What Cyber Attacks Against Ukraine Can Teach Israel

by Ophir Barel **(/experts/ophir-barel)**

Sep 8, 2022
Also available in
العربية (/ar/policy-analysis/aldrws-alty-ymkn-lasrayyl-astkhlasha-mn-alhjmat-alsybranyt-ly-awkranya)

ABOUT THE AUTHORS

Ophir Barel (/experts/ophir-barel)

Ofir Barel is a researcher at Yuval Ne'eman Workshop for Science, Technology and Security, Tel Aviv University. He is also a former researcher at the Institute for National Security Studies (INSS) and at the Center for Political Research at the Israeli Ministry of Foreign Affairs. Barel is a contributor to Fikra Forum.

Brief Analysis

Israel must look to the war in Ukraine for insight into potential cyber attacks and security strategies ahead of the November legislative elections.

The upcoming election for the 25th Knesset in Israel is being treated with indifference and cynicism among the local electorate: the prevailing mindset in the country is that what has not been achieved in the four election campaigns held since 2019—a political decision—will not be achieved on November 1 either. Current polls **(https://www.jpost.com/israel-news/article-715640)** show that this general assessment may be correct.

However, new elections also provide new opportunities for threats in the fields of cyber warfare and influence operations. While such tactics have appeared elsewhere before, they have yet to make a significant impact in Israel, one possible reason being the low rates of social media use among Ultra-Orthodox Jews in addition to language barriers. Nevertheless, an uptick in cyberattacks against Ukraine this year demonstrates the direction in which cyber warfare is headed and suggests the devastating impact that these attacks could have on Israel—either during this election cycle or in future cases—if the threats are not adequately addressed.

Since February 2022, Russia has launched **(https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2022)733549)** a barrage of cyber attacks and influence operations against the West and Ukraine, demonstrating a surge in their already-robust framework of cyber operations. Drawing from Russia's strategies, there are three major tactics that anti-Israeli elements could implement in order to intervene in the 2022 legislative elections.

The first means is the use of deepfake media clips. These are bogus videos and images (and more rarely texts) created through the use of AI based technology. In a political or military context, the main concern is that malicious actors will spread deepfake videos that could manipulate public opinion, such as leaders making statements they did not actually make.

In mid-March, it was reported **(https://techcrunch.com/2022/03/16/facebook-zelensky-deepfake/)** that pro-Russian entities circulated a deepfake video in which Ukrainian President Volodymyr Zelensky was seen calling on his citizens to surrender. Three months later **(https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko)** , during a video call between the heads of European capital cities, a man introduced himself as the mayor of Kyiv, Vitaly Klitschko. Soon after, it became known that this man was actually an impostor who managed to disguise himself as Klitschko using AI.

Though deepfakes are not new, the increasing accessibility of the technological and economic elements necessary to convincingly produce them has greatly expanded their scope. Between 2018 and 2020 the number of deepfake videos distributed on the Internet grew exponentially, doubling **(https://sensity.ai/blog/deepfake-detection/how-to-detect-a-deepfake/)** approximately every six months. However, the March incident with Zelensky constituted a precedent: it is the first known case **(https://www.inss.org.il/he/wp-content/uploads/sites/2/2022/02/%D7%9E%D7%96%D7%9B%D7%A8-220-%D7%93%D7%99%D7%A4-%D7%A4%D7%99%D7%99%D7%A7-%D7%95%D7%90%D7%AA%D7%92%D7%A8%D7%99%D7%9D-%D7%9C%D7%91%D7%99%D7%98%D7%97%D7%95%D7%9F-%D7%94%D7%9C%D7%90%D7%95%D7%9E%D7%99.pdf)** in which a certain country, or parties acting on its behalf, used deepfakes for gaining political or military influence in another country.

This precedent could encourage anti-Israeli actors to sabotage the proper course of the elections through the distribution of deepfake videos. It is true that these actors lack the ability to produce deepfakes of the same quality, and the videos would not likely mislead many voters, but still the use of deepfakes in any case could erode the public's confidence. The large amount of media attention that a deepfake can be expected to receive—as occurred in the two cases described above—may emphasize to some in the Israeli electorate the weaknesses of the domestic government, which has no solutions to such cyber threats. This erosion of trust is one of the distinct goals **(https://theconversation.com/why-public-trust-in-elections-is-being-undermined-by-global-disinformation-campaigns-181825)** of disinformation disseminators. Considering the growing divisiveness and repeated election cycles since 2019, such a goal will be easier to achieve in Israel as trust in government institutions is already declining.

The second tactic is a large-scale increase in bot usage in order to spread false information. Like deepfakes, the use of bots as a means of political influence is not new. Global research findings from recent years have demonstrated how bots are a significant manipulative weapon, both in terms of the amount of messages they spread and in terms of their ability to influence the political discourse. In April 2018, the PEW Research Center published a study **(https://www.pewresearch.org/fact-tank/2018/04/09/5-things-to-know-about-bots-on-twitter/)** that examined approximately 380,000 tweets which included links to sites focused on news and current events published over a period of six weeks. PEW found that bots had actually published a striking two-thirds of the tweets sampled. A study released a month later **(https://www.nber.org/system/files/working_papers/w24631/w24631.pdf)** by the National Bureau of Economic Research examined this phenomenon in the context of elections: during the 2016 U.S. presidential election and the UK referendum on EU membership, bots contributed significantly to the formation of echo chambers—virtual spaces used to amplify false messages—and increased the distribution of divisive rhetoric.

Moreover, the war in Ukraine has only provoked further innovation on the bot front, especially in terms of Russia's unbelievably large-scale bot farms. Between March **(https://www.zdnet.com/article/ukraine-takes-out-five-bot-farms-spreading-panic-among-citizens/#ftag=RSSbaffb68)** and August **(https://bit.ly/3BRicFD)** , Ukraine shut down six bot farms containing a total of 1.1 million bots—roughly 183,000 bots in each farm. To illustrate the gravity of the threat, this number is 22 times higher than the number of Russian bots thought to be active on Twitter during the U.S. elections (about 50,000 **(https://techcrunch.com/2018/01/19/twitter-updates-total-of-russia-linked-election-bots-to-50000/)**) just five years ago.

Of course, the Israeli political arena has already been introduced to the involvement of bots on a large scale: in mid-August, the Israeli media reported that the General Security Service (Shin Bet) removed 140,000 Iranian bots **(https://www.unitedagainstnucleariran.com/proxies-partners/shin-bet-reportedly-fears-russian-iranian-interference-upcoming-israeli-election)** attempting to influence the March 2021 elections. Apparently, The Shin Bet and the National Cyber Directorate (NCD) had the resources and abilities to uncover and shutdown the potentially massive bot networks. Nevertheless, using even more bots will multiply the burden on the Israeli authorities, and more bots will be able to slip under the radar, spreading subversive and controversial messages and thus further undermining an Israeli society that is already more divided and conflicted than ever. This is especially true in the case of using AI

bots, which are considered (https://www.nature.com/articles/d41586-020-03034-5) more sophisticated and harder to track.

The third means of cyber warfare that can be adopted from Russia's recent strategy is hacking into various media outlets in order to spread disinformation. On July 12, the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) published a report (https://www.infosecurity-magazine.com/news/ukraine-cyber-agency-cyber-attack/) noting that the number of cyber incidents with malicious codes during the second quarter of 2022 had increased by 38% compared to the first quarter of 2022. According to the report, the sectors that experienced the highest number of attacks by Russian hackers during this period were mass media networks and national and local government authorities. The attacks included disruption of media broadcasts—as was done in an attack in July (https://therecord.media/ukrainian-radio-broadcaster-hacked-to-spread-fake-news-about-zelenskys-health/) in which false information about Zelensky's health condition was published—and defacement attacks (https://www.mandiant.com/resources/blog/information-operations-surrounding-ukraine) , during which Russian hackers planted false messages to harm public morale, arouse divisions, and strengthen support in Russia.

It's important to note that cyber attacks of the above type have so far constituted only a small part of the Iranian cyber war against Israel. In fact, the overall balance of power between Israel and Iran in cyberspace does not yet clearly favor one side or the other. In cyber operations, Israel is better prepared (https://www.iiss.org/blogs/research-paper/2021/06/cyber-capabilities-national-power) for cyber threats and has superior offensive capacities, but on the other hand, Iranian information operations—despite being managed carelessly—have (https://time.com/6071615/iran-disinformation-united-states/) become more complex and better funded in recent years, (https://eeradicalization.com/wp-content/uploads/2022/08/The-Iranian-Information-Revolution-Report.pdf) ensuring the continuation of the threats even after their deplatforming.

In regards to the distruption of media platforms, the most recent Israeli case occurred in January 2022, when Iranian hackers attacked (https://www.haaretz.com/israel-news/2022-01-03/ty-article/jerusalem-post-maariv-hacked-on-anniversary-of-soleimani-assasination/0000017f-f663-d887-a7ff-fee7876e0000) the website of the Jerusalem Post and the Twitter account of Maariv newspaper on the anniversary of the assassination of Qassem Soleimani, though Iran denied its involvement. Further proving their cyber competence, Iran intervened in the dialogue surrounding the 2020 U.S. elections, sending email messages to voters in several states on behalf of the American far-right group "The Proud Boys" with threats to not vote for President Trump. The ability of the hackers to obtain these email addresses and personal information indicates that the Iranians are increasingly able to combine their offensive cyber capabilities with psychological warfare tactics in order to influence public opinion for political needs. In the foreseeable future, Iran may carry out more of these attacks against Israel.

While the use of cyber warfare in the war in Ukraine certainly presents new threats to the elections in Israel, an examination of the Ukrainian response can also suggest effective solutions. Among the multitude of cyber security and information warfare actions implemented by Ukraine and the Western countries since the outbreak of the war, two are worth noting:

The first solution is the deepening of international cooperation, which Israel is already working towards. Since 2019, Israel has taken steps to protect its elections from foreign interference —for example, establishing a dedicated team (https://www.inss.org.il/wp-content/uploads/2019/07/Cyber3.1ENG_3-29-42.pdf) led by the NCD. However, some intelligence experts in Israel have recommended (https://www.intelligence-research.org.il/userfiles/banners/%D7%94%D7%9E%D7%95%D7%93%D7%99%D7%A2%D7%99%D7%9F%20%D7%95%D7%94%D7%A9%D7%A4%D7%A2%D7%94%20%D7%96%I launching international corporations to protect the national elections. Regarding the war in Ukraine, it seems that this cooperation can be of a great value. In a hearing held in April in the House of Representatives, the commander of the American Cyber Command, Paul Nakasone, claimed (https://www.fedscoop.com/ukraine-crisis-demonstrates-cyber-concept-of-persistent-engagement/) that Ukraine has dealt with Russian cyber attacks better than expected due in part to western assistance in cyber security. Israel can benefit from this type of international cooperation, for example, by receiving intelligence on potential threats or disabling infrastructure used to carry out cyber attacks and influence operations.

Even so, the nature of the internet suggests that at least a few attacks will still break through even the most robust cyber security systems. As such, Israel must strengthen the digital literacy of its citizens. Here too, the war in Ukraine provides a model for a successful solution: the International Research and Exchanges Board (IREX) has been running a digital literacy education program in Ukraine since 2015, called Learn to Discern (L2D) (https://www.npr.org/2019/03/22/705809811/students-in-ukraine-learn-how-to-spot-fake-stories-propaganda-and-hate-speech) . In May, it released a survey (https://www.irex.org/success-story/irex-information-literacy-l2d-methodology-proving-vital-during-war-ukraine) conducted among Ukrainian middle school and high school teachers who were trained by IREX which revealed that 90% of the teachers used the knowledge they gained to help friends, family members, and colleagues better navigate the virtual information environment. Formerly (https://www.irex.org/sites/default/files/node/resource/evaluation-learn-to-discern-in-schools-ukraine.pdf) , it was found that the contents of the program helped students improve their digital literacy skills, with 18 percent improvement in ability to identify fake posts. Even if the time remaining until Election Day is too short for the full implementation of such a program, it is imperative to start enhancing digital literacy as soon as possible in order to reduce the gap in the Israeli public's digital literacy skills and prepare them to encounter cyber attacks and influence operations. ❖

RECOMMENDED

IN-DEPTH REPORTS

U.S. Counterterrorism Reimagined:

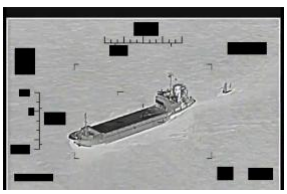
Tracking the Biden Administration's Effort to Reform How America Addresses Violent Extremism

Sep 7, 2022

◆

Matthew Levitt

(/policy-analysis/us-counterterrorism-reimagined-tracking-biden-administrations-effort-reform-how)



BRIEF ANALYSIS

Iranian Seizures Raise Questions About Unmanned Maritime Operations

Sep 7, 2022

◆

Farzin Nadimi

(/policy-analysis/iranian-seizures-raise-questions-about-unmanned-maritime-operations)

ARTICLES & TESTIMONY

No, Israel Isn't Falling Into China's Orbit

Sep 6, 2022

◆

Assaf Orion

(/policy-analysis/no-israel-isnt-falling-chinas-orbit)

TOPICS

Democracy & Reform (/policy-analysis/democracy-reform)

Military & Security (/policy-analysis/military-security)

REGIONS & COUNTRIES

Israel (/policy-analysis/israel)