BESA
The Begin-Sadat Center
for Strategic Studies
Bar-Ilan University
PERSPECTIVES
THE BEGIN-SADAT CENTER FOR STRATEGIC STUDIES

The BDS Campaign Against Israel "De-Localizes" the Palestinian Cause, Focuses on Global Surveillance

By Irina Tsukerman

BESA Center Perspectives Paper No. 2,202, June 19, 2023

EXECUTIVE SUMMARY: BDS supporters have shifted to a new strategy, a "de-localizing" of the Palestinian cause via attacks on Israel's cybersecurity industry. Their aim is to universalize an image of Israel as a facilitator of global rights abuses. This approach does not require adherents to support the Palestinian cause to gain momentum. In the face of regional geopolitical turmoil, Israel should develop an offensive disruptive response to undo the reputational damage caused by this aggressive form of information warfare.

BDS supporters are creating a new blood libel by universalizing Israel's role as the alleged root of human rights abuses around the world, not only for Palestinians. To reach this goal, they are targeting the very foundation of the Abraham Accords: Israel's famed cybersecurity industry.

On the strength of commercial spyware, Jerusalem has been able to translate security relationships into diplomatic breakthroughs as its more trusted partners were able to address some of their most significant threats coming from terrorist groups, revolutionary opposition, ideological extremists, and organized crime. The media scandal surrounding the now infamous Pegasus software allegedly used by a number of allies and ally-adjacent countries is just one example of how the BDS movement has succeeded in associating Israel with alleged human rights abuses.

A concerted lobbying campaign coupled with prolonged media scandals formed by a conglomerate of leftist publications frequently linked to Qatar, Muslim Brotherhood associates, and Arab Spring sympathizers resulted in the Biden administration's blacklisting of the developer of Pegasus, the NSO Group, and several other Israeli cybersecurity companies. The politicized human rights organizations behind this campaign – Canada-based Citizen Lab, Amnesty International, ACCESS NOW, and Front Line Defenders – have never provided evidence of a Pegasus presence for independent verification. These organizations were criticized by several technical experts for their failure to abide by the scientific method and to meet academic standards of transparency, verifiability, and independent peer review. Their response was to dismiss, ignore, or outright smear the experts who took issue with their reports.

While the methods and motivations of these organizations are a separate topic, their impact on Israel has been substantial. NSO Group has significantly curtailed its outreach to various countries, which has undermined Israel's diplomatic efforts and the expansion of the Abraham Accords.

Former Defense Minister Benny Gantz banned Israel from open exportation of any commercial spyware to Saudi Arabia and UAE, among other countries. More recently, a cybersecurity deal with Morocco was dropped by Israel, which looks damaging regardless of the reason due to the level of attacks on Rabat by Amnesty. India is reportedly on the hunt for alternatives to Pegasus after negative publicity drew attention to its own security concerns, threatening its blossoming defense relationship with Israel.

The loss of clients or potential clients does not stop with Pegasus. A different Israeli software company, Predator, has also become a source of contention. Another close and growing ally, Greece, ultimately voted to ban all commercial spyware, which could ruin important security arrangements with Israel.

The US is being pushed to ban all commercial spyware. If it complies, this will lead to the proliferation of unregulated black-market spyware, ruin Israel's cybersecurity industry, and prompt a rise in human rights abuses. This state of affairs would play to the advantage of hostile regimes, such as Russia, China, Iran, and North Korea.

BDS Propaganda Machine Openly Publicizes Its New Strategy

Israel's business and security relations are under attack, and BDS efforts are succeeding at getting allies like the US to shut down Israeli companies without

transparent investigation or fair examination of evidence and without giving Israel a chance to confront its accusers. A new, sinister phase to this international campaign is now underway, implemented by colluding anti-Israel interests.

The first public acknowledgment of the new strategy can be found in an article allegedly written by a Moroccan opposition couple. While the pair has supported Hezbollah and Iran in the past, the article bears hallmarks of planning by an intelligence agency. It discusses the socioeconomic and political situation in Morocco since the Arab Spring and blames the deepening cybersecurity relations between the "Makhzen" (the royal system) and Israel for propping up corruption, eliminating dissent, building up a police state, and stifling opposition and critics by spying on them abroad.

The article extrapolates this activity on an international level, then delves into conspiracy theories by claiming that Morocco, France, and Israel have created a network of assets who are used to attack the opposition. The article outlines the exact steps BDS supporters are taking to smear and delegitimize Israel.

Within a few days of the piece's publication, DAWN MENA, a project planned by Jamal Khashoggi and implemented by his associates and acolytes after his death, published a similar piece using nearly identical language and attacking Israel for the exportation around the globe of cybertechnologies allegedly used to spy on Palestinians. DAWN MENA is staffed by and linked to Al Jazeera reporters, Muslim Brotherhood associates (such as Dr. Dalia Fahmy), the son of the Saudi hate preacher Salman Al Oudeh, Abdullah Alaoudh, as well as Qatari, Algerian, and Armenian lobbyists and propagandists, including Doha-based Marc Owen Jones and Sarah Leah Whitson. The DAWN MENA piece parroted the language of the attacks on Israel's cybersecurity sphere, using its relationship with the US State Department to advance its political agenda in blaming Israel's Pegasus for Khashoggi's death, and also supported lawsuits that sought to expose the alleged use of Israeli cyberweapons to surveil members of the Saudi opposition and former Al Jazeera reporters. These unsubstantiated attacks on Israel ignore the vastly intrusive, systematic, and widespread Chinese surveillance technology that is being integrated en masse in Iran and Saudi Arabia, as well as other hostile intelligence cyber techniques.

No longer focusing exclusively on the Palestinians, this anti-Israel nexus is now focused on tainting Israel's cybersecurity industry in the eyes of the world as a weapon that supports corrupt regimes against peaceful civilians. These attacks deliberately ignore legitimate threats posed by supposedly peaceful dissidents and journalists who often double as political operatives, spies, and ideological

extremists. Thus, the effect is not only the besmirching of Israel's cybersecurity programs but a tarnishing of associations with Israel. The new Arab Spring is not based on direct confrontation between opposition groups and governments; rather, the aim is to attack and expose the adversary and the intermediary and create a non-state-based global movement against Israel.

This form of hybrid warfare against Israel is reaching new pinnacles of success. No longer constrained to academia, it now successfully uses political lobbying, the front pages of the news, international human rights NGOs, the education system, big tech companies competing with their Israeli rivals, the information security community, lawfare, and entire activist communities funded by state actors and affiliated movements designed for the sole purpose of attacking Israeli cyber institutions, assorted libertarians, and anyone who has a tendency not to question highly technical jargon on a scale that was unfathomable even ten years ago.

The political strategy of blacklisting companies like the NSO Group and Candiru is complemented by a series of international lawsuits against Israeli companies that bring together human rights organizations, social media companies, and private individuals. Columbia University has an entire department dedicated to turning lawfare into a form of political activism specifically against Pegasus. Their methods were candidly revealed in a Knights Institute panel with Salvadoran activist journalist Carlos Dada, who heads opposition party-backed publication *El Faro*. The object is to complement analogous lawsuits by activists in the US, Thailand, UK, and EU. Lawfare aims to have a chilling effect on potential clients, generate negative publicity, exhaust financial resources, and abuse the discovery process in the service of reputational damage.

The BDS movement's new method of attacking Israel is far more dangerous than its earlier tactics because it can easily draw in sympathizers around the globe and does not need to focus on Palestinians to achieve that goal. The shadow of the surveillance state and the abuse of power by corrupt governments are concepts familiar to people everywhere. To have Israel tied by association to the facilitation of alleged global human rights abuses is the newest, most successful iteration of the blood libel.

The rapprochement of the Arab world with Iran has deprived Israel of valuable allies. States that are now working with Iran, Qatar, and their intelligence facilitators, Russia and China, have significantly less incentive to share intelligence, join forces to uncover the organizers of this campaign, and fight back.

The BDS campaign is now shifting away from targeted scandals embarrassing to state actors, as the movement's goals in those states have largely been achieved. The next stage is to focus the bulk of the blame on Israel for allegedly making these "crimes" possible. Now that these countries are no longer being ostracized by the shadow of Pegasus and other software, Israel alone remains the culprit. All efforts will be used to isolate it from the international community on the basis of the allegedly antidemocratic nature of its commercial surveillance industry.

Israel should treat these attacks as information warfare, no less of a threat than kinetic operations in the field. The collusion of interests that are able to wage multi-year targeted campaigns is a potent threat. These interests have sufficient motivation, resources, and dedication to do significant and potentially irreversible damage.

State and non-state actors seeking to undermine Israel have chosen non-lethal methods of operations to achieve deadly goals, building up impact over time. To win the long game, Israel should mirror the methods used by the adversary and move from defensive to offensive measures. These should include political pressure on state actors to provide support, recruit skilled assets, uncover and reveal the interests and agendas behind these campaigns, and disrupt their operations with the help of security and intelligence agencies, law enforcement cooperation, friendly media, NGOs, think tanks, and industry allies.

This also means filing lawsuits for defamation, challenging participating parties on the paucity of legitimate evidence, and demanding independent review of the reports. Israel should question and challenge experts allegedly used in anti-Israel reporting and fight for a seat in parliamentary and congressional hearings to ensure fairness. Teams of experts have raised the alarm over the emerging threat. Now that the threat is overt, Israel should utilize these experts to advance its interests.

Irina Tsukerman is a New York-based national security and human rights lawyer, geopolitical analyst, and information warfare specialist. She is President of Scarab Rising, Inc., a media and security strategic advisory.