INSIGHTS

No. 266 | 14 September 2021

One Year On

Israel's Cybersecurity Cooperation with the GCC States

Nima Khorrami

NUS National University of Singapore | Middle East Institute Singapore

Series Introduction

The Abraham Accords: One Year On

The signing of the "Abraham Accords" between the UAE and Israel in August 2020, which sparked off the normalisation process between Israel and several other Arab states, was a culmination of the indirect or clandestine relations that Israel has had with some of the Gulf countries for about three decades.

Apart from examining the factors that contributed to the normalisation process, this series of *Insights* is aimed at taking stock of the Abraham Accords by looking at the shifts that have taken place in relations between Israel and the GCC states one year since the signing. The papers in the series will also look at the implications of the growing relationship and its possible trajectories, particularly considering the constraints on the part of the Gulf states in dealing with Israel and the evolving geopolitical context.

Cover photo: (L–R). Foreign Affairs Minister of Bahrain Abdullatif bin Rashid Al Zayani, then Prime Minister of Israel Benjamin Netanyahu, then US President Donald Trump signing the Abraham Accords at the White House on 15 September 2020. Alex Wong/Getty Images via AFP.

One Year On
Israel's Cybersecurity Cooperation with the GCC States

Nima Khorrami[1]

This article delves into the evolving cooperation in cyberspace between Israel and some of the GCC states. It highlights the commercial, psychological and strategic factors that drive Israel's willingness to cooperate with the GCC states in the cyber domain and examines the implications of this growing cooperation. It concludes by warning that unchecked cybersecurity cooperation between Israel and the GCC states could destabilise both the regional and global cyber domains.

Even before the signing of the "Abraham Accords" in August 2020, Israel was widely known to have had various interactions with some of the GCC countries, including cybersecurity cooperation. Saudi Arabia, which has yet to normalise relations with Israel, was one of those countries. The willingness on the part of the Israelis to engage in cybersecurity cooperation with the GCC countries is driven by a combination of political, strategic and commercial interests. But in exporting cybersecurity technologies to these countries, Israel may have indirectly contributed to the proliferation of cyber malware, which could erode regional security by increasing the prospect of state-sponsored cyberattacks on critical infrastructure. Israel also has lent itself to criticism that such technologies enhance the efforts of authoritarian

[1] The views and opinions expressed are those of the author and do not necessarily reflect the official policy or position of the OSCE Academy or the Arctic Institute. Neither do they reflect the official policy or position of the Middle East Institute, NUS.

regimes in the region to spy on political foes and to quell dissent. As cyberspace gains geopolitical prominence and Israel-GCC relations enter a new phase, the time is ripe to examine the drivers behind Israel's cyber cooperation with the GCC states and how its exports of cyber technologies will affect both regional security and domestic politics in the sheikhdoms of the Gulf.

Increasing Cybersecurity Cooperation

Lacking natural resources and surrounded by unfriendly states, Israel has had to rely on innovation and technological development since its birth as a nation state. Indeed, with its national security tightly linked to its ability to innovate, Israel's emergence as one of the most technologically advanced nations in the world ought not to be surprising. Israel is regarded as one of the market leaders in cyberweapons today.[2]

Amid increasing competition in the cybersecurity market, the Israeli government was reported to have eased some of its restrictions on the sale of cyberweapons to foreign entities in 2018 in the interest of maintaining the country's commercial advantage. Israeli companies exporting cybersecurity technologies were to be allowed exemptions from having to obtain marketing licences under "certain conditions related to the security clearance of the product and assessment of the

[2] Business Wire, "Global Military Cyber Weapons Market and Technologies Forecast Report 2021–2027", *Business Wire*, 9 July 2021, https://www.businesswire.com/news/home/20210709005126/en/Global-Military-Cyber-Weapons-Market-and-Technologies-Forecast-Report-2021-2027---ResearchAndMarkets.com; Ahmed El-Masry, "The Abraham Accords and their Cyber Implications: How Iran is unifying the region's cyberspace*",* Middle East Institute, (Washington, DC), 9 June 2021, https://www.mei.edu/publications/abraham-accords-and-their-cyber-implications-how-iran-unifying-regions-cyberspace

country toward which the product will be marketed".[3] Israel's defence ministry maintained that in easing the rules the government was still adhering to and protecting international standards of export control and supervision.

> "Amid increasing competition in the cybersecurity market, the Israeli government was reported to have eased some of its restrictions on the sale of cyberweapons to foreign entities in 2018."

Soon after the signing of the Abraham Accords, reports emerged that Israel's NSO Group Technologies had sold its infamous phone hacking software, Pegasus 3, to a number of GCC states, including the UAE and Saudi Arabia.[4] It is not clear when exactly these sales took place although they may have begun as early as in 2013 in the case of the UAE and 2017 in the case of Saudi Arabia.[5] But cybersecurity

[3] Tova Cohen and Ari Rabinovitch, "Israel Eases Rules on Cyber Weapons Exports despite Criticism", Reuters, 22 August 2019, https://www.reuters.com/article/us-israel-hackers-idUSKCN1VC0XQ

[4] i24, "Israeli Cybersecurity Firm Reportedly Sold Hacking Tech to UAE, Saudi Arabia", i24News, 23 August 2020, https://www.i24news.tv/en/news/israel/1598187507-israeli-cybersecurity-firm-reportedly-sold-hacking-tech-to-uae-saudi-arabia; Stephanie Kirchgaessner and Michael Safi, " Dozens of Al Jazeera Journalists Allegedly Hacked Using Israeli Firm's Spyware", *The Guardian*, 21 December 2020, https://www.theguardian.com/media/2020/dec/20/citizen-lab-nso-dozens-of-aljazeera-journalists-allegedly-hacked-using-israeli-firm-spyware

[5] Neri Zilber, "Gulf Cyber Cooperation with Israel: Balancing Threats and Rights", The Washington Institute for Near East Policy, 17 January 2019,

cooperation in other areas between Israel and some GCC countries may have begun much earlier.

The UAE was reported to have approached the US-based firm 4D Security Solutions, owned by an Israeli, Mati Kochavi, in 2007 to upgrade its defences around sensitive energy installations and establish a citywide smart surveillance system in Abu Dhabi known as Falcon Eye. According to multiple media reports, a Swiss company belonging to Kochavi won the contract to build these systems, with its Israel-based subsidiary, Logic Industries, providing the technology.[6] Subsequently, according to a former Israeli legislator, Riyadh sought Israeli cybersecurity assistance in 2012 to fix the damage arising from a major cyberattack against Saudi Aramco that wiped out three-quarters of the state-owned energy giant's computers. The incident, described at that time as the largest commercial cyberattack in history, was believed to have been the handiwork of the Iranians.[7] In 2017, *The Jerusalem Post* reported that Israeli companies were quietly negotiating with Saudi Arabia's sovereign wealth fund on possible ways to participate in the development of the Saudi smart city known as NEOM.[8] Apart from the sale of Israeli cybersecurity technologies, there also have been claims that

https://www.washingtoninstitute.org/policy-analysis/gulf-cyber-cooperation-israel-balancing-threats-and-rights

[6] Yossi Melman, "Israel-UAE: 25 Years of Secret Deals, with One Man at the Center", *Haaretz*, 20 August 2020, https://www.haaretz.com/israel-news/.premium-israel-uae-25-years-of-secret-deals-with-one-man-at-the-center-1.9080381?v=1628750197210; Neri Zilber, "Gulf Cyber Cooperation with Israel: Balancing Threats and Rights".

[7] Neri Zilber, "Gulf Cyber Cooperation with Israel: Balancing Threats and Rights"; Ahmed El-Masry, "The Abraham Accords and their Cyber Implications".

[8] Max Schindler, "Israeli Companies Talking to Saudi Arabia about $500b 'Smart City'", *The Jerusalem Post*, 25 October 2017, https://www.jpost.com/business-and-innovation/israeli-companies-likely-talking-to-saudi-arabia-about-500-bil-smart-city-508429

the UAE-linked firm DarkMatter was actively headhunting Israeli experts working at Unit 8200, Israel's elite cyber force.[9]

> "While most of these earlier transactions were conducted clandestinely, normalisation of relations has clearly made it easier for the GCC states to now openly engage Israel."

While most of these earlier transactions were conducted clandestinely, normalisation of relations has clearly made it easier for the GCC states to now openly engage Israel. Indeed, following the normalisation of relations between Israel and the UAE, the cybersecurity chiefs of both countries held an unprecedented public online meeting to discuss how to cooperate to address common cyberthreats.[10] Barely a year later, in April 2021, Israeli firms participated in the Cybertech Global conference held in Dubai and the two cybersecurity chiefs told *Haaretz* on the sidelines of the event that their relationship had since "matured into a 'brotherly' relationship" in the cyber arena. According to the newspaper, the UAE and Israel are currently sharing intelligence

[9] Amitai Ziv, "Mysterious UAE Cyber Firm Luring ex-Israeli Intel Officers With Astronomical Salaries", *Haaretz,* 16 October 2019, https://www.haaretz.com/israel-news/.premium-mysterious-uae-cyber-firm-luring-ex-israeli-intel-officers-with-astronomical-salaries-1.7991274

[10] Reuters, "UAE, Israeli Cyber Chiefs Discuss Joining Forces to Combat Common Threats", Reuters, 25 September 2020, https://www.reuters.com/article/israel-gulf-emirates-cyber/uae-israeli-cyber-chiefs-discuss-joining-forces-to-combat-common-threats-idUKL5N2GL4TR

and information on the Lebanese Hisballah movement's cyber activities.[11] The two chiefs revealed that there were now open lines of communication between them and between the two countries' computer emergency response teams, which have been holding workshops and sharing information. Moreover, the two raised the possibility of holding joint cybersecurity exercises in the future.[12]

Factors Driving Israel s Cybersecurity Cooperation

Normalisation of relations signals a realisation on the part of the Israeli government and its Bahraini and Emirati counterparts that there is a strategic need for them to reduce their susceptibility to the United States' whims in the region, notably in relation to US policy on Iran. Besides their shared dislike of Islamists, the UAE, Bahrain and Israel have been steadfast in their opposition to the current regime in Tehran and the removal of sanctions imposed on it. Removing sanctions, in their view, would not only provide the Islamic regime with a degree of legitimacy at home and abroad but would also enable it to conduct its regional policies more assertively. A more accurate reading of normalisation, therefore, is one that describes it as being born out of a shared desire for containing Iran as well as Islamists, with or without US support.

For Israel, sharing resources capable of detecting cybersecurity threats with partners that face the same sources of threat could give it early warning to deter similar attacks on itself. The sale of surveillance

[11] Omer Benjackob, "Israel and UAE Shared Intel on Hezbollah Cyberattack", *Haaretz*, 5 April 2021, https://www.haaretz.com/israel-news/tech-news/.premium-israel-and-uae-shared-intel-on-hezbollah-cyberattack-1.9683514

[12] Omer Benjackob, "Israel and UAE Shared Intel on Hezbollah Cyberattack"; Mandi Kogosowski, "UAE Cyber Security Head Calls For Joint Exercise with Israel", *Israel Defense*, 5 April 2021, https://www.israeldefense.co.il/en/node/49182

technology and other cybersecurity weapons also has psychological advantages for Israel that must not be underestimated. The Israeli government has an obsession with maintaining a qualitative edge over its adversaries in the region, notably Iran. Selling its state-of-the-art weaponry and spyware to countries that share its animosity towards the Islamic regime, i.e., the Gulf Arab states, has the potential to instil fear in Tehran,[13] given the reputed reliability and efficiency of such Israeli technology. It can give Israel an important psychological deterrence capability.

> "The Israeli government has for some time seen Israeli cybersecurity firms as an unofficial means of building relations with the GCC countries and overcoming the country's isolation in the region."

In addition, Israel frames its cyber interactions with the GCC states as a means of expanding its commercial presence in these countries while simultaneously buying their goodwill and their support for, or at least silence on, its broader regional interests with regard to Iran and Palestine. Indeed, the Israeli government has for some time seen Israeli cybersecurity firms as an unofficial means of building relations with the GCC countries and overcoming the country's isolation in the region.[14] Israeli firms have been involved in "track two" diplomacy

[13] Ministry of ICT, Iran, "Briefing No. 13", PAPSA, 2016, https://www.tic.ir/Content/media/filepool3/2016/11/628.pdf?t=636139402582751736

[14] Simon Handler, "Normalizing Arab-Israeli Relations through Cybersecurity Cooperation", Lawfare Blog, 14 August 2020,

for some time, and increased cyber cooperation between the GCC states and Israeli entities was indeed an important factor in the normalisation of Israel's relations with the UAE and Bahrain.[15] Thanks to their common animosity towards Tehran as well as the heavy presence of retired military and intelligence officers in their respective cyber sectors, cyber cooperation between Israel and its GCC counterparts has been a cost-effective way for the establishment of unofficial, yet significant ties and understanding between their defence/security officials. For instance, NSO's founders are all ex-members of the Israeli Unit 8200[16] while DarkMatter's founder, Faisal Al Bannai, hails from a family/tribe with close ties to security forces in the Emirates.[17]

There also is an important strategic interest involved in Israel's willingness to sell cyberweapons to selected foreign entities. The sale of spyware and hacking tools to particular states is a way of discouraging the latter from investing in the development of their own domestic capabilities in this sector. If these states can satisfy their needs by buying off-the-shelf products from Israel, or by developing such products in

https://www.lawfareblog.com/normalizing-arab-israeli-relations-through-cybersecurity-cooperation

[15] Simon Handler, "Normalizing Arab-Israeli Relations through Cybersecurity Cooperation"

[16] Jenna McLaughlin, "Facing a Public Backlash, an Israeli Spyware Firm Is Now Scoring Its Government Customers",
Yahoo News, 26 May 2021, https://ph.news.yahoo.com/an-infamous-israeli-spyware-firm-looks-to-bolster-its-image-by-scoring-customers-154024020.html?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAJlTFTTcE9ZprBtUaFfMPG9tAYo2zmN65e8IHnbP-XRm8MMP0PdNVwur11DuJpMxSgpCp7s_omA_NxyuoSnxKH-KwPPc-bnMaN5tJZWzsD8UwZkRAzvuhnDB7yYFNpVSr7qYevBj08kRPh1OQPEv9suayHCYNLWln5eSox3y6y-l

[17] Jon Gambrell, "UAE Cyber Firm Darkmatter Slowly Steps Out of the Shadows", AP News, 1 February 2018,
https://apnews.com/article/e6c2cb4445b5464b8b9548f7d314e9b8

cooperation with their Israeli counterparts, they would have less reason to develop their own indigenous capabilities, an undesirable eventuality from Israel's point of view, both for technological and commercial reasons.

Exporting cyber technologies to the GCC countries no doubt has a business angle for the Israeli firms concerned. Given the GCC countries' deep pockets and lack of indigenous capabilities, they represent a lucrative market for Israeli firms to exploit.[18] Also, the use of their products by certain GCC states to successfully spy on their critics and/or political activists has marketing advantages.[19] It demonstrates the cyber capabilities of the state of Israel and could have a buzz effect in that it helps amplify interest in the country's cyber products and surveillance tools, thereby paving the way for further expansion of Israeli firms into overseas markets. It could also catch the attention of both institutional and private investors and make it easier for Israeli firms to raise capital for their product research and development.

Implications of Israel-GCC Cybersecurity Cooperation

Israel's sale of spyware and other malicious digital tools to authoritarian regimes has come under criticism by human rights groups as being devoid of principle, given that such technologies can be used to infringe on the privacy of domestic populations. Israeli technology no doubt enables Abu Dhabi, Manama and Riyadh to monitor their citizens'

[18] Market Research, "GCC Cyber Security Market Forecast 2018–2028", Market Research.com, 2018, https://www.marketresearch.com/Visiongain-v1531/GCC-Cyber-Security-Forecast-11700089/

[19] Hagar Shezaf and Jonathan Jacobson, "Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays", *Haaretz*, 20 October 2018, https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027

online activities better and faster, which in turn could lead to a further erosion of public space for the expression of dissent. However, the use of such technologies is not likely to lead to any fundamental changes in domestic politics in Bahrain, the UAE or Saudi Arabia. It will certainly not catalyse a popular backlash against these regimes. While there has been some opposition to the normalisation of relations with Israel in some of the GCC countries,[20] this have been limited to online expressions of anger, shame, or disapproval, which the authorities have been quick to identify and "neutralise", a capability that perhaps can be attributed to the use of Israeli technology. This is best demonstrated in the case of the Israeli firm IntuView and its collaboration with the Bahraini and Saudi authorities. In the case of Saudi Arabia in particular, IntuView's technology has been credited for the marked improvement in Riyadh's efforts to monitor the online activities of Saudi citizens and jihadists since 2015.[21]

"Israel's sale of spyware and other malicious digital tools to authoritarian regimes has come under criticism by human rights groups as being devoid of principle."

More importantly, normalisation does not seem to have changed the power dynamics in the GCC states. However, it has the potential to further strengthen the dominant players in these states. Given the tribal and patronage-based nature of the GCC states' economies, key families

[20] Hamad al-Shamsi, "How the UAE Is Suppressing Criticism of Its Normalization With Israel", Democracy for the Arab World Now, 2 June 2021, https://dawnmena.org/how-the-uae-is-suppressing-criticism-of-its-normalization-with-israel/

[21] Neri Zilber, "Gulf Cyber Cooperation with Israel: Balancing Threats and Rights".

and business conglomerates will be allowed to prosper from the opening of ties and capitalise on the economic opportunities that are on the horizon for as long as they support the ruling families' efforts to boost ties with Israel. This is particularly true in sectors such as tourism, as well as medicine, agriculture and cybersecurity, where the GCC states have a great deal to learn from Israel.

"Increased cyber cooperation between Israel and the GCC states could … prompt the Iranian regime to both invest more in developing its own offensive capabilities and improve those of its proxy groups in order to mount coordinated and multifaceted preventive attacks."

While increased (cyber) cooperation will not significantly alter the nature of domestic politics in the GCC, the perceived deepening of their cyber cooperation does not bode well for the stability of the regional and global cyber domains. Regionally, increased cyber cooperation between Israel and the GCC states could further destabilise the region by prompting the Iranian regime to both invest more in developing its own offensive capabilities and improve those of its proxy groups in order to mount coordinated and multifaceted preventive attacks.[22] Owing to the difficulty of attribution in the cyber domain, Tehran is likely to seek to compensate for its own technological inferiorities by utilising the

[22] Tim Stickings, "Iran 'Giving Hezbollah cyber training' as It Embraces Digital Warfare", *The National*, 29 June 2021, https://www.thenationalnews.com/world/europe/iran-giving-hezbollah-cyber-training-as-it-embraces-digital-warfare-1.1251159

element of surprise to preemptively fend off an attack or intrusion before one has been initiated. In short, increased cyber cooperation between Israel and the GCC states could increase the prospect of more frequent and fatal state-sponsored cyberattacks in the Middle East.

Globally, the newfound cyber affinity between the Israelis and the GCC states could contribute to the proliferation of sophisticated spyware and consolidation of digital absolutism at a time when their Western allies are pushing for the creation of a democratic alliance to counter the perceived threats of digital authoritarianism.[23] It could substantially limit the appeal, and credibility, of US and EU criticisms of alleged Chinese, Iranian and Russian misconduct in cyberspace.

Whither Israel-GCC Cyber Cooperation?

Looking at the possible trajectory of Israel's covert and overt relations with the GCC states, the widely divergent views of both sides on Iran constitute a formidable obstacle to the longevity of their relations since they may not be able to devise a common path for the day after should there be a regime change in Tehran, or a substantial softening of the current regime's approach to international relations. Unlike the Arab trio, whose leaderships prefer an isolated Iran to one on good terms with the international community,[24] Israel would stand to benefit from the return of Iran to the international community's fold as a normal actor with a regime that plays by international rules and is no longer committed to the destruction of Israel. While such an Iran will be largely welcomed in

[23] Michael R. Pompeo, "The Clean Network", US Department of State, 2020, https://2017-2021.state.gov/the-clean-network/index.html

[24] Trita Parsi, "The Real Regional Problem With the Iran Deal", *Foreign Affairs*, 23 February 2021, https://www.foreignaffairs.com/articles/middle-east/2021-02-23/real-regional-problem-iran-deal

Israel, it may not be a development to be celebrated in Bahrain, the UAE or Saudi Arabia. After all, a brief glance at the history of Iran's relations with its southern neighbours reveals that their mutterings with Tehran have more to do with the latter's Persian, rather than Shi'a, identity.[25]

* *Mr Nima Khorrami is an Associate Research Fellow at the Arctic Institute in Washington, DC, and at the OSCE Academy in Bishkek. His areas of interest and expertise lie at the intersection of geopolitics, infrastructural development and technology.*

[25] Fred Halliday, "Arabs and Persians beyond the Geopolitics of the Gulf", *Cahiers d'études sur la Méditerranée orientale et le monde turco-iranien* 22 (1996): 1–17, https://doi.org/10.4000/cemoti.143

NUS National University of Singapore | Middle East Institute Singapore

29 Heng Mui Keng Terrace
Block B #06-06
Singapore 119620
Tel: +65 6516 2380; Fax: +65 6774 0458
Email: contact.mei@nus.edu.sg
www.mei.nus.edu.sg