Gulf Cyber Cooperation with Israel: Balancing Threats and Rights

by Neri Zilber **(/experts/neri-zilber)**

Jan 17, 2019
Also available in
العربية (/ar/policy-analysis/altawn-alsybrany-byn-dwl-alkhlyj-wasrayyl-almwaznt-byn-althdydat-walhqwq)

ABOUT THE AUTHORS

Neri Zilber (/experts/neri-zilber)
Neri Zilber, a journalist and analyst on Middle East politics and culture, is an adjunct fellow of The Washington Institute.

Brief Analysis

The provision of powerful cyber tools is important for national security in the Gulf states, but it has reportedly opened the door to human rights abuses.

The following is a corrected version of the original PolicyWatch.

In recent years, Iranian adventurism and other regional developments have produced a historic convergence of interests between Israel and the Gulf Arab states, with top Israeli officials making periodic visits there, intelligence cooperation becoming a regular occurrence, and cultural and economic ties slowly coming out into the open. Yet it is arguably in the cyber realm that these ties have been scrutinized most heavily. According to publicly available accounts, Arab governments have used Israeli technology to defend against cyberattacks and hunt down terrorists, but also to target internal critics—potentially including murdered Saudi journalist Jamal Khashoggi.

SHARED THREATS AND INTERESTS

The thawing of relations with the Gulf states began in the 1990s following the Oslo Accords and the nascent Israeli-Palestinian peace process. Most prominently, Prime Minister Yitzhak Rabin visited Oman in 1994, and Israel opened a trade office in Qatar two years later. Meanwhile, during negotiations over U.S. F-16 sales to the United Arab Emirates during this period, the Emirati government did not object to the presence of Israeli technology in the jets. As one U.S. official told the *New Yorker* last June, "The Emiratis wanted everything the Israelis had."

Over the past decade, growing military threats from Iran, its proxies, and Sunni jihadist groups like the Islamic State pushed Israel and the Gulf states into even closer security cooperation. This need first came to the fore in 2007, when the UAE approached the Israeli-owned, U.S.-based firm 4D Security Solutions to upgrade defenses around sensitive energy installations and establish a citywide "smart" surveillance system in Abu Dhabi. According to multiple media reports, AGT International—a separate Swiss company belonging to 4D owner Mati Kochavi—won the

reported $6 billion contract, with its Israel-based subsidiary Logic Industries providing the real technical expertise.

The resulting system, often called "Falcon Eye," is believed to have been completed by 2016. It comprises a network of cameras, sensors, and artificial intelligence platforms that provide everything from traffic control to intimate surveillance data. In 2014, elements of the system were reportedly harnessed to apprehend a female jihadist after a knife attack against an American schoolteacher.

The same consortium of Israeli-owned companies was later permitted to bid on a project intended to help manage pilgrim inflows to Mecca. Although the bid was unsuccessful, Bloomberg reported that Saudi authorities ultimately implemented an electronic system similar to the one proposed.

Riyadh has also sought Israeli assistance in addressing other cyber needs. In 2012, a major operation against Saudi Aramco wiped out three-quarters of the state-owned energy giant's computers (some 30,000 workstations), an incident described at the time as the largest commercial cyberattack in history. U.S. intelligence officials believe that the perpetrators of this Shamoon virus attack were sponsored by the Iranian government. Years later, Israeli high-tech entrepreneur and former lawmaker Erel Margalit told Calcalist that cybersecurity firms from his country had been brought in to help Saudi Aramco repair the damage, a task that took months.

In 2015, Riyadh approached the Israeli firm IntuView for help in tracking jihadists on social media. According to Bloomberg, the company fulfilled the request with software that could sift through 4 million Facebook and Twitter posts per day. Like many Israeli firms doing business in the Gulf, it established a cutout company in Europe to give the Saudis some deniability. IntuView's work with the Saudis later expanded to include monitoring public opinions about the royal family. According to *Haaretz*, Bahrain acquired a similar social media monitoring system from Verint, an Israeli-founded industry leader, sometime after 2011.

FROM DEFENSE TO OFFENSE

There is often a precarious line between defense and offense in the cyber realm. Defensive cyber actions may require aggressive operations against potential threats to provide early warning, determine attribution, and bolster deterrence. Yet this also creates the kind of capabilities that hold the potential for abuse, including surveillance and repression of anyone deemed by the powers-that-be to be an enemy of the state.

Indeed, pressing needs related to infrastructure protection, public safety, and jihadist surveillance in the Gulf states begat increasingly sophisticated intelligence gathering and information influence operations against prominent dissidents, as the *Washington Post* reported last December. One Israeli firm in particular **has been implicated (https://www.washingtoninstitute.org/policy-analysis/view/the-rise-of-the-cyber-mercenaries)** in these campaigns: the NSO Group, whose Pegasus spyware can remotely hack into smartphones to track movements, monitor messages, and take control of cameras and microphones.

According to the *New York Times*, the UAE began a relationship with NSO as early as 2013, eventually asking the firm for help intercepting communications by senior Qatari officials, a Saudi prince, and Lebanon's prime minister. In 2016, Pegasus was allegedly used to target Emirati dissident Ahmed Mansoor; over the next two years, the University of Toronto's Citizen Lab found suspected Pegasus infections in forty-five countries, including Algeria, Bahrain, Iraq, the Palestinian territories, and Saudi Arabia.

Among the individuals targeted in such incidents were two employees of Amnesty International, one based in Saudi Arabia. Another target was Omar Abdulaziz, a high-profile Saudi dissident living in Canada. Citizen Lab released the latter allegation on October 1, 2018, one day before Khashoggi was murdered in Saudi Arabia's Istanbul consulate. Abdulaziz had been in contact with Khashoggi; in a lawsuit filed in Tel Aviv, he alleged that information Saudi authorities obtained via Pegasus "contributed in a significant manner" to their decision to murder the journalist.

According to the *Washington Post*, several Western intelligence officials have confirmed that the sale of NSO software to Riyadh did in fact take place, via Luxembourg-based affiliate Q Cyber Technologies. Although no direct link between these tools and Khashoggi has been publicly verified, a recent *Haaretz* report asserted that NSO representatives met with two senior Saudi intelligence officials several times in 2017. The goal of the meetings, which took place in multiple European cities, was the sale of an advanced version of Pegasus, allegedly for $55 million. Notably, Saudi Crown Prince Muhammad bin Salman launched an extensive crackdown against internal opponents later that year. The *Wall Street Journal* subsequently reported that the Pegasus deal was brokered by two close aides to the crown prince who have been implicated in Khashoggi's murder, one of whom traveled to Israel.

HUMAN RIGHTS VS. REALPOLITIK

Although NSO has not publicly confirmed its client list, it has stated that it does not operate Pegasus for its customers. The firm also noted that it follows all relevant Israeli laws concerning the export of weapons—which cover offensive cyber tools like spyware and potential dual-use systems—as mandated by a regulatory body that sits inside the Defense Ministry. In other words, NSO would have had to receive permission from the Israeli government, likely up to the highest echelons, in order to sell such systems to an Arab state. In a recent interview with *Yediot Aharonot*, the company's CEO denied that Khashoggi had been targeted "by any NSO product or technology," though he did not expressly deny that Riyadh had been a client.

Cybersecurity is a major business for Israel, which receives an estimated 20 percent of all global investment in the sector and exports nearly $4 billion in related products and services. Some of that activity—whether directly or through European subsidiaries—has gone toward helping Gulf Arab governments handle highly sensitive security challenges. In addition, Israeli firms are reportedly eager to invest in Saudi Arabia's futuristic tech city NEOM.

Yet the capabilities involved in some of these transactions have also apparently been used to abet internal crackdowns on dissent, complicating Israel's clear diplomatic, economic, and military interest in normalizing relations with Arab states. As Netanyahu stated last month when tangentially addressing the Khashoggi crisis, "We always have tension between the most basic human rights, the right to life and the right of a free press, but on the other side there is also realpolitik. And I don't deny it. There's always a balance."

Striking the right balance is imperative, particularly for Israel's global reputation. Likewise, Arab governments face a glaring media spotlight whenever news surfaces of such relations. As one senior Saudi official told the *Wall Street Journal* in December, outreach to Israel "definitely cooled off right after Khashoggi's murder." Going forward, Israeli and Gulf leaders will need to tread carefully in order to shield their historic and burgeoning ties from such crises.

Neri Zilber is an adjunct fellow with The Washington Institute. ❖

ARTICLES & TESTIMONY

How to Make Russia Pay in Ukraine: Study Syria

Feb 15, 2022

◆

Anna Borshchevskaya

(/policy-analysis/how-make-russia-pay-ukraine-study-syria)

BRIEF ANALYSIS

Bennett's Bahrain Visit Further Invigorates Israel-Gulf Diplomacy

Feb 14, 2022

◆

Simon Henderson

(/policy-analysis/bennetts-bahrain-visit-further-invigorates-israel-gulf-diplomacy)

BRIEF ANALYSIS

Libya's Renewed Legitimacy Crisis

Feb 14, 2022

◆

Ben Fishman

(/policy-analysis/libyas-renewed-legitimacy-crisis)

TOPICS

Arab-Israeli Relations (/policy-analysis/arab-israeli-relations)

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

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

Terrorism (/policy-analysis/terrorism)

REGIONS & COUNTRIES

Israel (/policy-analysis/israel)

Gulf States (/policy-analysis/gulf-states)