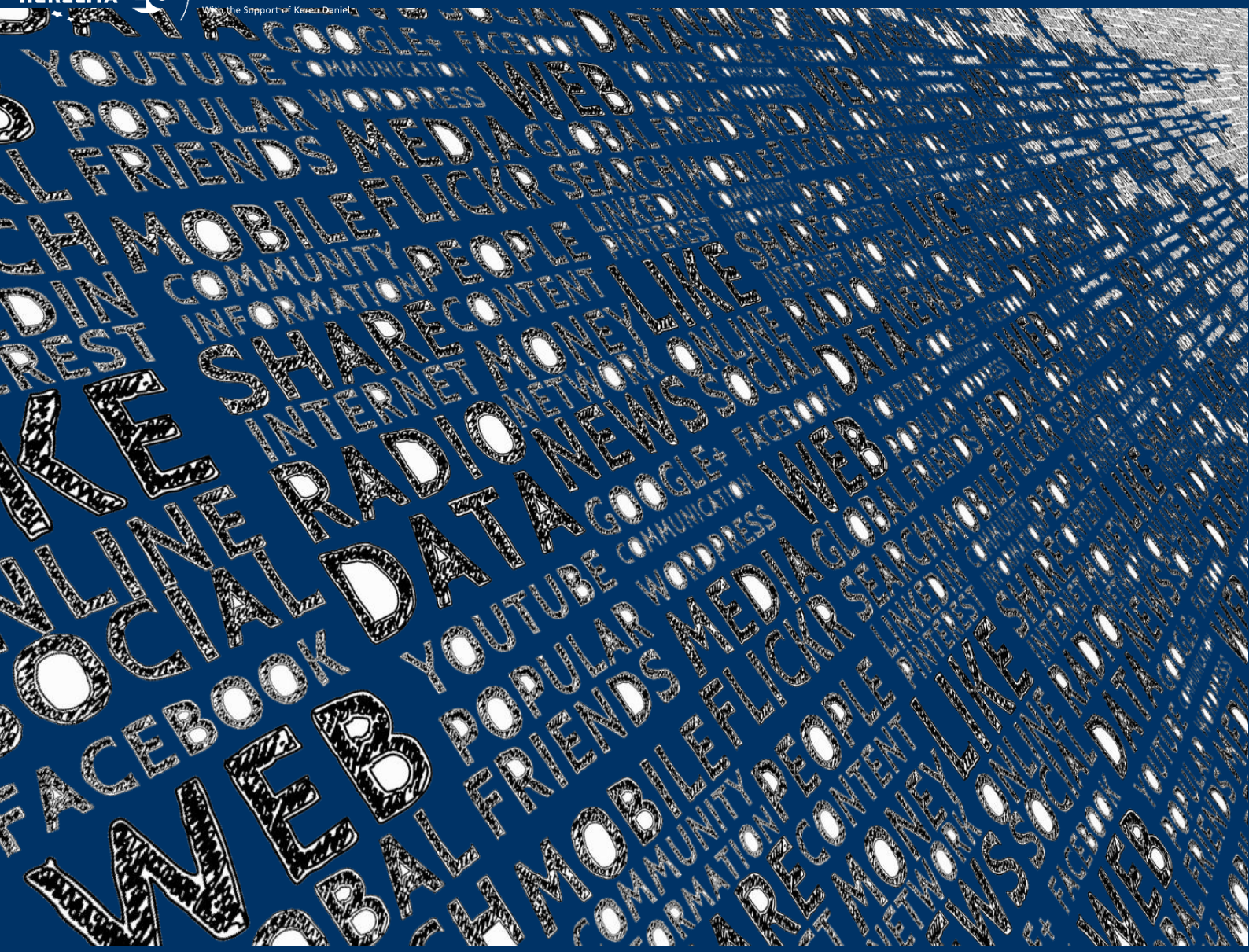
IDC HERZLIYA

ICT International Institute for Counter-Terrorism

With the Support of Keren Daniel



Digital Terrorism in the Israeli Election Campaign?

The interference of terrorist organizations and state sponsors of terrorism in the election campaign

Introduction

Approximately two years ago, following clear evidence of Russian interference in the US presidential election campaign, the US administration announced to dozens of countries around the world that their election campaigns were a target for the "Russian government's cyber activists". There is no doubt that the Russians used online measures to interfere in the election campaigns of most Western countries, including the US, Germany, Britain, France, Italy, Montenegro and more. Evidence of this even led Putin to admit half-heartedly the possibility that, according to him, patriotic hackers from Russia had carried out cyber-attacks "against countries that had strained relations with Moscow and did so on their own initiative". However, US intelligence authorities thought differently, and recently the US Justice Department filed indictments against 12 Russian intelligence officers, all of whom were employees of the Putin administration, on suspicion of acting under its guidance to skew the US elections. A report prepared for the US Senate Select Committee on Intelligence exposed the Russian disinformation campaign, which included millions of posts on social networks designed to influence the 2016 presidential election. Russian agents exploited all possible social networks, including Twitter, Facebook and YouTube, to influence the online discourse surrounding Donald Trump's candidacy. The goal of the Russians, according to the report, was to confuse, distract and influence voters. The Kremlin's efforts have been spearheaded by the Internet Research Agency, a Russian governmental body that has published posts on issues such as race, immigration and weapons in order to create disputes and divisions among American voters. The Russian agents, against some of whom indictments have already been filed in the US for criminal interference in the elections, divided the American electorate into key groups and conveyed specific messages to each group.[1]

A report prepared for the US Senate Select Committee on Intelligence exposed the Russian disinformation campaign, which included millions of posts on social networks designed to influence the 2016 presidential election.

In Israel, too, the fear of Russian interference in the upcoming election campaign has increased, as expressed in a statement by the head of the Shin Bet, Nadav Argaman, about a "foreign power" that

[1] "Five Takeaways From New Reports on Russia's Social Media Operations", *New York Times*, December 17, 2018, https://www.nytimes.com/2018/12/17/us/politics/takeaways-russia-social-media-operations.html

interferes in the Israeli political system via the Internet. [2]Attention, of course, is focused on Russia: With a number of organized attacks, the Russians demonstrated impressive capabilities of infiltration, hacking, interference and disruption using online means. Russian hackers, on behalf of Putin, already attacked Estonia (2007) and Georgia (2009), hacked into the election headquarters of the Democratic Party in the US, planted advanced viruses within the e-mail systems of government organizations in Germany, as well as in the German parliament and in the offices of Chancellor Angela Merkel's party, waged a cyber-attack against election campaigns in many countries, including the Ukraine (2014), the US (2016), France (2017), Germany (2017) and Holland (2017), and interfered in a referendums in Britain, Holland, Italy, and Spain (2017). In these attacks, they combined "hard" measures (such as disrupting the computer systems of election administration, hacking campaign managers' computers, leaking party data, etc.) and "soft" measures, mainly including penetrating and influencing the public discourse by invading social networks.[3]

The Threat is Not Only from Russia

Is Russia the only one threatening the election campaign in Israel? Terrorist organizations and state sponsors of terrorism should also be included on the map of online threats. There have already been past attempts by terrorist organizations and their agents to interfere in the Israeli election campaign. So far, they have done so mainly by launching terrorist attacks near Election Day, which had an impact on the election results. In an ongoing study of several election campaigns in Israel, it was found that a terrorist attack carried out within three months before an election correlated to an increased number of mandates in support of parties from the right-wing bloc in the area where the attack took place.[4]

Terrorist organizations are also preparing to participate in the 2019 election campaign. For example, Hamas spokesman, Fawzi Barhoum, stressed that "the brave resistance will not allow Palestinian blood to be used as a fuel for the election campaigns of the occupation. Rather, it seeks to preserve

[2] On July 7, 2019, the head of the Shin Bet, Nadav Argaman, appeared at a conference of the Friends of Tel Aviv University, during which he spoke of a "move that could affect the results of the upcoming election" due to be held on April 9, and warned of "interference by a foreign country". See: https://www.ynet.co.il/articles/0,7340,L-5443404,00.html

[3] Weimann, Gabi. "Will Putin Also Interfere in the Election Campaign in Israel?", *Ha'ayin Ha'shviit*, December 18, 2018, https://www.the7eye.org.il/313117 ;
"Senate reports show scope of Russian election meddling", *CNN Politics*, December 2018, https://edition.cnn.com/videos/politics/2018/12/17/russia-2016-report-social-media-ath-vpx.cnn

[4] Berrebi, Claude and Esteban Klor, "Are Voters Sensitive to Terrorism? Direct Evidence from the Israeli Electorate", Samuel Neaman Institute, https://www.neaman.org.il/Are-Voters-Sensitive-Terrorism-Evidence-Electorate-HEB

the blood of the Palestinians and the interests of the Palestinian people…".[5] In contrast, the Israeli media has reported in recent days that the Hamas secret council decided to gradually escalate until the elections in Israel without being dragged into war, in order to extract additional gains from Israel in the near future. According to Palestinian sources, the Hamas leadership understands that until Election Day, Netanyahu is more easily pressured because he does not want a war and, therefore, he can be forced to enter the second stage in ceasefire agreements. [6]Hamas is not the only organization following the election campaign in Israel. Hezbollah has also been conducting psychological warfare against Israel, with the help of Iran, since the 1990's. In an interview held on January 27, 2019, which was published by the moqawama.org Web site, Hezbollah Secretary-General, Hassan Nasrallah, emphasized:

"I do not want to interfere in their [Israel's] elections since, for us, Netanyahu, Barak and [any Israeli] person, whether dead or alive, is no different". It should be understood that "this person [meaning Netanyahu], especially in the weeks and months until the election, may make mistakes in assessing the results of his crises and his aspirations. This is a person who will sacrifice anything to remain prime minister or to stay out of jail". [7]

However, terrorist organizations are not satisfied with the "old type" of conventional attack; they are fully aware of the existence of cyber warfare, digital tools, and the use of online platforms for attacks. Israel has often suffered cyber-attacks by members of terrorist organizations and their supporters who tried to disrupt critical systems and Web sites, hack into accounts, and more. The question is, what will prevent organizations such as Hamas, Hezbollah, the Palestinian Islamic Jihad and terrorism-sponsoring governments, such as Iran or Syria, from using digital terrorism against the Israeli election campaign? At a cyber conference held at the end of January 2019, Israeli Prime Minister Benjamin Netanyahu said that "Iran attacks Israel in cyberspace daily, and we are monitoring and preventing it every day."[8]

Interference in the election campaign through hacking computers and other online means, like any other crime, requires two conditions: motivation and ability. Motivation exists, as we have seen in the past. Terrorist organizations and state sponsors of terrorism have a great interest in disrupting Israel's election campaign and influencing its results. But what about their ability to disrupt Israel's election campaign? Terrorist organizations in the Middle East have knowledge and experience in

[5] January 22, 2019. https://twitter.com/HamasInfoEn/status/1087825799993061377
[6] January 28, 2019. https://twitter.com/kann_news/status/1089585334323736582
[7] https://www.moqawama.org/essaydetails.php?eid=35453&cid=330
[8] Namar, Stav, "Netanyahu: January 29, 2019, "Netanyahu: "Iran Attacks Israel in Cyberspace Daily"", Maariv Online, January 29, 2019 https://www.maariv.co.il/business/tech/Article-682404

using psychological warfare on the Internet, including interference on social networks. In 2017, Hamas waged a cyber-attack on social networks in the framework of which it created dozens of fake profiles of young, beautiful women who reached out to IDF soldiers, and extracted classified and sensitive information from them. Dozens of soldiers fell into the trap. In July 2018, Hamas renewed its efforts and again activated fake profiles on social networks in order to take control of soldiers' mobile phones and computers. This time, the terrorist organization succeeded in upgrading its methods and trying to hunt soldiers through the WhatsApp application and other social networks. Hamas is neither alone nor different: all terrorist organizations in the Middle East are active on social networks and are experienced in malicious interference on these networks.

Recently, a comprehensive study was conducted that reviewed the digital weaknesses in the Israeli election campaign.[9] The study, which was carried out by two former Shin Bet officials, identified the various threats and classified them into three types: 1. attacks on the election process; 2. attacks on political players, such as parties, election headquarters, candidates and campaigns; 3. attacks on social networks, which are likely to serve an arena for influencing public opinion and social discourse. Israel, a recognized cyber power, is capable of defending itself from "hard" types of attacks on the election campaigns. Israelis experience thousands of attempts daily to infiltrate and disrupt the computer systems of the government, the army, banks, energy, transportation and more. Its extensive experience in developing sophisticated defenses will pose a serious challenge to hackers serving terrorist organizations, Iran or Syria. But what about "soft", less violent attacks? Here, the Israeli defense will face more difficulty: social networks can be breached by anyone and the ability to manage, control and block content is in the hands of private companies like Facebook, Google and Microsoft, whose powerlessness has already been demonstrated.

Social networks can be breached by anyone and the ability to manage, control and block content is in the hands of private companies like Facebook, Google and Microsoft, whose powerlessness has already been demonstrated

Avatars, Bots and Trolls in the Service of Terrorism

[9] Shamir, Ron and Eli Bahar, "Defending Israel's Elections from Cyber-Attack – What Should be Done?", The Israeli Institute for Democracy and the Cyber Security Research Program, the Faculty of Law, Hebrew University, January 2019.

How can terrorist organizations and their supporters attack Israeli political discourse? Through social networks, it is possible to spread false rumors, promote "fake news", incite and radicalize discourse, cause harm to candidates and parties, widen social rifts, and plunge the election campaign into an abyss of extremism, distrust, sectarianism and violence. To do this, terrorists have digital tools that are well-known from the online commercial world: "avatars", "bots" and "trolls". An **avatar** is a fictional digital character that appears on the Web and pretends to be real. For instance, fictitious users can be found on social networks equipped with a name, profile and pictures that seem real but, in reality, are imaginary figures whose purpose is to promote certain messages. A **bot** is a software application designed to perform actions online by mimicking a normal user, that is, a kind of robot that poses as a human user. It is possible to set up a bot network, meaning a network of dozens or even thousands of fake and automatic profiles. Such bots can be programmed to create greater exposure for certain posts (or more likes, shares, and comments), thereby affecting the algorithm that promotes them on the social network and increasing exposure. As was recently reported, the defense establishment in Israel estimated that approximately 30% (!) of all discourse on social networks is the product of bots. [10]A **troll** is a user whose entire purpose is to provoke and inflame the discourse. A troll will write controversial, false or slanderous things in order to promote interest. A troll can be a real user, but also an avatar or a bot.

The defense establishment in Israel estimated that approximately 30% (!) of all discourse on social networks is the product of bots.

Terrorist organizations use bots as a component of the propaganda campaign they promote. For example, in January 2019, a bot appeared on a Telegram channel belonging to an Islamic State-supporting group that offered variety of options for users: join the group's Telegram account and join a group of activists responsible for distributing the organization's propaganda materials on social networks, such as Facebook and Twitter.

[10] Ilnai, Itay, "Invasion of the Political Bots", *Yedioth Ahronoth*, weekend supplement, January 18, 2019, pp. 22-30.

A bot allowing users to contact the owner of a Twitter account by Al-Asif Abd al-Rahman, a senior Salafi-jihadist commander in Syria

A bot allowing users to join the Islamic State's Telegram account

A bot that was published on an Islamic State-supporting Telegram account, in which supporters of the organization were offered to use the bot to join the group, which will be entrusted with the dissemination of the organization's propaganda materials on social networks

A bot of the Ebaa news agency, which belongs to Hayat Tahrir al-Sham in Syria, allowing the organization's supporters to send articles to the agency. The banner that was uploaded to Telegram read, "Be a reporter for Ebaa ... Send us exclusive news from your site"; "Share your opinions and suggestions with us".

An online attack using these means against a foreign political campaign, election campaign, referendum or political discourse has many advantages when used by a terrorist organization or supporters of terrorism. First, because it allows remote interference at relatively low cost, with complete anonymity and without the need for weapons or explosives. A computer and keyboard are sufficient. Second, because it also allows small groups, organizations and individuals to conduct effective attacks. Third, because such attacks undermine the social order, corrupt the political discourse, and undermine public confidence in the democratic system and the political system as a whole. These have always been the desire of terrorist organizations throughout terrorism's long history. On the eve of the 2019 elections, Israeli society is divided, stratified and split. It has religious, economic, social, ethnic, national and ideological conflicts. An inciting discourse could deepen divisions, widen gaps, and create polarization and radicalization. Hostile elements, including terrorist organizations and their state sponsors, are likely to use avatars, bots and trolls to harm the election campaign by deliberately defacing the public discourse. It is important to understand that the goal of terrorism has always been to undermine the regime and the stability of an enemy state. Terrorist organizations can sow and deepen divisions, and create distrust of a democratic society's government, authorities and institutions without the use of bombs, missiles or attacks.

Hostile elements, including terrorist organizations and their state sponsors, are likely to use avatars, bots and trolls to harm the election campaign by deliberately defacing the public discourse.

Knowledge Flows from Terrorism-Sponsoring Countries

As stated, terrorist organizations in the Middle East, from the Islamic State to Hamas and Hezbollah, have the knowledge required to engage in malicious interference in social networks, and some have even tested it in the past. This knowledge may even spill over to terrorist organizations from state sponsors of terrorism. For instance, both Iran and Syria are equipped with hacker units that serve the regime. In November 2018, it became known that Iran had operated a network of 98 Web sites for the dissemination of "fake news" in 28 different countries, including Israel.[11] This Iranian activity was directed mainly against countries known to have interests contrary to Iran's, such as the United States, Britain, Latin America, India, Saudi Arabia, Israel, Turkey and Yemen. Approximately 40 of the sites disseminated reports in Arabic, 22 of them in English, and the rest in dozens of different languages. The Iranian fake news sites also included accounts on social networks, Twitter, Facebook and Instagram. The accounts served as both the official accounts of the Web sites and as fake accounts posing as Web users who distributed the articles. However, Iran is not the only one involved in this: According to a follow-up conducted by Noam Rotem, there are ten bot networks operated by Saudi Arabia, Russia, the United States and Israel that currently operate on Twitter and distribute content directed at the Israeli public.[12]

In November 2018, it became known that Iran had operated a network of 98 Web sites for the dissemination of "fake news" in 28 different countries, including Israel.

Meanwhile, it was found that Facebook, Google and Twitter removed thousands of accounts originating in Iran in 2018. Facebook said in a statement that Iran had tried to promote Iranian propaganda through forged accounts, some of which were found to be linked to Iranian-owned media. Twitter also said it had deleted accounts originating in Russia and Iran that were intended to influence mid-term elections in the United States via messages against Trump and against weapons possession. Iran's goal was to promote a narrative that would be in line with its interests on Facebook, Instagram, Twitter, Google and YouTube, and to influence the internal political discourse within the United States. [13]Iran, which steadily continues to arm terrorist organizations in the Middle

[11] "Global Iranian Disinformation Operation", Clearsky LTD, November 30, 2018.
[12] Berkovitz, Uri, "Hackers Exposed: A Saudi Network of Bots Operating in Israel", *Globes*, January 22, 2019 https://www.globes.co.il/news/article.aspx?did=1001269980
[13] "Facebook deletes Iran-linked pages over effort to sow discord among US voters", *The Guardian*, October 26, 2018, https://www.theguardian.com/technology/2018/oct/26/facebook-iran-pages-deleted-fake-divisive-content-us-uk-voters

East, is likely to transfer its advanced knowledge and accumulated experience in sophisticated cyber warfare to the organizations it sponsors. The Iranians are also trying to interfere in the election campaign in Israel using bots: a report by the American company, Vocativ, which was published in January 2019, indicates that there is a growing presence of active bots operated from Iran on Israeli social networks, and that they respond automatically and in a pre-programmed manner to every development in Israel and in the election campaign. Thus, some 350 fake Iranian accounts were discovered on various social networks aimed at creating a discourse around points of contention in Israeli society. The Iranians' messages are on Facebook pages, Twitter and Telegram and are estimated to reach a potential exposure of half a million Israelis every month.[14].

How Do We Protect Ourselves?

First, we can learn from the experience of other countries to defend ourselves against digital attacks on political campaigns and political discourse. Clearly, the solution is not simple and requires a combination of various means and the development of new tools for monitoring, identifying, attributing and stopping an attack. Monitoring the online discourse in order to identify attacks is a method taken by several countries: Several countries decided to establish public and private research and monitoring bodies to work to examine dissemination on social networks, expose lies and manipulations, and report them to the public. Such bodies include the Ukrainian StopFake and the EU's European External Action Service (EEAS). Monitoring, of course, is a difficult challenge that requires sophisticated resources and tools, but even more complicated is the problem of identifying the attack and the attacker. In order to know who is responsible for an attack, several advanced technologies were proposed to identify and indicate the attacker. [15]Finally, a series of steps were

A complex array of actions and tools for monitoring, identification and defense, alongside the promotion of public awareness, requires concerted and coordinated effort, regulation and resources.

"These are the liberal memes Iran used to target Americans on Facebook", *USA TODAY*, August 24, 2018, https://www.usatoday.com/story/tech/news/2018/08/24/how-iran-targeted-u-s-facebook-youtube-and-twitter-liberal-memes/1079882002/

"Facebook, Google and Twitter remove hundreds of accounts from Russia and Iran that tried to influence US elections", *CNBC,* August 22, 2018, https://www.cnbc.com/2018/08/22/facebook-and-twitter-dismantle-disinformation-campaigns-tied-to-iran-and-russia.html

"Revealed: Iran's 'clumsy' troll army pushed one million tweets in effort to destabilize region", *The National*, October 18, 2018, https://www.thenational.ae/world/mena/revealed-iran-s-clumsy-troll-army-pushed-one-million-tweets-in-effort-to-destabilise-region-1.781713

[14] Report: "Iranian "Bot" Army Trying to Influence Israeli Elections", Ynet, January 31, 2019 https://www.ynet.co.il/articles/0,7340,L-5455832,00.html#autoplay

[15] Lazer et al., The Science of Fake News, 359 (6380) *Science* 1094 (2018)

proposed in various companies to "vaccinate" the public: namely, a public information campaign on how to identify fake information, how to avoid spreading false information, and more.[16]

A complex array of actions and tools for monitoring, identification and defense, alongside the promotion of public awareness, requires a concerted and coordinated effort, regulation, resources and more. To this end, Israel must establish a new and advanced body to monitor the Internet, protect against attacks on discourse, attack the attackers, and more. Shamir and Bahar proposed establishing a dedicated body – a monitoring unit – to monitor content on the Internet. This unit will not monitor entities or individuals identified as Israelis or engage in censorship of content on the Internet. Its purpose will be to identify attempts by entities, organizations or countries outside of Israel that seek to harm the political discourse in Israel. They propose that this body, which is part of the national cyber network, employ criteria for identifying content that is part of an attack by a foreign entity on the Israeli election campaign. When such a move is discovered, it will report it to the chairman of the Central Elections Committee and the Shin Bet. These bodies will coordinate arrangements regarding the responsibility for handling and foiling the attack. However, until such a body is set up, and considering the proximity of the elections and the immediacy of the threats, it is highly doubtful that we will be able to build digital defenses against cyber-attacks.

Considering the proximity of the elections and the immediacy of the threats, it is highly doubtful that we will be able to build digital defenses against cyber-attacks.

The success of cyber-attacks on election campaigns in many countries raises serious questions about their ability to defend themselves. There is no doubt that an array of defensive actions is needed to strengthen the ability of democracies to effectively defend themselves against such attacks. However, it is important to remember that when a liberal democracy seeks to employ protective measures, concerns arise that these measures will damage the principles of a liberal democracy, such as privacy, freedom of expression and freedom of information. Only a proper

The threat, however, does not end on Election Day: terrorist organizations and terrorism-sponsoring states certainly have a great interest in continuing to attack the political discourse, social harmony and stability of Israeli society even after the elections.

Constanze Stelzenmuller, The Impact of Russian Interference on Germany's 2017 Elections (Testimony before the U.S. Senate Select Committee on Intelligence June 28, 2017), https://tinyurl.com/ycx4fent

[16] Darrell M. West, "How to Combat Fake News and Disinformation", Brookings (December 18, 2017).

balance between considerations of national security and those of ensuring the values of democracy - will be the right solution. The threat, however, does not end on Election Day: terrorist organizations and state sponsors of terrorism certainly have a great interest in continuing to attack the political discourse, social harmony and stability of Israeli society even after the elections. Israel, which has previously learned to defend itself from most cyber-attacks, will also be forced to fight in the arena of social networks, both contemporary and in the future.

ABOUT THE ICT

Founded in 1996, the International Institute for Counter-Terrorism (ICT) is one of the leading academic institutes for counter-terrorism in the world, facilitating international cooperation in the global struggle against terrorism. ICT is an independent think tank providing expertise in terrorism, counter-terrorism, homeland security, threat vulnerability and risk assessment, intelligence analysis and national security and defense policy.

ICT is a non-profit organization located at the Interdisciplinary Center (IDC), Herzliya, Israel which relies exclusively on private donations and revenue from events, projects and programs.

ABOUT THE TERRORISM AND THE MEDIA DESK

Terrorists are increasingly making use of online and offline media tools to promote their illicit activities.

In addition, countries such as Iran and Syria support terrorist organizations through a variety of means, including communication platforms. These countries elections and develop hostile discourses targeting other countries.

Researchers:

Prof. Gabriel Weimann , Head of "Terrorism and Media Desk"

Dr. Eitan Azani Dr. Liram Stenzler-Koblentz Nava Getahun

Dr. Moran Yarchi Dr. Erga Atad Doron Rokah

Dr. Michael Barak Lorena Atiyas-Lvovsky