Digital recognition: cybersecurity and internet infrastructure in UAE–Israel diplomacy

BASSANT HASSIB AND JAMES SHIRES[*]

[*] This article is part of a special section in the November 2024 issue of *International Affairs* on 'Cybersecurity in world politics', guest-edited by Tobias Liebetrau and Linda Monsees. The authors are grateful to the special issue guest editors for their vision and encouragement; to the participants in a workshop "cybersecurity in/for world politics" held in the University of Copenhagen on 8-9 February 2024 for their insightful comments; and to two anonymous reviewers for their detailed and constructive feedback. Funding for James Shires' contribution to this article was provided to ECCRI by UK Research and Innovation (UKRI), as a member of the consortium for the Horizon Europe project Reigniting Multilateralism Through Technology (REMIT). REMIT research is conducted under the umbrella of the European Union's Horizon Europe research and innovation program, grant agreement No 101094228. UKRI's and the European Commission's support to the project does not constitute an endorsement of its findings, which reflect the views of the authors alone. UKRI and the European Commission are not responsible for any use which may be made of the information contained therein.

In 1994, officials from Israel and the United Arab Emirates (UAE) met secretly in Washington DC to alleviate Israel's security concerns around the proposed sale of F-16 aircraft to the UAE by the United States.[1] More than two decades later, on 15 September 2020, the two countries signed the Abraham Accords, agreeing to '*recognize* and respect each other's sovereignty and right to live in peace and security, develop friendly relations of cooperation between them and their peoples, and settle all disputes between them by peaceful means'.[2] The Abraham Accords, however, were notable not just for their ambitious—and, since the latest Gaza war which began in October 2023, increasingly hollow—claim to resolve the Arab-Israeli dispute. They also included a heavy emphasis on technological cooperation, especially around digital technologies. Half of the 12 named cooperation 'spheres' in the treaty concern technological innovation, in addition to its attestation of the importance of science and technology cooperation 'in the growth of multiple key sectors', *and* the dedication of a whole sphere to cooperation on various forms of ICT innovation.[3] What role, then, did digital technologies play in this landmark shift in UAE–Israel recognition?

The concept of recognition, central to the Abraham Accords, has attracted much attention in International Relations (IR). Notwithstanding the wider political and philosophical connotations of recognition, the focus of IR accounts is primarily on recognition of states *as states*: that is, on recognition of their rights and obligations as sovereign members of the international system. IR theories of recognition, however, hardly consider the role digital technologies play in state recognition. Within more narrowly legal approaches, the contribution of digital technologies to paradigmatic moments of state recognition like the Abraham Accords remains unnoticed. For more expansively sociological perspectives, digital technologies are an underappreciated aspect

[1] Adam Entous, 'Donald Trump's new world order', *New Yorker*, 11 June 2018, https://www.newyorker.com/magazine/2018/06/18/donald-trumps-new-world-order. (Unless otherwise noted at point of citation, all URLs cited in this article were accessible on 26 Sept. 2024.)

[2] US Department of State, *Abraham Accords peace agreement: treaty of peace, diplomatic relations and full normalization between the United Arab Emirates and the State of Israel*, 15 Sept. 2020, https://www.state.gov/wp-content/uploads/2020/09/UAE_Israel-treaty-signed-FINAL-15-Sept-2020-508.pdf (emphasis added).

[3] The seven sectors with a clear technological component in the Treaty Annex are: finance and investment; innovation, trade and economic relations; science, technology and peaceful uses of outer-space; environment; healthcare; agriculture and food security; and telecommunications and post. In the last of these, the parties 'strive to develop frameworks for innovation in ICT', explicitly mentioning submarine cables, e-commerce, satellite systems, fibre optics, broadcasting services, advanced fixed and wireless communications, 5G networks and smart cities.

of state capacity, identity and self-image. Finally, digital technologies also force us to rethink assumptions about the role of non-state actors, especially the private sector. This article therefore asks: what is the role of digital technologies in state recognition?

This article uses the UAE–Israel case to inductively develop three propositions regarding the role of digital technologies in state recognition. First, states use digital technologies—and the private sector companies that own and operate them—as *diplomatic lubrication*: a means to navigate around and overcome difficult diplomatic relationships, building momentum towards recognition. Second, digital competition between states leads them to conform their national economic structures towards global technology companies in similar ways, thereby indirectly recognizing each other as equal participants in a global contest—which we term *market-oriented homogenization*. Third, states and private sector actors involved together in transnational internet infrastructure projects develop technical working practices, interests and dependencies that facilitate diplomatic recognition—which we term *infrastructural integration*. Building on these three propositions, we put forward an overall concept of 'digital recognition' to capture their common theme: the influence of digital technologies, their owners or their operators on state recognition. This article thus contributes to IR theories of technology and international relations, as well as helping to overcome what Monsees and Liebetrau describe as the "three biases" in existing cybersecurity literature in IR: focusing on the state, the military and operating from a Western starting point.[4]

The article is structured as follows. The next section sets out the background to the Abraham Accords and the role of digital technologies. After a brief methodological discussion, the second section details three aspects of digital technologies—cybersecurity, cloud computing and subsea cables—and their connection to the Abraham Accords and UAE–Israel diplomacy, developing the above three propositions from each one in turn. The third section synthesizes these propositions, while the fourth discusses their theoretical implications. The article concludes with a reflection on the generalizability of this argument.

[4] Linda Monsees and Tobias Liebetrau, 'Cybersecurity and International Relations: developing thinking tools for digital world politics', *International Affairs* 100: 6, 2024, pp. 000–000, https://doi.org/10.1093/ia/xxxxx.

The Abraham Accords in context

The Abraham Accords appeared to the casual observer as a sudden and dramatic reversal of the UAE's previous policy of 'no normalization without statehood', adopted by nearly all Arab states: namely, formal recognition of Israel in return for Israel's recognition of an independent Palestinian state. This reversal was a major political gamble for the UAE. Egypt had been shunned by other Arab states after its recognition of Israel at the 1978 Camp David Accords,[5] and Jordanian normalization in 1994 took place during the high-water mark of the Palestinian peace process, a year after the Oslo Agreement.[6] While the Abraham Accords came with an Israeli commitment to 'halting the annexation of the Palestinian territories' (presented by the Emirati foreign minister as a 'significant diplomatic achievement'), they did not provide a path to Palestinian statehood.[7]

The UAE was widely regarded as the leading Arab actor in the Abraham Accords. Of the other three Arab signatories, Morocco and Sudan accepted significant diplomatic gains from the United States (recognition of sovereignty over Western Sahara and removal from diplomatic sanctions respectively) in return for their participation,[8] while Bahrain was primarily seen as a bellwether for the potential inclusion of Saudi Arabia.[9] However, informal UAE–Israel cooperation began well before the signing of the Accords, across fields of security, military,

[5] Avi Shlaim, *Lion of Jordan: the life of King Hussein in war and peace* (New York: Alfred A. Knopf, 2008).

[6] Karim Makdisi, *Palestine and the Arab-Israeli conflict: 100 years of regional relevance and international failure*, MENARA Working Papers (Middle East and North Africa Regional Architecture, 2018), https://www.iai.it/sites/default/files/menara_wp_27.pdf.

[7] UAE Government, Ministry of Foreign Affairs, 'Freeze on annexation of Palestinian territories a significant diplomatic achievement: Dr. Anwar Gargash', 13 Aug. 2020, https://www.mofa.gov.ae/en/mediahub/news/2020/8/13/13-08-2020-uae-palestine.

[8] Linah Alsaafin, 'Where do Morocco and Sudan relations stand with Israel?', Al Jazeera, 18 Sept. 2023, https://www.aljazeera.com/news/2023/9/18/where-do-morocco-and-sudan-relations-stand-with-israel.

[9] Peter Baker, Isabel Kershner, David D. Kirkpatrick and Ronen Bergman, 'Israel and United Arab Emirates strike major diplomatic agreement', *New York Times*, 13 Aug. 2020, https://www.nytimes.com/2020/08/13/us/politics/trump-israel-united-arab-emirates-uae.html; Martin Chulov, 'Saudi heir and Jared Kushner inch Kingdom towards deal with Israel', *Guardian*, 14 Sept. 2020, https://www.theguardian.com/world/2020/sep/24/saudi-heir-and-jared-kushner-inch-kingdom-towards-deal-with-israel.

commerce, sports, health and energy.[10] Both countries share key national security concerns, namely Iran, the expansion of terrorism and Islamist movements supported by Iran, and the regional influence of Turkey. On the security and military front, the UAE and Israel began overt security cooperation in 2006, when the UAE was granted access to Israeli satellite images.[11] This cooperation accelerated rapidly in the years leading up to the Abraham Accords, driven by the US. Both countries participated in joint US-supervised military exercises in 2017 and 2019, and both joined a US-established international alliance on maritime security.[12] Also in 2019, three secret US-sponsored conferences led to a dedicated trilateral forum to strengthen security cooperation against Iran.[13]

Although the Abraham Accords enjoyed strong support from US President Donald Trump and his closest advisers, US foreign policy also influenced UAE–Israel recognition at a more strategic level. US strategic retrenchment in the region caused it to seek to share security burdens with key regional states such as the UAE, bringing them closer to Israel.[14] The UAE thus became a primary player in a ‘network-centric’ regional order,[15] rather than a passive recipient of US protection, with increased military assertiveness in Yemen, the Horn of Africa and Libya.[16]

[10] Although not considered further here, non-security cooperation includes the establishment of an Israeli diplomatic office in Abu Dhabi in 2015 to facilitate its membership of the UAE-based UN International Renewable Energy Agency (IRENA), and Israeli national participation in sports ranging from judo to cycling.

[11] Sigurd Neubauer, ‘Israel: a strategic partner for the UAE?’, *Fair Observer*, 27 Nov. 2017, https://www.fairobserver.com/region/middle_east_north_africa/israel-united-arab-emirates-gulf-cooperation-council-news-91711.

[12] Arab Center for Research & Policy Studies, *The ‘Abraham’ Agreement: normalization of relations or announcement of an existing Emirati–Israeli alliance?* (Doha: Arab Center for Research & Policy Studies, 2020), https://www.dohainstitute.org/en/PoliticalStudies/Pages/The-Abraham-Agreement-Normalisation-of-Relations-or-Declaration-of-Existing-Alliance-between-Israel-and-UAE.aspx.

[13] Dave Lawler and Barak Ravid, ‘Scoop: Israel and UAE discuss anti-Iran cooperation at secret White House meeting’, AXIOS, 4 Feb. 2020, https://www.axios.com/2020/02/04/israel-uae-white-house-meeting-iran-trump-kushner.

[14] Md Muddassir Quamar, ‘Changing regional geopolitics and the foundations of a rapprochement between Arab Gulf and Israel’, *Global Affairs* 6: 4–5, 2020, pp. 593–608, https://doi.org/10.1080/23340460.2020.1865110.

[15] Andreas Krieg, ‘The war in Gaza, the decline of US leadership and the emergence of a networked regional order’, *Mediterranean Politics*, publ. online 26 May 2024, https://doi.org/10.1080/13629395.2024.2358618; Alessandro Marrone and Karolina Muti, *NATO’s future: Euro-Atlantic alliance in a peacetime war* (Rome: Istituto Affari Internazionali, 2020), pp. 2–3.

[16] Ebtesam Al Ketbi, ‘Contemporary shifts in UAE foreign policy: from the liberation of Kuwait to the Abraham Accords’, *Israel Journal of Foreign Affairs* 14: 3, 2020, pp. 391–8, https://doi.org/10.1080/23739770.2020.1845067.

Meanwhile, Israel continued to receive extensive and virtually unconditional US support. The Abraham Accords therefore represent an explicit reassertion of the UAE's security interests over any supposedly normative considerations regarding Palestinian statehood.[17] These longer-term trends, especially the multifaceted influence of the US, are a crucial backdrop for this article's focus on digital technologies.

Digital technologies and the Abraham Accords

Both Israel and the UAE lean on digital technologies as part of national identities, economic strategies and security advances—but in very different ways. For the UAE, digital technologies are the basis for an ambitious post-oil economy, driven by digital entrepreneurship, blockchain fintech, artificial intelligence (AI) and a 'Dubai' model of a business-friendly, socially conservative but tourism- and entertainment-focused society.[18] On the Israeli side, the key to its world-leading technology sector, according to many, has been the close connection to its military.[19] Israeli national service provides practical experience, connections and knowledge for post-military entrepreneurs, using technology companies to bypass its controversial reputation and overcome local conflicts.[20] With over 7,000 start-ups and over 400 hubs focusing on technology and cybersecurity, international and multinational technology corporations have heavily invested in Israel, with many setting up Israeli offices or subsidiaries.[21] Given this

[17] Neil Quilliam and Sanam Vakil, *A pyramid of multilateral confidence-building measures in the Middle East* (Rome: Istituto Affari Internazionali, 2020), p. 3, https://www.iai.it/en/pubblicazioni/pyramid-multilateral-confidence-building-measures-middle-east.

[18] Robert Mogielnicki, 'The emergent Gulf sovereign wealth fund–global tech nexus', Arab Gulf States Institute in Washington, 2 May 2024, https://agsiw.org/the-emergent-gulf-sovereign-wealth-fund-global-tech-nexus.

[19] Ori Swed and John Sibley Butler, 'Military capital in the Israeli hi-tech industry', *Armed Forces & Society* 41: 1, 2015, pp. 123–41, https://doi.org/10.1177/0095327X13499562; Nir Reuven, 'Is Israel the "start-up nation" because of its unique security situation?', Begin–Sadat Center for Strategic Studies, 28 Dec. 2023, https://besacenter.org/is-israel-the-start-up-nation-because-of-its-unique-security-situation; Anchal Vohra, 'Israel's military-technology complex is one of a kind', *Foreign Policy*, 19 Dec. 2023, https://foreignpolicy.com/2023/12/19/israels-military-technology-complex-is-one-of-a-kind.

[20] Yoav Dubinsky, 'Sport–tech diplomacy: exploring the intersections between the sport–tech ecosystem, innovation, and diplomacy in Israel', *Place Branding and Public Diplomacy*, vol. 18, 2020, pp. 169–80, https://doi.org/10.1057/s41254-020-00191-2; Itzhak Mashiah and Eli Avraham, 'The role of technology and innovation messaging in the public diplomacy of Israel', *Journal of Global Politics and Current Diplomacy* 7: 2, 2019, pp. 5–28, https://journal.centruldedic.ro/wp-content/uploads/2020/01/Mashiah_Avraham_2019-2.pdf.

[21] Israel Innovation Authority, 'Innovation in Israel', https://innovationisrael.org.il/en/contentpage/innovation-israel; Start-up Nation Central, 'Start-up Nation finder', https://finder.startupnationcentral.org.

shared, although qualitatively different, digital focus for Israel and the UAE, it would be surprising if digital technologies did not also contribute to their international relations, including arguably the most fundamental element: recognition of other sovereign states.

Methodologically, such mutual prioritization of digital technologies makes this case an appropriate site for theory development regarding the role of such technologies; what Bennett and Elman call ‘conceptual innovation’, following David Collier in describing its purpose as ‘extracting ideas from close range’ in a single, detailed case.[22] This is what we refer to in the introduction as an inductive approach (moving from the particular to the general), rather than vice versa.[23] While case-studies in IR are usually nationally bounded, this is a single case of bilateral recognition involving two states, incorporating additional complexity as these states are simultaneously competing to advance their national economies *and* cooperating in developing diplomatic relationships, with both goals involving the same digital technologies.[24] Although such multiple levels of interaction are problematic for the isolation of variables in theory testing, in this instance the ‘fuzzy’ nature of the case helps to surface several ways in which digital technologies contribute to UAE–Israel recognition, captured by the three propositions in the following subsections.[25]

Within the wider ambit of digital technologies, we focus on cybersecurity and two aspects of internet infrastructure—cloud computing and subsea internet cables. We select these elements not only because they are areas of high priority for both Israel and the UAE, but because they are highly interdependent. Cloud computing requires a resilient internet infrastructure, with speed partly dependent on the number and bandwidth of cable connections between countries. Both cable and cloud infrastructure require stability and security, relying on cybersecurity

[22] See Alexander L. George and Andrew Bennett, *Case studies and theory development in the social sciences* (Cambridge, MA: MIT Press, 2005); Andrew Bennett and Colin Elman, ‘Case study methods in the International Relations subfield’, *Comparative Political Studies* 40: 2, 2007, pp. 170–95, https://doi.org/10.1177/0010414006296346.

[23] In non-positivist methodologies, there is a more iterative interaction between theory and empirics. Daniela Lai and Roberto Roccu, ‘Case study research and critical IR: the case for the extended case methodology’, *International Relations* 33: 1, 2019, pp. 67–87, https://doi.org/10.1177/0047117818818243.

[24] Audie Klotz, ‘Case selection’, in Audie Klotz and Deepa Prakash, eds, *Qualitative methods in International Relations: a pluralist guide* (London: Palgrave Macmillan, 2008), https://doi.org/10.1057/9780230584129_4.

[25] On fuzziness, see John Gerring, *Case study research: principles and practices* (Cambridge, UK: Cambridge University Press, 2006).

technologies for data protection and resilient connectivity. This interdependence means we can only understand the contribution of these different sectors to UAE–Israel recognition by considering them together.

Cybersecurity

On 24 September 2020, less than two weeks after the signing of the Abraham Accords and at the height of the COVID–19 pandemic, Israel and the UAE held an online conference between senior officials to discuss shared cyber threats.[26] In the conference Igal Unna, the head of Israel's National Cyber Directorate, asserted that 'we [Israel and the UAE] are threatened by the same threats ... because of the nature of the region, because of the nature of our new, 'outed' relations and because of who we are—strong economically and technologically'.[27] This statement pinpoints the reason for the centrality of cybersecurity to the Abraham Accords. On the one hand, Israel's unmatched offensive and defensive cyber capabilities made it an attractive potential partner to help the UAE counter Iranian cyber threats. On the other, Israel saw the UAE as an Arab leader with financial heft and enthusiasm for digitalization, and thus a potential market for Israeli military technologies and cybersecurity products.[28]

Cybersecurity cooperation between the UAE and Israel had already increased substantially in the years preceding the Abraham Accords, including periodic visits by top Israeli officials to the UAE.[29] One notorious example of such cooperation in action is the sale of surveillance software.[30] Most prominently, the UAE purchased Israeli company NSO Group's Pegasus spyware, which was used to spy on activists, academics and journalists, as well as rebellious

[26] 'UAE, Israeli cyber chiefs discuss joining forces to combat common threats', Reuters, 24 Sept. 2020, https://www.reuters.com/article/us-israel-gulf-emirates-cyber/UAE–Israeli-cyber-chiefs-discuss-joining-forces-to-combat-common-threats-idUSKCN26F2UK.

[27] 'UAE, Israeli cyber chiefs discuss joining forces to combat common threats'.

[28] Mohamed Soliman, 'How tech is cementing the UAE–Israel alliance', Middle East Institute, 11 May 2021, https://www.mei.edu/publications/how-tech-cementing-UAE–Israel-alliance.

[29] Neri Zilber, 'Gulf cyber cooperation with Israel: balancing threats and rights', Washington Institute, 17 Jan. 2019, https://www.washingtoninstitute.org/policy-analysis/gulf-cyber-cooperation-israel-balancing-threats-and-rights.

[30] Elia Zureik, 'Settler colonialism, neoliberalism and cyber surveillance: the case of Israel', *Middle East Critique* 29: 2, 2020, pp. 219–35, https://doi.org/10.1080/19436149.2020.1732043.

members of Dubai’s royal family.[31] UAE cooperation with NSO started as early as 2013, in what was described as the ‘next big deal’ for NSO.[32] To facilitate such cooperation, in 2019 Israel’s ministry of defence eased export control rules on spyware to allow Israeli tech companies to quickly access markets like the UAE.[33] The Israeli government then authorized three export deals in the UAE, mediated by former senior Israeli defence officials, bringing in US$80 million in revenue for NSO.[34] As summarized by Isaac Ben-Israel, a leading cyber expert and chairperson of the Israeli Space Agency: ‘there was nothing wrong with using technology to form a bond with neighbours that have shunned formal ties … [spyware sales] is a legitimate tool of diplomacy’.[35]

Surveillance cooperation extended beyond spyware. Already in 2007, the UAE had approached the Israeli-owned, US-based firm 4D Security Solutions to upgrade defences around sensitive energy installations and establish a citywide ‘smart’ surveillance system in Abu Dhabi.[36] The system was implemented by AGT International—owned by Israeli tech pioneer Mati Kochavi—via its Israel-based subsidiary, Logic Industries. A landmark 2019 report stated that former members of the foremost Israeli signals intelligence department, Unit 8200, moved to work for a cybersecurity company called Dark Matter, closely associated with the UAE’s intelligence services.[37]

[31] Bassant Hassib and James Shires, ‘Cybersecurity in the GCC: from economic development to geopolitical controversy’, *Middle East Policy* 29: 1, 2022, pp. 90–103 at p. 101, https://doi.org/10.1111/mepo.12616.

[32] Bill Marczak et al., *The great iPwn: journalists hacked with suspected NSO group iMessage ‘zero-click’ exploit* (Toronto: Citizen Lab, 2020).

[33] Simon Handler, ‘The zero-day war? How cyber is reshaping the future of the most combustible conflicts’, Atlantic Council, 28 Oct. 2019, https://www.atlanticcouncil.org/blogs/new-atlanticist/the-zero-day-war-how-cyber-is-reshaping-the-future-of-the-most-combustible-conflicts.

[34] All following details in this paragraph derived from Ronen Bergman, ‘Weaving a cyber web’, *Ynetnews*, 1 Nov. 2019, https://www.ynetnews.com/articles/0,7340,L-5444998,00.html.

[35] Tova Cohen and Ari Rabinovitch, ‘Israel eases rules on cyber weapons exports despite criticism’, Reuters, 22 Aug. 2019, https://www.reuters.com/article/us-israel-hackers/israel-eases-rules-on-cyber-weapons-exports-despite-criticism-idUSKCN1VC0XQ.

[36] All details in the following two sentences derived from Zilber, ‘Gulf cyber cooperation with Israel’.

[37] Wadih Awawdah, ‘Israeli sources: “Tel Aviv uses UAE to spy on Qatar, Iran and Hezbollah”’, *Middle East Monitor*, 19 Oct. 2019, https://www.middleeastmonitor.com/20191019-israeli-sources-tel-aviv-uses-uae-to-spy-on-qatar-iran-and-hezbollah; Christopher Bing and Joel Schectman, ‘Inside the UAE’s secret hacking team of American mercenaries’, Reuters, 30 Jan. 2019, https://www.reuters.com/investigates/special-report/usa-spying-raven.

However, spyware sales and surveillance cooperation are only the tip of the iceberg. Cybersecurity is a huge business for Israel, which exports nearly US$4 billion worth of related products and services globally each year.[38] Israel has the highest per capita concentration of cybersecurity companies in the world, and very few engage in offensive activities (hacking external targets). The vast majority operate in relatively benign fields, such as threat intelligence, intrusion detection and prevention, or training and awareness. Although some scholars acknowledge this broader industry in analyses of Israel's global perception and power projection, these works have rarely focused on Israel–UAE relations in any detail.[39]

Cybersecurity interactions featured prominently in the wave of post-normalization activities. In 2021 Dubai hosted the Israeli Cybertech Global Conference, organized by Kenes Exhibition and Israel Defense Magazine.[40] Tel Aviv and Abu Dhabi then launched the 'UAE–IL tech zone' to connect UAE–Israeli technological companies, business and government collaborations.[41] Synaptech, an Abu Dhabi-based company backed by the Israeli Avnon Group, announced funding of US$100 million for a joint venture in Abu Dhabi akin to the model of Israel's 'Start-Up Nation' to develop strategic industries including cybersecurity.[42] UAE's ambassador to Israel, Mohamed al-Khajah, launched a cooperation task force with Eugene Kandel, CEO of Israeli Startup Nation Central, focusing especially on financial technology, cyber and digital health.[43]

Crucially, cooperation went beyond joint events and investment announcements to include practical cybersecurity coordination. UAE-based EliteCISOs and Israel's Cyber Together claimed to cooperate on knowledge-sharing, professional training and cybersecurity workshops

[38] Zilber, 'Gulf cyber cooperation with Israel'.

[39] Fabio Cristiano, 'Israel: cyber securitization as national trademark', in Scott N. Romaniuk and Mary Manjikian, eds, *Routledge companion to global cyber-security strategy* (Abingdon and New York: Routledge, 2021). For an exception, see Zilber, 'Gulf cyber cooperation with Israel'.

[40] Afini Nurdina Utami and M. Hamdan Basyar, 'Strengthening cybersecurity of the United Arab Emirates after the establishment of diplomatic relations with Israel', *Journal of Middle East and Islamic Studies* 9: 1, 2022, p. 11, https://doi.org/10.7454/meis.v9i1.146.

[41] See 'The UAE–IL Tech Zone', https://www.uaeil.tech.

[42] Utami and Basyar, 'Strengthening cybersecurity of the United Arab Emirates', p. 12.

[43] Shoshanna Solomon, 'Joint Israel–UAE taskforce to study ways to boost tech cooperation', *Times of Israel*, 13 April 2021, https://www.timesofisrael.com/joint-israel-uae-taskforce-to-study-ways-to-boost-tech-cooperation.

to help confront emerging threats to both countries.[44] Tel Aviv-based cybersecurity firm ClearSky published reports of a hacking group attributed to Hezbollah, which was responsible for cyber attacks on targets including Egypt, the UAE, Saudi Arabia and Israel.[45] The UAE–Israel joint project 'Crystal Ball'—a digital platform to detect and repel cyber attacks through intelligence-sharing and collaboration—was announced at the 2023 Cyber Week event in Tel Aviv, supported by Microsoft, Israeli defence company Rafael and Abu Dhabi-based CPX. In his remarks, UAE cybersecurity chief Mohamed Al-Kuwaiti underlined that that UAE's relations with Israeli tech companies were essential to its cybersecurity. In his words, 'cyberthreats do not distinguish between nations … we need to unite against those threats'.[46]

Overall, this section has shown that cybersecurity contributed to Israel–UAE recognition in the lead-up to the Abraham Accords through covert spyware sales, then as part of the publicity surrounding the Accords themselves, and afterwards developed into more practical cooperation. Crucially, each phase was largely driven by the states involved, directing companies with close national security ties (such as NSO, staffed by Israeli military veterans, or Dark Matter, associated with UAE security agencies) to act in ways that further the states' agendas—in this case, diplomatic relations and, ultimately, formal bilateral recognition. Consequently, we suggest this role could best be described as diplomatic lubrication: while it was not the underlying rationale for recognition for either state, cybersecurity helped to kick-start and maintain the recognition process.

The suitability of cybersecurity for this role is due in part to the way in which digital technologies, while far from borderless, significantly alter traditional notions of security and territory.[47] Cyber threats such as ransomware, on which Crystal Ball focused, target victims based partly on technological vulnerabilities that spread through software, undermining

[44] Shoshanna Solomon, 'UAE, Israel battle computer hackers together with "Crystal Ball" platform', *The Circuit*, 28 June 2023, https://circuit.news/2023/06/28/UAE–Israel-create-crystal-ball-platform-to-fight-hackers.

[45] Soliman, 'How tech is cementing the UAE–Israel alliance'.

[46] Shoshanna Solomon, 'UAE, Israel battle computer hackers together with "Crystal Ball" platform'.

[47] Fabio Cristiano, 'Deterritorializing cyber security and warfare in Palestine: hackers, sovereignty, and the national cyberspace as normative', *Cyber Orient* 13: 1, 2019, pp. 28–42; Daniel Lambach, 'The territorialization of cyberspace', *International Studies Review* 22: 3, 2020, pp. 482–506, https://doi.org/10.1093/isr/viz022; Jordan Branch, 'What's in a name? Metaphors and cybersecurity', *International Organization* 75: 1, 2021, pp. 39–70, https://doi.org/10.1017/S002081832000051X.

conventional security architectures built around intentional and predictable adversaries. Tackling such threats (via defence or offence) thus requires new forms of international engagement, especially between states with complementary digital capacities. Similarly, commercial spyware sales help states overcome digital security protections and encrypted messaging protocols to target what they see as national security threats. These new dependencies underpin the diplomatic value of cybersecurity companies, which provide technologies, products and services to help states to effectively combat these emerging security threats.

Cloud computing

A few days before the signing of the Abraham Accords—but after their public announcement—the Emirati company G42 declared that it was to open an international office in Israel. G42, a technology company specializing in AI, big data and cloud computing that is chaired by the UAE's national security advisor Sheikh Tahnoon bin Zayed Al-Nahyan, is a standard-bearer for the UAE's digital economic ambitions and identity. G42's press release gave two reasons for this move: first, to connect G42 to Israeli talent, technologies and resources; and, second, to serve 'as a gateway for Israeli companies … to expand their operations in the UAE'.[48] Peng Xiao, CEO of G42, summarized: 'The new Israeli office will … give us access to one of the most vibrant and mature tech ecosystems in the world.'[49] G42's Israel expansion also included a joint venture with Israel's Rafael in April 2021, described by the latter's CEO Yoav Har-Even as 'another leap in the relationship between our countries'.[50] This section explores how the UAE and Israel have developed similar strategies to embrace cloud computing technologies while insisting on security restrictions.

In 2021 commentators on Israel's local cloud computing sector suggested it had grown more slowly than its US or European counterparts, in part due to concerns around 'security [and] data

[48] G42, 'G42 to open international office in Israel', 10 Sept. 2020, https://www.g42.ai/resources/news/g42-to-open-international-office-in-israel.

[49] G42, 'G42 to open international office in Israel'.

[50] 'Abu Dhabi's G42 forms JV with Israel's Rafael to commercialize AI, big data tech', *Forbes Middle East*, 19 April 2021, https://www.forbesmiddleeast.com/innovation/artificial-intelligence-machine-learning/abu-dhabis-g42-forms-jv-with-israels-rafael-to-commercialize-ai-big-data-tech.

sovereignty'.[51] These terms refer to the fear that global cloud computing requires countries to send sensitive government or personal data for processing elsewhere, presenting individual and national security risks. Israel's flagship attempt to capture the economic benefits of cloud computing while managing these risks is a tendering contract, known as Project Nimbus, for a range of government services, awarded in May 2021. The tender came with localization conditions, including the construction of at least three physically separate data centres. The contract was ultimately awarded to Google Cloud Platform and Amazon Web Services (AWS), each of which announced new Israeli cloud 'regions' (a region being a set of data centres) around the time of the contract.[52] This localization condition was crucial, as the other bidders either did not invest in dedicated data centres (IBM), delayed their construction (Microsoft), or also launched them shortly before the Nimbus decision (Oracle).[53]

Most coverage of Project Nimbus, especially since the onset of the Gaza war, has focused on the provision of computing resources to politically sensitive aspects of the Israeli government, including the 'defence establishment' and land authority (responsible for settlements). This focus, while important, inaccurately paints the relationship between the Israeli government and these cloud companies as close and productive. Instead, Project Nimbus has been beset with delays, meaning that many Israeli government agencies still use local Microsoft solutions.[54] Some setbacks arise from the company side—reportedly unmet Israeli expectations that Google and AWS would bring their valuable suite of solutions in-country —while others come from favouritism baked into the contract. The Israeli government allowed relatively high charges for third-party users of these services (up to 20 per cent), while Google offered Israel a 15 per cent

[51] Donna Goodison, 'AWS' Israeli cloud contract, data centers will boost partner ecosystem: AllCloud CEO', CRN, 11 June 2021, https://www.crn.com/news/cloud/aws-israeli-cloud-contract-data-centers-will-boost-partner-ecosystem-allcloud-ceo.

[52] Sebastian Moss, 'Google plans to build fourth Israeli data center, despite employee protests over Nimbus contract', *Data Centre Dynamics*, 11 Nov. 2021, https://www.datacenterdynamics.com/en/news/google-plans-to-build-fourth-israeli-data-center-despite-employee-protests-over-nimbus-contract.

[53] Alex Alley, 'Microsoft to deploy Israeli cloud region: the scramble for Middle East is well underway', *Data Centre Dynamics*, 23 Jan. 2020, https://www.datacenterdynamics.com/en/news/microsoft-deploys-israeli-cloud-region.

[54] Assaf Galid, 'gwgl wʾmzwn hshqy ʾt hʿnn hmmshlty - ʾk hlqwḥwt lʾ bʾym', [Google and Amazon launched the government cloud two years ago—but the customers are not coming], *Globes*, 8 Aug. 2023, https://www.globes.co.il/news/article.aspx?did=1001454378.

discount on consulting fees for its cloud services.[55] Both Microsoft and Oracle have appealed against the contract decision and have continued to invest in their Israeli presence, meaning that the struggle over economic benefits and security concessions is far from over.

A similar story applies in the UAE. While the UAE has had a data protection law since 2021 and a cloud security policy since 2023, the executive regulations of the former have not been published, meaning it cannot yet be enforced. Instead, companies have sought to overcome more nebulous security concerns by partnering closely with local entities. Microsoft, the first hyperscaler to locate a cloud region in the UAE, did so in conjunction with the former national telecom provider, Etisalat (now e&), in part to ensure national control.[56] Oracle's expansion from a data centre to full cloud region in 2019–2020 was presented in terms of 'disaster recovery' and a preference for keeping data local.[57] IBM launched twin data centres in Abu Dhabi and Dubai for 'extra security' in January 2020,[58] while Amazon—as in Israel—worked gradually up to cloud region investment between 2018 and 2022.[59] Some commentators have suggested the attractiveness of the UAE for these companies is due not to its local entrepreneurial sector, but to its rather close connections to big regional markets in Saudi Arabia and Israel, as well as across the Indian Ocean.[60] Not all moves were successful, though—Microsoft delisted its Abu Dhabi cloud region in 2023, retaining only the other, in Dubai.

The most striking common factor in these investments is their relationship to G42 and its subsidiaries. G42 Cloud announced a partnership with IBM in February 2022, and then with Dell

[55] Billy Perrigo, 'Exclusive: Google contract shows deal with Israel defense ministry', *TIME*, 12 April 2024, https://time.com/6966102/google-contract-israel-defense-ministry-gaza-war.

[56] Microsoft, 'Microsoft to deliver the intelligent cloud from new datacenters in the Middle East', 14 March 2018, https://news.microsoft.com/en-xm/2018/03/14/microsoft-to-deliver-the-intelligent-cloud-from-new-datacenters-in-the-middle-east.

[57] Alkesh Sharma, 'Oracle to launch new cloud facilities in UAE and Saudi Arabia', *The National*, 19 Sept. 2019, https://www.thenationalnews.com/business/technology/oracle-to-launch-new-cloud-facilities-in-uae-and-saudi-arabia-1.912274.

[58] John Benny, 'IBM launches two UAE data centres in Middle East push', CIO, 7 Jan. 2020, https://www.cio.com/article/201505/ibm-launches-two-uae-data-centres-in-middle-east-push.html.

[59] Alvin R. Cabral, 'Amazon web services launches second Middle East cloud region in the UAE', *The National*, 30 Aug. 2022, https://www.thenationalnews.com/business/economy/2022/08/30/amazon-web-services-launches-second-middle-east-cloud-region-in-the-uae.

[60] Simon Sharwood, 'Arabian, sorry, Amazon Web Services to land in Bahrain and UAE', *The Register*, 27 Sept. 2017, https://www.theregister.com/2017/09/27/aws_middle_east.

and SAP[61] in late 2022. Microsoft then signed an agreement with G42 in April 2023, branding its collaboration as ‘sovereign cloud’ and explaining that G42’s understanding of the UAE’s security requirements was central to this partnership.[62] In April 2024 Microsoft invested US$1.5 billion in G42, receiving a seat on the board and US guarantees that G42 would divest from Chinese technologies. Throughout the growth of cloud computing in the UAE, the state has worked to maintain its security requirements through its close links to key local companies, as well as facilitating diplomatically useful ties to Israel, as noted above.

Overall, although this section began with evidence that cloud computing lubricated UAE–Israel recognition—via G42’s actions after the Abraham Accords—the thrust of the analysis has been on competition. In the context of what some observers have called, with uncomfortable colonial echoes, a ‘scramble for the Middle East’ in cloud computing in the years around the Abraham Accords,[63] both Israel and the UAE have sought to maximize the benefits of cloud adoption, while imposing what they see as necessary security restrictions and hard-fought contract concessions. Their strategies were different: Israel opened a single major contract to all the big hyperscalers, inviting competition between them but creating inefficiencies due to overpromises and technological lock-in, while the UAE built up G42 as a gateway to its national cloud, creating overlapping partnerships while absorbing talent and material assets such as data centres. Despite these differences in the detail, the high-level outcomes were remarkably similar, as both Israel and the UAE positioned themselves according to the requirements, policies and practices of these multinational companies. We suggest this matching orientation can be best described as *market-oriented homogenization*, each indirectly recognizing the other as a legitimate competitor while cooperating in some discrete areas.

A longstanding strain of International Political Economy (IPE) has critically evaluated how neo-liberal market mechanisms forced states to standardize macroeconomic policies, with parallels

[61] System Analysis Program Development (SAP) is a multinational enterprise headquartered in Walldorf, Germany. It develops enterprise resource planning (ERP) software for companies, which collects and processes data on one platform and provides cloud and AI solutions.

[62] Microsoft, ‘G42 teams up with Microsoft to explore acceleration of UAE’s digital transformation’, 11 April 2023, https://news.microsoft.com/en-xm/2023/04/11/g42-teams-up-with-microsoft-to-explore-acceleration-of-uaes-digital-transformation; Dan Swinhoe, ‘Microsoft and G42 to set up sovereign cloud in UAE’, *Data Centre Dynamics*, 6 Sept. 2023, https://www.datacenterdynamics.com/en/news/microsoft-and-g42-to-set-up-sovereign-cloud-in-uae.

[63] Alley, ‘Microsoft to deploy Israeli cloud region’.

also in longer-term concessionary practices of both the energy and defence industries.[64] However, the market-oriented homogenization generated by digital technologies is qualitatively different. It is enacted not just at the strategic or policy level, but at the level of wires and code, hardware and software. This phenomenon goes beyond regulatory alignment and diffusion, involving repeated interactions with complex socio-technical digital systems. While such interactions often include policy commitments (training a certain number of students, creating a certain value of local business), they also include technological commitments: to develop new ways of integrating cloud services with government or business practices, and to build and maintain dedicated data centres, programming languages and skill sets. These states are not just offering—or being asked for—policy changes, but also technological alignment with that company, and are explicitly asking for *digital* sovereignty in return.

Subsea cables

There are around 30 undersea internet cables in the Middle East, generally built and managed by consortia of national telecoms companies, large infrastructure multinationals and government agencies. While the governance of internet cables is highly commercialized, with private companies operating much of the infrastructure, a recent fibre-optic cable project demonstrates how these public–private consortia contribute to Israel–UAE recognition, by positioning each other as partners in the same community. In 2020, prior to signing the Abraham Accords, Cinturion—a US-based company backed by an Israeli infrastructure investment fund, Keystone, with a 25 per cent stake—announced the development of the Trans Europe Asia System (TEAS) cable with landing stations in Saudi Arabia, UAE and Israel. Also in 2020, Cinturion entered a partnership with New York-based investment firm Stonecourt Capital. One of Stonecourt's partners, Arik Arad, is former head of security for Israeli airline El Al at Ben Gurion Airport and chairperson of Israeli cyber aviation company CyViation, which includes Stonecourt Capital as an investor along with IAI (Israel Aerospace Industries). This cable project sought to establish an alternative route in the Middle East—bypassing a bottleneck in Egypt—that is more resilient to

[64] Timothy Mitchell, *Rule of experts: Egypt, techno-politics, modernity* (Berkeley, CA: University of California Press, 2002); Arturo Escobar, *Encountering development: the making and unmaking of the Third World* (Princeton: Princeton University Press, 1995).

disruptions and less expensive to operate.[65] Thus, for Cinturion, opening new corridors for internet traffic between India and Europe will help it build more resilient connectivity for users and customers, own more cables, roll out data/cloud centres (mainly in Israel, the UAE and Saudi Arabia) to catch up with their cloud computing rivals—mainly the companies covered in the previous section.

For Israel, Cinturion's cable represents the potential for the co-creation (albeit via US-based commercial intermediaries) of new regional internet infrastructure with the UAE. Israel also sees cables as a tool to strengthen ties with regional neighbours and broker an official normalization deal with Saudi Arabia, akin to the deal with the UAE. As Israel's then minister of communication, Yoaz Hendel, put it in 2022, 'in any place where you can lay down cables overland or undersea, you also create mutual interests'.[66] This was reinforced a year later by Israeli Prime Minister Benjamin Netanyahu, who highlighted the benefit of fibre-optic cables as a way to link Israel to countries across Asia, Middle East and Europe. In his words, 'the most obvious [link] is a fibre optic connection. That's the shortest route. It's the safest route. It's the most economic route'.[67] There is an additional domestic rationale at play as well: cable projects improve Israel's own internet infrastructure, providing high-paid technology jobs in poorer areas of the country and reducing inequality.

For the UAE, an integrated Cinturion cable with Israel translates into more widely available domestic high-speed internet connectivity and cooperation with Israel to maintain resilient connectivity through Israel's cybersecurity technologies, detailed in the subsection above.[68] In 2023 Centurion signed an agreement with du, a commercial brand of the Emirates Integrated

[65] Paul Cochrane, 'Israeli-backed internet cable aims to link country to Saudi Arabia and Gulf states', *Middle East Eye*, 3 April 2023, https://www.middleeasteye.net/news/israel-saudi-arabia-gulf-states-internet-cable-link; Paul Cochrane, 'UAE landing station confirmed for fibre optic cable set to link Israel to Gulf states', *Middle East Eye*, 22 Sept. 2023, https://www.middleeasteye.net/news/uae-landing-station-confirmed-fibre-optic-cable-set-link-israel-gulf-states.

[66] Chris Pleasance, 'Google plans fibre-optic cable linking Saudi Arabia and Israel as it connects India to Europe and opens a new route for global internet traffic', *Daily Mail*, 24 Nov. 2020, https://www.dailymail.co.uk/news/article-8982279/Google-plans-fibre-optic-cable-linking-Saudi-Arabia-Israel.html.

[67] Cochrane, 'UAE landing station confirmed for fibre optic cable'.

[68] 'Israel hopes new data cables can make friends of former enemies', *The Economist*, 5 March 2022, https://www.economist.com/middle-east-and-africa/2022/03/05/israel-hopes-new-data-cables-can-make-friends-of-former-enemies.

Telecommunications Company, and Saudi Arabia to build its landing stations (in Saudi Arabia, on the Red Sea coast near Neom City) .[69] The project is also backed by the Saudi-based GCC Interconnection Authority, a private company jointly owned by the six states of the Gulf Cooperation Council, which signed an agreement with a consortium consisting of Saudi Arabia's Etihad Atheeb Telecommunication Company and Cinturion.[70]

A similar two-way underwater fibre-optic cable project proposal was announced in June 2023, connecting the Mediterranean and the Red Sea to link Europe, the Gulf and Asia. The cable will be built by the Israeli state-owned Europe Asia Pipeline Company in cooperation with the UAE. An official at the Israeli ministry of communications, Elad Malka, stated that 'the Abraham Accords made this [project] possible'. In a similar vein, Netanyahu reportedly commented: 'Today we are reaping more fruit of the historic Abraham Accords … this will attract investors and turn Israel into a global communications centre'.[71]

Although the Cinturion project remains in progress and has not materialized to the extent of cybersecurity or cloud computing, it highlights a third way in which digital technologies contribute to UAE–Israel recognition. Necessarily, cooperation on subsea cable projects is almost always multilateral, rather than bilateral, also involving many private sector partners in a large and often unwieldy consortium that generates mutual interests and dependencies, jointly digital and material. Such *infrastructural integration* does not generate the same momentum for diplomatic alignment as the lubrication of cybersecurity technologies above, nor does it occupy a predominantly competitive space where states homogenize for economic advantage. Instead, by binding states to a larger consortium, infrastructural integration contributes to recognition by normalizing and routinizing cooperation in the eyes of and along with others—both states and private sector partners.

[69] Cochrane, 'UAE landing station confirmed for fibre optic cable'.

[70] Melanie Mingas, 'TEAS project reaches new milestone', *Capacity*, 16 July 2020, https://www.capacitymedia.com/article/29otcfa1zpmeiisxxi22o/news/teas-project-reaches-new-milestone.

[71] Etgar Lefkovitz, 'UAE expected to join Israel in global communications project', Jewish News Syndicate, 14 June 2023, https://www.jns.org/abraham-accords/uae/23/6/14/294791.

Of course, the role of technology ‘megaprojects’ in state self-images is far from a new phenomenon.[72] However, digital infrastructural integration is qualitatively different to other large infrastructure consortia. In cable projects, states seek to ‘plug in’, quite literally, to data flows over the global internet, thereby conforming to the internet’s open standards and protocols and the governance structures that come with them: a cooperative, rather than competitive, homogenization, undertaken for interoperability more than for market success. The geopolitical implications of shared digital infrastructure—for both war and peace—are a major topic of current policy and academic debate, as data flows and physical links connect states in new and unanticipated ways.[73] Our contribution here is to suggest that among these implications is a shift in state recognition.

Synthesizing the role of digital technologies in recognition

So far, this article has identified three phenomena involving digital technologies—diplomatic lubrication, market-oriented homogenization and infrastructural integration—which occurred in the lead-up to, directly around and after the mutual recognition of Israel and the UAE at the Abraham Accords. Each of these phenomena foregrounds a different relationship between states and private companies, each with a different mechanism, result and contribution to UAE–Israel recognition. Each of these phenomena also includes a uniquely digital element, distinguishing them from other fields where states leverage corporate relationships for diplomatic and security concerns, conform to requirements of multinational companies, or embark on public-private partnerships for transnational infrastructural projects. These characteristics are summarized below in table 1.

<table>

Table 1: The role of digital technologies in UAE–Israel recognition

[72] Geoffrey L. Herrera, *Technology and international transformation: the railroad, the atom bomb, and the politics of technological change* (Albany, NY: SUNY Press, 2006); Keller Easterling, *Extrastatecraft: the power of infrastructure space* (London: Verso, 2014).

[73] Henry Farrell and Abraham L. Newman, ‘Weaponized interdependence: how global economic networks shape state coercion’, *International Security* 44: 1, 2019, pp. 42–79, https://doi.org/10.1162/isec_a_00351.

Aspect	Cybersecurity	Cloud computing	Subsea cables
Context	Increase in transnational cyber threats	Cloud underpins digital economic growth	Digital economies require greater connectivity
Mechanism	State-directed sales of cybersecurity tools and intelligence (offence and defence)	Competition for multinational cloud contracts	Partnership in consortiums generates mutual material/digital interests and dependencies
Result	Diplomatic lubrication	Market-oriented homogenization	Infrastructural integration
Primary direction of influence	States -> companies	Companies -> states	States + companies -> environment
Primary UAE–Israel dynamic	Cooperative	Competitive	Cooperative
Impact on UAE–Israel recognition	Builds informal relationships and provides public demonstration of cooperation	Perceives other states as legitimate competitors with similar interests and technological structures	Normalizes and routinizes cooperation in the eyes of other states and private sector actors

<endtable>

First, *diplomatic lubrication* describes the ability of states to direct private cybersecurity sales towards diplomatically favourable, national security-focused outcomes. For both Israel and the UAE, cyber threats—both internal and external—presented new vulnerabilities, forcing them to rethink their security posture and their traditional security partners. Cybersecurity companies on both sides developed products and services to help them effectively combat cyber threats, acting as a practical demonstration of cooperation and rapprochement. This cooperation initially functioned as informal recognition by UAE of Israel's state identity and capacities, due to its status as an unparalleled cybersecurity superpower. Diplomatic lubrication was initially the result of covert agreements between senior officials, with the UAE putting principles aside to obtain what it saw as the highest quality cyber-offensive products and services, and Israel observing the power of cybersecurity sales as diplomatic leverage. It then translated into legal recognition with the Accords, enabling the cyber-defensive market to also flourish.

Market-oriented homogenization, in contrast, covers the techniques states and multinational cloud companies use to negotiate market entry as part of their expansion into the Middle East region. While cloud investment also provides some level of diplomatic lubrication, the main insight here is that cloud multinationals perceive Israel and the UAE as very similar state actors: competing with similar requests, looking for the same benefits and offering similar commercial opportunities. Economic competition within narrow bounds set by an oligopolist global cloud market reinforces the legitimacy of other competitors for the same investment, simply by recognizing them as engaging in the same technical practices (building datacentres, developing compatible products), commercial signalling (domestic joint ventures) and individual upskilling (training and education). Market-oriented homogenization contributed to recognition by separately aligning state and private sector capabilities and practices in parallel to political normalization. Furthermore, since cloud centres require significant cybersecurity investment, they encourage further cybersecurity cooperation between both states, reinforcing the mechanism above.

Finally, *infrastructural integration* addresses the way states and companies generate mutual interests and dependencies through shared digital infrastructure, recognizing each other's value as a useful internet transit point and commercial consortium partner. This phenomenon is fundamentally material as well as legal and political. Infrastructural integration is driven by a combination of technical factors: cost, speed and resilience. It prioritizes questions of geography, environment and practical installation, while also finding ways to finesse project plans to accommodate diplomatic sensitivities. In addition, internet cables permit the participation of states in global cloud architectures, providing the necessary data speeds for high performance cloud computing, therefore reinforcing market-oriented homogenization at the data level through cooperative peer relationships at lower levels of the stack. While the main purpose of this article has been to develop these theoretical propositions from a detailed analysis of the UAE–Israel case, the next section goes further, considering broader implications for IR theories of state recognition.

Implications for theories of state recognition

The three phenomena above can be grouped together as ‘digital recognition’, defined as *the influence of digital technologies, their owners, or operators on state recognition*. In this section, we identify two implications of these phenomena for theories of state recognition. In line with the theory-development ambition set out above, the aim of this section is to highlight where digital recognition confirms, challenges or illuminates gaps in existing understandings of state recognition. Subsequent possible theoretical advances are out of scope, including testing the generalizability of these phenomena and developing a more theoretically robust account of their inter-relationship.

First, existing theories of state recognition can be characterized by an expansion from a formal component of international law to encompass a far wider range of state interactions, including issues of national identity, ontological security and moral positioning.[74] The concept of international recognition emerged within international law, considering conditions for states to be recognized as sovereign members of the international order, with accompanying rights and obligations.[75] International legal scholarship takes two approaches to international recognition: constitutive and declaratory. The former holds that states are granted recognition only by virtue of the consent of existing states, while the latter maintains that states are granted recognition by virtue of their own existence.[76] States seek ways to gain constitutive recognition for reasons of

[74] Alex Hoseason, ‘Recognition, multiplicity and the elusive international’, *Journal of International Political Theory* 18: 2, 2022, pp. 205–24, https://doi.org/10.1177/17550882211021438.

[75] Malcolm N. Shaw, *International law* (Cambridge, UK: Cambridge University Press, 2021).

[76] James Crawford, *The creation of states in international law*, 2nd edn (Oxford: Oxford University Press, 2006); L. Oppenheim, *Oppenheim’s international law* [1905], 9th edn, ed. by Robert Jennings and Arthur Watts (Oxford: Oxford University Press, 2008); Jens Bartelson, ‘Three concepts of recognition’, *International Theory* 5: 1, 2013, pp. 107–29 at pp. 115–16, https://doi.org/10.1017/s175297191300002x; Mikulas Fabry, *Recognizing states: international society and the establishment of new states since 1776* (Oxford and New York: Oxford University Press, 2010).

both security and development.[77] Constitutive international recognition can be explicit (formally stated) or implicit (via practice or other indirect signals), alternatively expressed as *de jure* or *de facto* recognition respectively. *De facto* recognition does not necessarily include establishing diplomatic relations.[78]

Broader approaches to international recognition move beyond international law, following Honneth in arguing for the significance of recognition theory to IR overall.[79] Such approaches address how states acquire recognition through their interaction with other states, and the consequences of those efforts;[80] Lebow and Lindemann stress that the struggle for recognition can reproduce or exacerbate conflicts, while Wolf suggests that recognition fosters international cooperation and peace.[81] Other scholars expand the concept of recognition even further. Bartleson defines epistemic recognition as acknowledgment of self-recognition, by virtue of possessing certain capacities, or as mutual recognition of states' identities and values.[82] Ricoeur and Wendt emphasize that being recognized is fundamentally an assurance of a state's own identity and capacity, which cannot exist independently from interaction with other states.[83] Coppieters even posits new forms of 'engagement without recognition' to maintain peace and trust between adversaries, establish regional stability and create trade and business avenues.[84]

[77] Gëzim Visoka, Edward Newman and John Doyle, eds, 'Introduction: statehood and recognition in world politics', in Gëzim Visoka, John Doyle and Edward Newman, eds, *Routledge handbook of state recognition* (Abingdon and New York: Routledge, 2019), p. 2.

[78] Shaw, *International law*, p. 394.

[79] Axel Honneth, 'Recognition between states: on the moral substrate of international relations', in Thomas Lindemann and Erik Ringmar, *International politics of recognition* (Boulder, CO: Paradigm, 2014).

[80] Patricia Greve, 'Ontological security, the struggle for recognition, and the maintenance of security communities', *Journal of International Relations and Development*, vol. 21, 2018, pp. 858–82, https://doi.org/10.1057/s41268-017-0108-y.

[81] Richard Ned Lebow, *Why nations fight: past and future motives for war* (Cambridge, UK: Cambridge University Press, 2010); Thomas Lindemann, *Causes of war: the struggle for recognition* (Colchester: ECPR Press, 2010); Reinhard Wolf, 'Respect and disrespect in international politics: the significance of status recognition', *International Theory* 3: 1, 2011, pp. 105–42, https://doi.org/10.1017/s1752971910000308.

[82] Bartelson, 'Three concepts of recognition', p. 108.

[83] Paul Ricoeur, *The course of recognition*, transl. by David Pellauer (Cambridge, MA: Harvard University Press, 2007); Alexander Wendt, *Social theory of international politics* (Cambridge, UK: Cambridge University Press, 1999); Alexander Wendt, 'The state as person in international theory', *Review of International Studies* 30: 2, 2004, pp. 289–316, https://doi.org/10.1017/s0260210504006084.

[84] Bruno Coppieters, 'Engagement without recognition', in Visoka, Doyle and Newman, *Routledge handbook of state recognition*.

The investigation of UAE–Israel recognition undertaken here indicates the importance of both approaches: narrowly legal, and expansively political and sociological. The Abraham Accords represented a clear mutual declaration of recognition, with the pomp and circumstance designed to symbolize a historic moment in regional relations, and an accompanying text of equal gravitas. In so far as *de jure* legal recognition remains the paradigm of state recognition (declaratory or constitutive), the empirical section above shows how digital technologies facilitated this moment. However, the role of digital technologies extends beyond legal recognition, even in its most diluted constitutive *de facto* form. The sections on cloud computing and subsea cables especially suggest that recognition builds on broader market legitimacy, technical capacity, and aspects of a state's identity and self-image, with the long history of security cooperation prior to the Abraham Accords underlining the varieties of engagement possible without formal legal recognition.

Second, despite the rich growth in recognition theory, the role of the private sector in international recognition remains underresearched.[85] Even treatments focused on market dynamics, where private sector actors are undoubtedly relevant, remain focused on state actions.[86] One exception is in international history, where scholars have explored extensively the idea that the English East India Company and its continental counterparts acted as 'company-states', contributing to the recognition of sovereign states in many regions of the world.[87] Overall, the highly varied diplomatic actions of these company-states can be summarized as efforts to make their economic interests legible to states or peoples they encountered, and to translate non-sovereign state systems into modes of being amenable to the exertion of those interests.

[85] See for example Stefan Talmon, *Recognition of governments in international law: with particular reference to governments in exile* (Oxford: Oxford University Press, 1998); David Raič, *Statehood and the law of self-determination* (The Hague: Kluwer Law International, 2002); Crawford, *The creation of states in international law*.

[86] Tian He and Michael Magcamit, 'The CPTPP, cross-strait tensions, and Taiwan's *recognition for survival strategy* under the democratic progressive party', *International Relations of the Asia-Pacific* 24: 2, 2024, pp. 217–5, https://doi.org/10.1093/irap/lcad013.

[87] Swati Srivastava, 'Corporate sovereign awakening and the making of modern state sovereignty: new archival evidence from the English East India Company', *International Organization* 76: 3, 2002, pp. 690–712, https://doi.org/10.1017/s002081832200008x.

This highlights the way in which related concepts to recognition, such as sovereignty, are crucial to understanding the aims and practices of state recognition. Concepts of sovereignty have undergone a very similar expansion and reformulation to concepts of recognition, including what Srivastava calls ‘hybrid sovereignty’, where sovereignty is negotiated by both public and private entities in a range of constellations and networks.[88] Others have gone further, identifying historic forms of political authority that go beyond a ‘sovereignty heuristic’, with contemporary relevance.[89] Strikingly, the trajectory of debates over recognition and sovereignty is almost exactly the inverse of those concerning digital technologies and the internet, where early conjectures of a non-sovereign space have been gradually replaced by various forms of ‘cyber’ and ‘digital’ sovereignty.[90] Some scholars even argue that the sheer quality and scale of multinational technology companies means they act almost as company-states, developing new forms of public–private relations.[91]

The role of digital technologies in state recognition, however, has remained unexplored. The three phenomena here call for further research to combine the fine-grained public–private approach of theorists of sovereignty and distributed political authority with internet scholars’ acknowledgement that digital technologies create fundamentally new kinds of public–private cooperation, reconstituting both sides of the boundary—and the boundary itself. More concretely, the kinds of quasi-territorial power and bargaining at work in cloud negotiations over ‘sovereign’ data, or sharing of data and threat intelligence of ‘national’ cyber threats, not only underline the central role of the private sector in state recognition, but suggest an extension to what Cocks calls the ‘political delusion’ of a sovereign state in the face of myriad digital

[88] Swati Srivastava, *Hybrid sovereignty in world politics* (Cambridge, UK: Cambridge University Press, 2022). See also Jordan Branch, *The cartographic state: maps, territory, and the origins of sovereignty* (New York: Cambridge University Press, 2014).

[89] Julia Costa Lopez, ‘Political authority in international relations: revisiting the medieval debate’, *International Organization* 74: 2, 2020, pp. 222–52, https://doi.org/10.1017/S0020818319000390.

[90] Lucas Kello, ‘The meaning of the cyber revolution: perils to theory and statecraft’, *International Security* 38: 2, 2013, pp. 7–40, https://doi.org/10.1162/ISEC_a_00138; Dennis Broeders and Bibi van den Berg, *Governing cyberspace: behavior, power and diplomacy* (Lanham, MD: Rowman & Littlefield, 2020).

[91] Florian J. Egloff, *Semi-state actors in cybersecurity* (New York: Oxford University Press, 2022); Tobias Liebetrau and Linda Monsees, ‘Assembling publics: Microsoft, cybersecurity and public-private relations’, *Politics and Governance* 11: 3, 2023, https://doi.org/10.17645/pag.v11i3.6771.

dependencies.[92] Put differently, the Abraham Accords may have put digital technologies at their core, but even as they did so, those technologies unwittingly unravel the Accords' meaning as a document of purely *state* recognition.

Conclusion

This article has sought to contribute to IR theories of state recognition by putting forward the concept of 'digital recognition': the influence of digital technologies, their owners or operators on state recognition. It argued that, within a landscape where digital technologies undoubtedly reshape geopolitics and geoeconomics, the concept of digital recognition calls attention to the ways in which such technologies affect the legal and political perspectives, attitudes and approaches of states towards each other; in other words, to the new ways in which states recognize each other in the digital era. The three propositions developed here—diplomatic lubrication, market-oriented homogenization and infrastructural integration—illustrate how the dynamics of UAE–Israel recognition go beyond international legal status, building upon years of prior secret cooperation and interaction due to overlapping security interests—especially in relation to Iran—and morphing to accommodate new digital security threats and economic promises.

This argument has broader conceptual and policy implications. Conceptually, the increasing influence of digital technologies on all aspects of state relations means that digital technologies are likely to contribute to international recognition dynamics beyond the UAE–Israel case. While their exact influence depends both on the specific digital technologies involved and the national and regional context, the three propositions developed in this article provide a starting-point for others to evaluate their application in cases where digital technologies are equally crucial to states' identities and strategies (such as China's policy towards Taiwan or Hong Kong, or Russia's recognition of Abkhazia and South Ossetia or Transdniestria), or alternatively to test them in cases where the role of digital technologies is less obvious (such as Western Sahara, the Chagos Islands or South Sudan).

[92] Joan Cocks, *On sovereignty and other political delusions* (London: Bloomsbury, 2014), https://doi.org/10.5040/9781780933573.

From a policy perspective, the argument developed here has implications for UAE–Israel relations and the expansion of the Abraham Accords to other key regional states, such as Saudi Arabia, in the shadow of the Gaza war. For the UAE, the key policy lesson is that digital recognition is a continual process, which will continue to be influenced by the commercial practices and incentives of private actors in relatively obscure settings. For the wider Middle East, outgoing US President Joe Biden's grand bargain attempts to end the Gaza war by offering Israel public recognition from Saudi Arabia, which Saudi Arabia claims to consider only in return for Israel's recognition of a Palestinian state. State recognition in Middle East politics, then, will continue to have seismic impacts on regional and global security for years to come. The propositions here indicate how digital technologies could play a constructive role, as with UAE–Israel, or—in a move well beyond the scope of this article—if the inverse propositions of diplomatic friction, market-oriented heterogeneity and infrastructural fragmentation could instead deepen divides over the role of digital recognition in Middle East peace.