What Cyber Attacks Against Ukraine Can Teach Israel

by Ophir Barel (/experts/ophir-barel)

Sep 8, 2022
Also available in
israeli ([/policy-analysis/address-uty-ymin-liees-ylimsha-mn-albjmat-alybeart-ty-anekranya)]

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-715460](https://www.jpost.com/israel-news/article-715460)) 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](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 hocus 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/](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](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 deep fake videos distributed on the Internet grew exponentially. Two months after the March incident with Zelensky, the same actor tried another tack, a video showing Kyiv mayor Vitali Klitschko in a meeting with his colleagues, 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](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 in Israel than governments in other countries.

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/](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](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 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](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 actually published a striking two-thirds of the tweets sampled.

Threats are being undermined by global disinformation campaigns. The fact 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](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 in Israel than governments in other countries.

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/](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](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 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](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 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](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 actually published a striking two-thirds of the tweets sampled.

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-pandemic-cyberattacks-russia-affiliated/](https://www.zdnet.com/article/ukraine-takes-out-five-bot-farms-spreading-pandemic-cyberattacks-russia-affiliated/)) and August ([https://bitt.ly/3Br1CFD](https://bitt.ly/3Br1CFD)), Ukraine shut down six bot farms containing a total of 1.3 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://www.jpost.com/israel-news/world-news/4000)) just five years ago.

Of course, the Israeli political arena has already been involved in the manipulation 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-elections](https://www.unitedagainstnucleariran.com/proxies-partners/shin-bet-reportedly-fears-russian-iranian-interference-upcoming-israeli-elections)) 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/d41586-020-03014-5) 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), in which hacking attacks disrupted media platforms.

It’s important to note that cyber attacks of the above type have so far only constituted one 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.fedscoop.com/ukraine-crisis-demonstrates-cyber-concept-of-persistent-engagement/) 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://zerocalization.com/wp-content/uploads/2022/08/The-Iranian-Information-Revolution-Report.pdf) It is expected that cyber threats from Iran will become more sophisticated and harder to track.

In regards to the disruption of media platforms, the most recent Israeli case occurred in January 2022, when Iranian hackers attacked (https://www.haaretz.com/islam-news-2022-01-09/iranian-hackers-attack_1.6806994) 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 vote for President Trump. In response, Ukrainian authorities have obtained email addresses and personal information that indicates 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.

Chinese hackers—called the Red Hacker Group—have used a method similar to the one used by Iranian hackers to attack the website of an Israeli newspaper during the war in Ukraine.

In regards to the threats of cyber warfare, it is important to note that while the United States and Israel are working on solutions, they still need to improve their cyber capabilities if they want to reduce the gap with the advanced cyber capabilities of Iran. The United States and Israel need to work together to improve their cyber capabilities and create a strong defense against cyber threats. It is also important to note that the use of cyber warfare in the war in Ukraine certainly presents new threats to the elections in Israel, as well as to the elections of other countries. However, 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. The Ukrainian government has taken steps to protect its elections from foreign interference by using international cooperation and information warfare actions implemented by Ukraine and the Western countries since the outbreak of the war, and it is important to take these steps to improve the protection of elections from cyber threats.
No, Israel Isn't Falling Into China's Orbit

Sep 6, 2022

Assaf Orion

/no/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)