The Lavender Veil: A Novel Theoretical Framework for Analyzing the Role of Covert Digital Security Partnerships in Arab-Israeli Relations

Wells Benjamin

School of Public and International Affairs, University of Georgia

CURO Undergraduate Research

Dr. Eli Sperling

11 December 2025

Introduction

The 21st century has seen the rapid proliferation of advanced digital technologies that have fundamentally reshaped social, economic, and political spheres across the world. Military application of software is not new to the contemporary era, but has expanded rapidly in the past decade. Military software is most often applied to the cyber and information domains, and can serve to greatly enhance the intelligence capabilities of states that integrate these systems into their intelligence cycle. Israel represents one of the world's leaders in military software production and usage, and continues to iterate new programs with consequential security applications. Since the 1970s, actors within the Israeli Defence Forces (IDF) have intentionally sought to develop advanced software oriented human capital, and as a result, the IDF has integrated many educational programs into their training process[1]. Today, many of Israel's most successful tech entrepreneurs hold connections to Israeli military intelligence units like Unit 8200, and this coalescence of the tech sector and military has resulted in Israel being a world leader in the development of security-related software[2]. The consistent presence of internal security threats originating from Palestine and external threats from Tehran and her allies in the past three decades has further driven both the need for these platforms and the ability to actively use them in the field. Israel has consistently used internal conflicts to test and improve upon military software before exporting it to the global market[3]. While much of these exports are targeted at Israeli allies like France and India, there has been a growing trend in sales of military software to Arab states that have traditionally avoided purchasing Israeli weapons.

---

[1] Breznitz, D. (2002). The military as a public space: the role of the IDF in the Israeli Software Innovation System (pp. 130-48). Samuel Neaman Institute for Advanced Studies in Science and Technology.
[2] Rousseau, J. P. (2017). The history and impact of unit 8200 on Israeli hi-tech entrepreneurship (Bachelor's thesis, Ohio University).
[3] Afrose, S. (2025). Algorithmic Surveillance and Digital Occupation: Pegasus Spyware and Artificial Intelligence Targeting Systems in Kashmir and Palestine.

Within the context of the Abraham Accords, Israeli-Emirati security cooperation has expanded rapidly in the past decade, with both states seeking to balance against the shared threats of Iran and internal dissidence[4]. This partnership has seen limited cooperation in traditional arms sales, with Israeli-made air-defense and drone systems being employed by the UAE during recent missile attacks by Iran[5]. UAE-owned subsidiaries of Israeli defense firms have been awarded lucrative orders for Israeli designed air defense platforms like SPYDER and Barack, and the two states have participated in joint military drills multiple times since 2021. Within these partnerships Arab states like the UAE are able to mobilize their considerable financial capital to form joint development agreements with Israeli firms that hold abundant human capital. While some states like Morocco and the UAE have been open to public diplomatic engagement with Israel, other key regional actors like Saudi Arabia remain hesitant to be openly associated with Israel within security contexts. In place of traditional alliance formation, the UAE and Saudi-Arabia have opted to engage with Israel via covert partnerships focused on advanced military software that allows for covert security linkage. Sales of the Israeli spyware platform Pegasus to Saudi Arabia and other Arab states have been ongoing since the 2010s, and the unique role of spyware platforms as a service rather than a good allows for robust security partnerships to quietly form[6]. Outside of spyware, Israel is also a world leader in the employment of AI in warfare, and during the most recent Gaza war widely employed systems like Lavender and Gospel to accelerate intelligence collection and targeting[7]. These systems are

---

[4] Dana, T. (2023). The new (dis) order: The evolving UAE-Israel security alliance. *Journal of Palestine Studies*, *52*(3), 62-68.

[5] Warrick, K. (2022, November 7). *Israel-UAE Defense Cooperation Grows Under the Abraham Accord*. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/israel-uae-defense-cooperation-grows-under-abraham-accord

[6] Kareem, K. (2024). A comprehensive analysis of pegasus spyware and its implications for digital privacy and security. *arXiv preprint arXiv:2404.19677*.

[7] Gusterson, H. (2024). It's all Lavender in Gaza. *Anthropology Today*, *40*(6), 1-2.

formed as bespoke products for the IDF, but the human capital behind their creation remains liquid and capable of developing similar products tailored to Arab states' security concerns.

This paper argues that two key areas of security partnership between Israel and Arab states, spyware that allows for improved internal security and artificial intelligence that benefits external security, are utilized as a quiet form of alliance building. Spyware such as Pegasus is capable of enabling Arab states to collect intelligence on internal dissidence, allowing for an enhanced ability to quell internal political opposition. AI tools serve as force multipliers for a variety of military contexts and can provide transformative benefits to cyber, intelligence, and kinetic domains, enhancing the ability of states to respond to external threats. The analysis of these cases is undertaken through a synthesis of neoclassical realist and constructivist logic that is applied to real-world cases of security cooperation between Israel and Arab states. The assumptions of neoclassical realism, that states exist in an anarchic system that forms rational choice logic promoting cooperation and balancing against shared threats, remain in place and are seen as the driving force behind state behavior. Constructivist logic is integrated to explain the role of domestic political concerns that mediate state behavior. Factors such as religious and national identity are seen as the source of constructivist cycles that form the symbolic costs behind state behavior in the execution of decisions motivated by realist logic.

The external shock of regional security threats produces the choice of increasing capability through cooperation, and given the qualitative military advantages held by the United States and Israel alongside the shared threat perceptions, Arab states are incentivized towards partnerships. Alliances with the US and Israel provide access to advanced technologies, including strategically

relevant capabilities like aircraft and air defense, as well as intelligence sharing and diplomatic leverage[8]. Arab states are, however, forced to mediate their decisions through their domestic lens and understand the risks inherent to cooperation with states viewed as normatively incompatible by much of their populations. Prior to 9/11, the US-Saudi relationship was strained over US support for Israel; however, in the wake of the war on terror, Saudi Arabia faced far greater threats from Islamic extremists, necessitating continued cooperation[9]. The fact that many of the 9/11 terrorists held significant connections to Saudi Arabia provoked further discord in the relationship, but also demonstrated the threat to national security posed by internal extremism within Saudi-Arabia. During the War on Terror, Saudi Arabia was forced to maintain robust ties with the US despite normative risks, and through this process, Arab elites recognized the severe potential domestic costs associated with decisions made to maintain external security. Learning from these lessons, today Arab states still seek to maximize security, but make decisions with normative blowback considered. The reluctance of Arab states to continue with the Abraham Accords process until they perceive the Palestinian issue to be stable demonstrates this[10]. While Saudi and Emirati political leadership are still keen to continue normalization with Israel, and have still done so quietly during the war, the public nature of comprehensive diplomatic frameworks like the Abraham Accords is particularly vulnerable to oppositional public dissent. The constructivist feedback cycle that produces varying degrees of internal dissent based on how apparent cooperation with Israel and the US is thereby incentivizes cooperation that provides the greatest increase in capability without modifying domestic perceptions of state leadership. For this reason, traditional military acquisitions are costly beyond what is rational to increase

[8] Bents, E. R. (1995). *The Sale Of US Military Aircraft to Saudi Arabia* (No. AFITCICIA95009).
[9] Ottaway, D. (2009). The King and us: US-Saudi relations in the wake of 9/11. *Foreign Aff.*, *88*, 121.
[10] Monshipouri, M., Dorraj, M., & Fields, J. (2025). The Gaza War and the Future Of the Abraham Accords. *Middle East Policy*.

security, incentivizing cooperation that is both covert and not easily attributable to partnerships with Israel and the US. Acquisition and co-development of spyware and AI intelligence tools is thus the logical choice for Arab leaders to take, and allows for capability increases that overcome normative constraints. The two key areas of current and future cooperation in the software space are cyber capabilities and artificial intelligence tools.

The following sections will apply an integrated theoretical framework to two domains of Israeli-Arab cooperation that exemplify the logic and explanatory ability of the theory.

1. Spyware tools like the Israeli "Pegasus" platform enhance regime security and the ability of Arab states to maintain domestic control over the normative cycle.
2. AI-enhanced defense analytical tools, which have a wide range of military applications and serve as a qualitative multiplier for capability.

These two cases demonstrate how Arab-Israeli partnerships are advancing within a "grey zone" of security cooperation, that is, outside of the traditional conception of alliance formation.

Theory

The past two decades have seen a fundamental shift in the nature of military technology as rapid advancements in surveillance and AI tools have introduced new problems and opportunities on the global stage. These tools provide a new capability for states to enhance their external and internal security through novel means that utilize advanced software in order to improve decision-making and intelligence collection. The Middle East has seen widespread implementation of advanced software for security purposes, driven by regional competition between American allies and the Iranian Axis of Resistance across traditional domains as well as information spaces. The dynamic tech sector within Israel has contributed substantially to this development. Israeli human capital has allowed for extensive development of advanced

platforms like Pegasus and Lavender, as Israel ranks first in the world for research and development as a share of total GDP[11]. The Gulf states, on the other hand, hold substantial financial resources gained from hydrocarbon exports, and are actively seeking to diversify their economies away from export dependency[12]. While traditional theoretical logic would predict the emergence of security and economic partnerships between Israel and Arab states in software development due to the highly mutualistic nature of potential partnerships that trade human capital for financial leverage, this has not occurred. The shared threat of Iran has led to a linkage between Israel and Arab states, but strict normative concerns within Muslim populations have prevented outright alliance formation. I argue in this paper that Israel and the Gulf States utilize covert digital security partnerships to overcome normative restraints towards traditional security relationships, and that this process can be explained by a theory that synthesizes neoclassical realist and constructivist frameworks.

Realist theory has long been used to explain state behavior in the Middle East, as the persistence of armed conflict within the region gives a wide range of applications. The balancing behavior of states in the region is of particular note, as it closely follows a neoclassical realist framework, with states like Saudi Arabia and the UAE seeking to maintain security against rising Iranian regional power[13]. The United States has long acted as an external security provider to Arab states in the region as well as Israel, but efforts to form a comprehensive alliance network between American partners have largely failed[14]. Much of the literature explains this discrepancy through

[11] Offenhauer, P. (2008). Israel's Technology Sector.
[12] Al Naimi, S. M. (2022). Economic diversification trends in the Gulf: The case of Saudi Arabia. *Circular Economy and Sustainability*, *2*(1), 221-230.
[13] Darwich, M. (2022). The view from Riyadh: A neoclassical realist perspective of Saudi foreign policy towards Iran in the post-2011 Middle East. In *Saudi Arabia and Iran* (pp. 14-32). Manchester University Press.
[14] Rakipoğlu, M. (2017). Revisiting the saudi position during the Iran-Iraq war through the lens of balance of threat theory. *Ortadoğu Etütleri*, *9*(1), 118-134.

the logic of Walt[15], in that states feel they can increase security through informal balancing that does not take the form of traditional alliance structures. While this does explain the fact that these informal relationships exist, it fails to fully account for why they are being chosen in favor of outright security cooperation[16] [17]. It has been argued that these states do not see closer ties as a rational choice given the American nuclear umbrella as an ultimate security guarantee; this overly systemic approach fails to account for the role domestic politics plays in foreign policy choices. Neoclassical Realism has expanded upon classical assumptions by integrating domestic variables, but it fails to account for how technological innovation alters state constraints, as well as their ability to overcome them. Likewise, constructivist theory has examined the normative limitations of Arab-Israeli cooperation, but does not explore how digital instruments allow states to both manage and overcome these limitations[18]. This paper bridges these gaps by examining the role of technology in contemporary Arab-Israeli relations.

The two-level game proposed by Putnam serves as an initial bridge between domestic and international politics in state behavior, allowing for theoretical integration of domestic political concerns[19]. The second level of Putnam's theory posits that leaders must consider the approval of domestic actors when making foreign policy decisions, and that foreign and domestic politics maintain a reciprocal relationship. When applied to the Middle East, it demonstrates the rationality behind decisions made by actors like the Saudi Crown Prince Mohammed bin Salman

[15] Walt, S. M. (1985). Alliance Formation and the Balance of World Power. International Security, 9(4), 3–43. https://doi.org/10.2307/2538540
[16] Schweller, R. L. (2014). Unanswered threats: A neoclassical realist theory of underbalancing. In *The Realism Reader* (pp. 265-271). Routledge.
[17] Morsy, A. (2019). Alliances and Threats in the Middle East: Neoclassical Realism and the Balance of Interest. *POMEPS Studies 34: Shifting Global Politics and the Middle East*, 81-85.
[18] Katzenstein, P. J. (Ed.). (1996). *The culture of national security: Norms and identity in world politics*. Columbia University Press.
[19] Putnam, R. D. (2017). Diplomacy and domestic politics: the logic of two-level games. In *International organization* (pp. 437-470). Routledge.

Al Saud to continue seeking Western partnerships while maintaining distance from Israel. The Saudi-American partnership is longstanding, and while it remains a matter of contention within Saudi Arabia, it is generally accepted as permissible by Saudi society. In the words of former president Barack Obama, when asked if the Saudis were friends of the US, "It's complicated," yet the alliance remains in place to this day, and has strengthened under the first Trump administration[20]. When a constructivist approach is integrated into this analysis, the framework is further strengthened by allowing for the explanation of what drives normative values into domestic politics, and therefore into international politics. Wendt's influential logic of norms that impact state behavior being formed through a reciprocal feedback system remains highly pertinent[21].

Following the widespread unrest of the Arab Spring, many Arab leaders saw how quickly internal discontent could be translated into a concrete security threat. The rapid spread of protest movements facilitated by social media and instant communication has demonstrated how quickly unrest could increase in severity during the digital age. The response of Morocco to protests in 2011 illustrates this point well, as the Moroccan regime drafted a reformed constitution in response to demands from digitally organized protesters[22]. While adept statecraft prevented protests from escalating to a level that truly threatened the power of the monarchy, the ability of organic protest movements to catalyze demands into state action was clearly shown. In the wake of these events, the Moroccan government began purchases of the Israeli Pegasus system, and

[20] Gause, F. G. (2016). The Future of US-Saudi relations: The kingdom and the power. *Foreign Affairs*, *95*(4), 114-126.
[21] Wendt, A. (1992). Anarchy is what states make of it: the social construction of power politics. *International organization*, *46*(2), 391-425.
[22] Benchemsi, A. (2012). Morocco: Outfoxing the opposition. Journal of democracy, 23(1), 57-69.

credible evidence shows frequent internal usage against dissident groups in order to surveil journalists and human-rights lawyers[23]

Arab leaders have recognized how maintaining internal security relies not only on managing a population's views of adherence to norms, but also on the ability of a state to monitor and control dissenting opinions. Anti-Israeli sentiment remains deeply entrenched in most Arab societies, and this divide has been considerably deepened by the war in Gaza, with growing outcry from the Arab public for states to take a more assertive approach to solving the Palestinian issue[24]. The role of Saudi Arabia as a religious leader within the Muslim world produces even greater risks of normative blowback on the international as well as domestic stage, limiting feasible implementation of the pure realist logic that would drive alliance formation.

The internal threat posed by internal dissent is amplified by the willingness of Iran to utilize irregular warfare techniques to support dissident non-state actors through a complex network of proxies. Since the 1980s, Tehran's Islamic Revolutionary Guard Corps–Quds Force (IRGC-QF) has continuously refined its development of asymmetric tactics. In Iraq, Iran has continuously supported the formation of Shiite militias like the Popular Mobilization Forces (PMF), and uses its influence over these groups to impact Iraqi domestic politics[25]. Within Lebanon, Iranian support of Hezbollah has allowed Iran to impact Lebanese politics through its influence over a quasi-state actor within Lebanon[26]. Iranian state media channels frequently amplify sectarian

[23] Galal, A. (2023). Mapping the supply of surveillance technologies to Africa Morocco country report. *Editor: Tony Roberts*.
[24] Nassar, Y. (2024). Israel's War on Gaza. *Al-Muntaqa: New Perspectives on Arab Studies*, *7*(2), 111-123.
[25] Smith, C., & Knights, M. (2025). How Iran aligned militias seized Iraq: irregular warfare, lawfare and regime change. Small Wars & Insurgencies, 36(4), 659-697.
[26] DeVore, M. R. (2012). Exploring the Iran-Hezbollah relationship: A case study of how state sponsorship affects terrorist group decision-making. Perspectives on terrorism, 6(4/5), 85-107.

sentiment within Saudi Arabia's Eastern province, and this has resulted in Shiite protests against the Saudi Monarchy[27]. Material support for the Houthis in Yemen has enabled the Houthis to remain a consistent threat to Saudi sovereignty, as well as a threat to international trade[28]. Throughout the Arab world, there is a consistent trend of Iran utilizing proxy actors and information warfare to threaten its enemies, and this provides a strong source of external threat generation within Arab states. Through these networks, Iran has historically sought to destabilize Arab regimes and provide an intermediary option for kinetic actions, and in response, states like Saudi Arabia have turned to spyware to help manage internal dissent, both provoked by Iran and organically present[29]. This mechanism serves to unify systemic and state-level security threats beyond the scope of traditional realist approaches, while also showcasing that the role of classical assumptions about state behavior remains pertinent. Arab states are thus posed with a considerable challenge: How can internal and external security be simultaneously maintained without producing normative blowback?

The Abraham Accords served as a strong first step in achieving this goal; however, the October 7th attacks and subsequent Israeli response derailed them. While Arab leaders maintained the goal of improving security via multilateral cooperation with partner states, doing so with Israel became far more daunting given the reignition of the Palestinian issue as a major domestic political concern. Given the barriers to traditional security cooperation with Israel, Arab states have found cooperation in certain key technological areas as a method by which external security

---

[27] Matthiesen, T. (2014). The Local and the Transnational in the Arab Uprisings. The Protests in Saudi Arabia's Eastern Province. *The Silent Revolution: The Arab Spring and the Gulf States*, 105-143.
[28] Johnston, T., Lane, M., Casey, A., Williams, H. J., Rhoades, A. L., Sladden, J., ... & Haberman, R. (2020). *Could the Houthis be the next Hizballah Iranian proxy development in Yemen and the future of the Houthi movement* (No. RR2551).
[29] Marczak, B., Anstis, S., Crete-Nishihata, M., Scott-Railton, J., & Deibert, R. (2020). Stopping the press: New york times journalist targeted by saudi-linked pegasus spyware operator.

can be improved without sacrificing internal stability. Developments in digital security tools within the past two decades have enabled states to receive the benefits of traditional alliance formation in a covert manner. The construction of this "gray zone" of partnership satisfies Realist incentives while minimizing constructivist disincentives. Digital security cooperation allows for a mechanism of quiet balancing in which capability is enhanced, and partnerships are deepened, without overt political alignment towards Israel. The neoclassical realist assumption that states foreign policy choices are mediated by domestic factors, yet are still ultimately driven by power maximization, is fully realized here[30]. The systemic concern for security against Iran is translated into the state level, where it is mediated by leaders based on concerns of normative blowback. Through this mediation, traditional forms of security cooperation with Israel become irrational, and quiet power maximization through covert sales of Israeli technology becomes highly favorable. The nature of these platforms allows for a functional bypass of the constructivist feedback loop that disincentivizes partnership with Israel, as they remain out of the domestic population's view. Artificial intelligence's mercurial nature allows for commercial cooperation to easily translate into military applications, with platforms being dual-use by the nature of the technology. Arab usage of spyware like Pegasus is similarly made opaque due to its classified nature and the difficulty in attribution of cyber tactics back to state intelligence services. Both AI and spyware exist within a blind spot of traditional realist logic, which is unable to properly account for power maximization that exists outside the realm of traditional military force. Solely using traditional realist logic is unable to account for the tangible security benefits of such technologies, as they provide no clear material advantage, yet can serve to greatly enhance capabilities.

[30] Rose, G. (1998). Neoclassical realism and theories of foreign policy. *World politics*, *51*(1), 144-172.

Case Study 1: Pegasus

Introduction

This case study will track the historical development of the Pegasus spyware platform from its inception to contemporary usage by state actors. Pegasus has emerged as one of the most consequential digital surveillance tools ever designed and has seen widespread proliferation in the past two decades. Alongside sales to traditional allies of Israel, many states not traditionally aligned with Israel, including Arab states, have bought this platform. The unique status of tools like Pegasus as services rather than traditional security sales has enabled the building of sustained relationships between the Israeli arms industry and foreign governments, which has translated into deeper overall security cooperation. The inherently covert nature of spyware has allowed Arab states to form a security partnership around Pegasus that does not hold the same normative constraints as traditional alliance formation. Despite the covert nature of this tool, widespread public outcry against its usage to monitor and suppress internal political dissidence has demonstrated the constructivist risks of Arab states utilizing Israeli technology.

Subheading 1.1: Inception and Capability

Pegasus is a comprehensive spyware tool developed by the Israeli cyber-intelligence firm NSO Group in 2011. NSO Group was founded by the members of a failed tech startup called CommuniTake that developed software capable of remotely accessing smartphones for tech support purposes[31]. After CommuniTake garnered little commercial interest, NSO Group founder Shalev Hulio was contacted by an unknown European intelligence agency that saw potential in their technology beyond customer service based applications. The development of powerful

[31] Bergman, R., & Mazzetti, M. (2022). The battle for the world's most powerful cyberweapon. The New York Times Magazine, 28.

encryption algorithms has made interception of cellular signals difficult to transform into concrete intelligence, because even if a signal could be intercepted, it was very difficult to decrypt. NSO Group sought to provide an innovative workaround to this issue by building a tool that targeted the smartphone itself rather than the signals it produced. The founders of CommuniTake brought in former Mossad agent Niv Karmi and began aggressively hiring veterans of Israeli military intelligence. Utilizing the technical knowledge gained from employees' service in units like Unit 8200, NSO Group was able to accelerate the development of Pegasus, and in 2011, the first iteration of it was ready to enter the market.

The first major sale to a foreign actor was to Mexican law enforcement, which aimed to utilize Pegasus to gain intelligence on drug cartels operating within Mexico. NSA often fed intelligence to Mexican intelligence which the NSA gained from hacked cellphones owned by Mexican criminals, and consequently Mexican authorities wanted greater capabilities and full control over them. NSO Group founders met with former Mexican president Felipe Calderón, and after approval from the Israeli Ministry of Defense, sold Pegasus to the Mexican government. Even at this initial stage, the Israeli government sought to turn these partnerships into concrete diplomatic benefits. It was understood that sales of Pegasus could act as a unique method for garnering better relations with states that were traditionally wary of Israel. Mexican authorities found Pegasus to be tremendously useful, and NSO Group entered the global cyber intelligence market as a powerful player with a uniquely capable system. While powerful intelligence agencies like the NSA had similar capabilities, Pegasus was the first off-the-shelf tool of its kind, and presented enormous security benefits through its ability to tap into cellphones.

NSO Group found a unique market niche in the early 2010s, filling gaps in intelligence capabilities held by smaller states that the US was unwilling to fully share intelligence with. The 2012 sale of Pegasus to Panama considerably deepened relations between the two states, and during a 2013 UN vote, Panama and Mexico were two of the only Latin American states to not vote in favor of recognizing the statehood of Palestine[32]. During this period, NSO Group was seeing rapid revenue growth, and in 2014 American private equity firm, Francisco Partners, acquired a majority stake in NSO Group for $130 million. Backed by American financial capital and with a proven product, sales of Pegasus expanded considerably in this period. Between 2014 and 2018, Pegasus was bought by over forty countries, and saw widespread use in a variety of applications[33]. While primarily used for conventional law enforcement and intelligence purposes like counternarcotics and counter terror, Pegasus has also been widely used as a means for controlling internal political opposition. The capabilities that make Pegasus so valuable as a legitimate tool, in turn, make it extremely effective at policing opposition parties, political activists, journalists, and lawyers.

Subheading 1.2: Arab Internal Security

Within Arab states, there is a considerable need for leaders to maintain high levels of internal control over their populations. The monarchic political structure of the UAE and SA does not allow for political pressure to be vented through democratic institutions, which makes internal dissent a matter of state survival. In SA, the Arab Spring did not result in widespread protest movements across the country, but the Shia population of the Eastern province did engage in protests[34]. SA responded with a brutal crackdown that involved the use of live ammunition

[32] Munck, R., & Pozzi, P. (2019). Israel, Palestine, and Latin America: Conflictual Relationships. *Latin American Perspectives*, *46*(3), 4-12.
[33] Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries.
[34] Kamrava, M. (2012). The Arab Spring and the Saudi-led counterrevolution. *Orbis*, *56*(1), 96-104.

against protesters and showcased the willingness of the monarchy to maintain stability through any means necessary. Fears of Iranian influence over the Shia minority within SA have further stoked anxieties regarding minority revolt, and the success of Iranian support for the Houthis rebels in recent years has cemented the reality of these concerns.

Despite the risks of lengthy prison sentences for online dissent, as showcased by the 2022 trial against women's rights activist Salma al-Shehab over social media posts criticizing the monarchy, much of Saudi political dissent has moved into online spaces[35]. In response, the Saudi government has put forth significant investment into tools to monitor and track figures critical of the monarchy. Pegasus provides a comprehensive tool capable of surveilling Saudi citizens anywhere in the world, and was used to track the journalist Jamal Khashoggi prior to his 2018 assassination [36]. Pegasus provides Saudi security services with actionable intelligence at a very low risk and is able to penetrate online spaces where dissent propagates. Investigations by NGOs have revealed widespread usage of Pegasus to target activists critical of the human rights abuses within Saudi Arabia, and despite a temporary Israeli ban on spyware exports to the kingdom in 2018 following the Jamal Khashoggi case, the partnership continues[37].

The UAE faces similar concerns regarding internal dissent and has become increasingly repressive towards internal threats since the Arab Spring. In the wake of the Arab Spring, many

---

[35] Amnesty International. (2025, February 6). *Saudi woman imprisoned for tweeting in support of women's rights released after four-year ordeal*. https://www.amnesty.org/en/latest/news/2025/02/saudi-woman-imprisoned-for-tweeting-in-support-of-womens-rights-released-after-four-year-ordeal/

[36] Amnesty International. (2021, July 18). The Pegasus Project. https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

[37] Scott-Railton, A., Marczak, B., Razzak, N. A., Deibert, R., & Crete-Nishihata, M. (2018, September 18). *Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries*. Citizen Lab. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

members of the Emirati political opposition were imprisoned for belonging to the "UAE94" movement which the UAE alleges plotted to overthrow the government[38]. In 2014, the UAE passed a comprehensive counter-terror law that provides broad legal authority for the state to act against any group deemed antagonistic to the state[39]. Influence from Islamic organizations linked to the Muslim Brotherhood has stoked fears around the monarchy losing legitimacy to religious groups, and as such, a plethora of NGOs have been designated as terrorist groups in the UAE. The willingness of the Emirati government to sentence political dissidents to lengthy prison sentences or even death has demonstrated the willingness of the state to use whatever means are available to suppress internal threats. This counter-terror justification has also been used against human rights advocates, including the notable case of well-known activist Ahmed Mansoor. Mansoor was sentenced on two separate occasions for his usage of social media platforms to call for internal reform within the UAE, and his second trial has resulted in a 15-year prison sentence[40]. Similar to Saudi Arabia, the UAE has turned towards spyware tools like Pegasus to enforce state authority across digital realms.

Pegasus has also been utilized to target actors outside of domestic boundaries, with the UAE and Saudi Arabia allegedly perpetrating a hacking campaign against Al-Jazeera journalists[41]. The Qatari-based news organization has often run stories critical of the Saudi and Emirati governments, and an attack like this could allow for further infiltration into the constructivist

---

[38]Amnesty International. (2021, July 2). *UAE: Nearly a decade of unjust imprisonment for 'UAE 94' dissidents*. https://www.amnesty.org/en/latest/news/2021/07/uae-nearly-a-decade-of-unjust-imprisonment-for-uae-94-dissidents-2/

[39]Human Rights Watch. (2014, December 4). *UAE: Terrorism law threatens lives, liberty*. https://www.hrw.org/news/2014/12/04/uae-terrorism-law-threatens-lives-liberty

[40]Human Rights Watch. (2025, March 7). UAE: Ahmed Mansoor's 15-Year Sentence Upheld. https://www.hrw.org/news/2025/03/07/uae-ahmed-mansoors-15-year-sentence-upheld

[41]Business & Human Rights Resource Centre. (2021, July 18). *Al Jazeera journalists allegedly hacked using NSO Group spyware*. https://www.business-humanrights.org/en/latest-news/al-jazeera-journalists-allegedly-hacked-using-nso-group-spyware/

feedback loop that builds international condemnation towards authoritarian regimes. The Al-Jazeera attack showcases the difficulty of attribution back to the user of Pegasus, as substantial technical analysis is needed to detect a Pegasus attack, and directly attributing the attack to a state actor is nearly impossible. As Gulf states have sought to grow their soft power in the 21st century, promoting an image of a domestically stable political situation is essential for building claims of international legitimacy and attracting foreign partnerships[42]. The role of Saudi Arabia as the new state representative of Sunni Islam grants considerable ideational power, but requires legitimacy as a state that is both stable and a model for other Muslim nations. Pegasus has provided a critical tool for Saudi Arabia and the UAE to manage domestic political opposition and monitor external critics. The growth of online political organizations by opposition figures has emerged as a trend from the Arab Spring, and has been solidified by heavy state repression against protest movements. In response, the UAE and Saudi Arabia have turned to digital tools as the next step in ensuring normative security against perceived threats by human rights advocates, hostile foreign states, and the international media.

Case Study 2: **Artificial Intelligence**

Technology has always played a central role in the progression of military affairs, and some technologies can shift the paradigm of the international security environment entirely. Artificial Intelligence has the potential to revolutionize military capabilities across the world and is a key field of international competition between states. The ongoing war between Ukraine and Russia has shown the potential for AI to act as a supportive element of military operations, and continued adaptation further enhances the ability of states to perform complex data-heavy tasks

[42] Gökalp, D. (2020). The UAE's humanitarian diplomacy: Claiming state sovereignty, regional leverage and international recognition. *CMI working paper*.

like ISR and air defense[43]. The war in Gaza has shown a similar progression, as the IDF has heavily relied upon AI software to assist in accelerating the speed of translating intelligence collection into targeting information.

Subheading 2.1: Lavender

The IDF has implemented numerous AI systems during the recent invasion of Gaza, with Lavender being the most consequential. Lavender is a program that seeks to overcome the human bottleneck in intelligence collection through AI automation. The massive ISR network used by Israel during the war and prior to it provides immense amounts of data that are traditionally analyzed by humans to produce actionable intelligence. The sheer scale of the available information leads to the human role in analysis being the primary limiting factor towards faster decision making[44]. Lavender allows for an accelerated targeting process, at the cost of accuracy[45]. When coupled with precision weapons, this means that targets of opportunity can be struck at a greater rate, and especially in the early months of the war, this system was key to Israeli operational planning. The relative immaturity of Lavender as a system has led to significant criticism of it as a source of excessive civilian casualties in the war, and the usage of AI in target generation raises considerable ethical and legal concerns[46]. Despite these challenges,

[43] Bondar, K. (2024). *Understanding the Military AI Ecosystem of Ukraine*. Center for Strategic and International Studies (CSIS).
[44] Sylvia, N. O. A. H. (2024). The Israel Defense Forces' Use of AI in Gaza: A Case of Misplaced Purpose. Royal United Services Institute (RUSI).

[45]Dan, Y. (2024, April 3). *'Lavender': The AI machine that directed a large part of the assassination bombings in Gaza*. +972 Magazine. https://www.972mag.com/lavender-ai-israeli-army-gaza/

[46]United Nations. (2024, June 10). *COI report: Detailed findings on military operations in the OPT (10 Jun 2024)*. https://www.un.org/unispal/document/coi-report-detailed-findings-on-military-operations-in-opt-10jun24/

Israeli usage of AI systems may serve as an example for the capacity of advanced software to provide security benefits within the Middle East.

Subheading 2.2: Saudi and Emirati AI Strategy

The Gulf states have looked towards AI as a means for economic diversification away from export-driven hydrocarbon economies. The ambitious Vision 2030 set of policy goals set forth by Saudi Crown Prince Mohammed bin Salman in 2016 outlines AI as a key area for driving economic growth within the kingdom[47]. Saudi Arabia has instituted numerous talent development programs that aim to foster a globally competitive Saudi tech sector, and considerable effort has been put into developing an entrepreneurial ecosystem. The Saudi Data and Artificial Intelligence Authority was formed as a government body dedicated to achieving the lofty goals of Vision 2030, and considerable progress has been made in integrating AI into Saudi educational and economic spheres[48]. The massive financial capital gained from oil exports has facilitated an accelerated development of the Saudi AI sector. Alongside economic goals, Vision 2030 aims to localize 50% of Saudi defense spending and greatly enhance the domestic arms industry.

Foreign firms have been critical in the development of the Saudi tech sector, and a 2025 deal brokered by President Trump between NVIDIA and the kingdom is set to bring in substantial capital and technical expertise[49]. American defense firms like Teledyne have moved to set up

[47] Memish, Z. A., Altuwaijri, M. M., Almoeen, A. H., & Enani, S. M. (2021). The Saudi Data & Artificial Intelligence Authority (SDAIA) vision: leading the kingdom's journey toward global leadership. *Journal of epidemiology and global health*, *11*(2), 140-142.
[48] Elhajji, M., Alsayyari, A. S., & Alblawi, A. (2020, March). Towards an artificial intelligence strategy for higher education in Saudi Arabia. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-7). IEEE.
[49] NVIDIA. (2024, June 3). *Saudi Arabia and NVIDIA to build AI factories to power the next wave of intelligence for the age of reasoning*. NVIDIA News.

regional headquarters in Riyadh, furthering collaboration between American and Saudi industries[50]. A majority of these efforts focus on dual-use technology that can be easily translated into military capability. The mercurial nature of AI as a technology allows for software that can be adapted outside of its original use case and into a security-focused application. AI technology works mutually with a variety of military mission sets, and holds particular promise for cyber and UAV-related capabilities[51].

The UAE has also invested significantly in developing a domestic AI ecosystem, and the UAE Strategy for Artificial Intelligence 2031 outlines ambitious goals focused on turning Abu Dhabi into a globally significant AI hub[52]. The state-owned defense conglomerate EDGE Group has outlined AI-integrated capabilities as a core goal in future products, and significant foreign investment has accelerated this progression[53]. EDGE has made direct investments into Israeli defense firms with a 2025 venture to purchase a thirty per cent stake in Thirdeye Systems[54]. A 2021 agreement between Israel Aerospace Industries and EDGE to develop counter-UAS capabilities marked a critical step in the integration of the Israeli and Emirati defense industries[55]. Under the Abraham Accords framework, defense cooperation has served to facilitate

---

https://nvidianews.nvidia.com/news/saudi-arabia-and-nvidia-to-build-ai-factories-to-power-next-wave-of-intelligence-for-the-age-of-reasoning

[50]Teledyne FLIR Defense. (2023, December 12). Teledyne FLIR Defense names Riyadh-based managing director for Middle East and North Africa. Teledyne FLIR Defense News. https://defense.flir.com/about/news/teledyne-flir-defense-names-riyadh-based-managing-director-for-middle-east-and-north-africa/

[51]Omer, N. (2025, March 18). AI As a Force Multiplier in the Middle East Defense Systems. Innov8 (Kurdistan Innovation and Technology Organization). https://innov8.krd/2714

[52]United Arab Emirates, Cabinet of Ministers. (2017). *UAE National Strategy for Artificial Intelligence 2031*. Mohamed bin Zayed University of Artificial Intelligence. Retrieved December 3, 2025, from https://staticcdn.mbzuai.ac.ae/mbzuaiwpprd01/2022/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf

[53]EDGE Group. (n.d.). Technology & innovation. Retrieved December 3, 2025, from https://edgegroupuae.com/technology-innovation

[54]The Media Line Staff. (2024, May 22). *UAE's EDGE acquires stake in Israeli firm to boost drone detection technology*. The Media Line. https://themedialine.org/headlines/uaes-edge-acquires-stake-in-israeli-firm-to-boost-drone-detection-technology/

[55]Israel Aerospace Industries (IAI). (n.d.). Strategic agreement between EDGE and IAI. Retrieved December 3, 2025, from https://www.iai.co.il/strategic-agreement-between-edge-and-iai

general normalization of the Israeli-Emirati partnership, and future cooperation between Israeli and Emirati firms is set to continue[56]. Programs that involve joint development and technology transfers are particularly beneficial for enhanced cooperation and set a precedent for greater future integration. AI-based cooperation is particularly mutually beneficial, as it links the human capital-rich Israeli tech ecosystem with Emirati venture capital. Collaboration between the Israeli and Emirati industry has linked the two states' innovation ecosystems and set the stage for future cooperation[57].

Discussion

Israel is uniquely positioned to provide digitally based security capabilities to Gulf States. While the US has been the traditional security provider in the region, a renewed focus on domestic issues and great-power competition has begun a trend towards withdrawal[58]. Israel is not only a world leader in military technology capable of matching the quality of American arms, particularly in the software domain, but it also holds a very strong strategic interest in balancing against Iran through alliance formation. The battle-tested nature of Israeli systems and personnel further increases their competitiveness in the international market. Israel holds a regionally unique tech ecosystem wherein military service is easily translated into entrepreneurial capital, and the continuous conflict seen in the past three years against both Iran and NSA threats is likely to further enhance this process. As partnerships between the Israeli and Saudi/Emirati defense bases grow under a renewed push for enhanced realist power, evidenced by policy

[56]Warrick, K. (2022, November 7). Israel-UAE Defense Cooperation Grows Under the Abraham Accords. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/israel-uae-defense-cooperation-grows-under-abraham-accords
[57]Zitser, J. (2023, May 7). Israeli start-up secures $22m to develop AI-powered drone detection technology. The Jerusalem Post. https://www.jpost.com/business-and-innovation/article-742509
[58] Military Times. (2025, October 1). US military starts drawing down mission in Iraq, officials say. https://www.militarytimes.com/news/pentagon-congress/2025/10/01/us-military-starts-drawing-down-mission-in-iraq-officials-say/

frameworks like Vision 2030, this process will quietly build strong security linkages between the involved states.

The sale of Pegasus from an Israeli firm to Arab states represents a consequential shift towards cooperation in the relationship between Israel and other Middle Eastern states. While NSO Group is a private entity, it is heavily regulated by the Israeli government and holds close ties to Israeli intelligence. Public purchases of a product from this kind of firm would face considerable backlash among the citizens of Arab states. The covert nature of these spyware sales has acted as a normative bypass that overcomes public outrage towards government action through secrecy, allowing for closer ties to be forged between states that are unable to form traditional alliances due to constructivist constraints. Constructivist theory argues that state behavior is heavily influenced by reciprocal feedback loops driven by social interaction. These feedback loops are able to transmit public outrage into modifications of state behavior, even in non-democratic states, as elites are concurrently influenced through the same cycle. Arms sales are a cornerstone of Israeli foreign policy, but the ability for this process to occur within the Middle East has been historically limited[59]. When the normalization process accelerated in the 2010s, Saudi Arabia saw considerable public backlash over leaked plans to form concrete ties with Israel[60]. The covert sale of Pegasus allowed for the two states' intelligence apparatuses to begin forming linkages, without facing backlash. This level of linkage in the intelligence sphere is historically significant and represents the start of a trend towards stronger security ties outside of traditional alliance structures. Given the significant setbacks faced by the Abraham Accords after the Israeli

[59] Salman, Y. (2025). Light unto the Nations Through Arms Sales: Israel's Arms Diplomacy Goals, Achievements, and Limitations. *Contemporary Review of the Middle East*, *12*(2), 209-229.
[60]The New Arab Staff. (2024, May 29). Saudi Arabia plans official ties with Israel, leaked document suggests. The New Arab. https://www.newarab.com/news/saudi-arabia-plans-official-ties-israel-leaked-document

invasion of Gaza, this mechanism holds renewed importance as it provides a pathway for cooperation that is largely immune to domestic concerns in Arab States around Israel. Pegasus was particularly well-suited for this process as it simultaneously allowed for an enhanced ability to police internal dissent while building bridges with Israel. Pegasus represents the ideal choice for building security linkages as it provides a strong material benefit that is not attached to the severe normative costs of traditional military acquisitions. These factors made it a rational choice within Arab leaders' cost-benefit analyses, as it was capable of achieving gains in two key strategic areas simultaneously without normative blowback.

While Pegasus provided some external security through enhanced intelligence collection capabilities, burgeoning cooperation in the field of artificial intelligence acts as a linkage mechanism between Israeli and Gulf State security. Sales of Pegasus acted as proof of concept for further defense-industrial base cooperation centered around security-oriented software purchases. The effectiveness of Pegasus and the willingness of the Israeli state to allow unrestricted use of it by Arab States built crucial trust between actors regarding future partnerships. Building on the nascent partnerships and lines of communication provided by Pegasus, Arab states are now developing deeper security partnerships with Israel based around AI. While many of the deals made in this area are public, the technical complexity of the product and dual-use capabilities inherent to this field of technology maintain a veil that obfuscates the strategic depth of the agreements from public eyes. AI is a powerful tool for gaining a qualitative edge, and the security threats faced by Middle Eastern states are particularly ripe use cases for AI. The risk of total war between militarily equivalent states in the Middle East remains low, with non-state actors and long-range strikes being the primary tools used by Iran to target both

Israel and Gulf States. The most mature current application of AI to the military field is to enhance intelligence processing, which is a critical step in both counter-terror and missile defense areas, both of which face time-sensitive target discrimination challenges[61]. AI is also emerging as a powerful tool in military training, potentially granting untested Arab forces access to realistic training scenarios, particularly in the air domain[62]. AI is positioned to be a critical capability in modern military strategy and holds equally important sway in the civilian economic sphere. This importance furthers the ability of AI to be used as an instrument for quietly building ties, as its perceived necessity lessens the normative costs associated with Arab-Israeli partnership. The escalating depth of AI-focused ties demonstrates the ability of covert digital security partnerships to enable high-end cooperation between states, in a process that occurs largely outside the bounds of traditional theoretical approaches.

The case studies of Pegasus and AI Cooperation demonstrate the need to build scholastically eclectic international relations theories to account for the impact of complex geopolitical developments and the changes to the international system caused by emerging technologies. When used alone, both Neoclassical Realism and Constructivism hold little explanatory power for the relationships described in both cases. Much of the scholarly backbone of traditional theories was formed based on analysis conducted during the bipolar moment of the 20th century, and holds decreasing relevance in the 21st century. The intersection of digital communication and normative cycles showcased by events like the Arab Spring demonstrates the continued relevance of constructivism, but constructivist analysis holds limited predictive power.

---

[61] Bovet Emanuel, P. (2025). *Exploring Decision Advantages: Improving Speed, Precision and Efficiency inMilitary Targeting by Applying Artificial Intelligence* (Doctoral dissertation, Försvarshögskolan (FHS)).
[62]Helsing. (2024, June 14). Helsing AI agent successfully completes Saab Gripen E test flight. Helsing Newsroom. https://helsing.ai/newsroom/helsing-ai-agent-successfully-completes-saab-gripen-e-test-flight

Coalescing different schools of thought may reduce parsimony, but it is necessary for confronting the heterogeneous causal layers currently driving international politics. The existence of a normative bypass mechanism formed by covert security partnerships based around cooperation and sales of security-oriented software represents a significant addition to the analysis of Arab-Israeli relations. Bridging these theoretical gaps provides a way by which the complex and multi-level security landscape of the Middle-East, in which normative issues coalesce with threats posed by hostile state and non-state actors to drive state behavior. Technology is a critical, yet overlooked variable, that has served to build Realist power while overcoming normative processes that impact the legitimacy of Arab leaders. Contemporary alliance formation has begun to occur in a far more irregular manner than the clear alignments of the Cold War, and theoretical eclecticism provides a bridge by which theory can remain relevant in a rapidly changing international landscape.

Conclusion

In the case of alliance formation between Israel and Arab states, traditional theories are woefully inadequate in accurately explaining the nature of the partnerships that exist and are being formed. The integration of domestic politics into the framework of Neoclassical Realism and analyses like the Two-Level Game is a valuable starting point, but constructivism and regional studies approaches are still needed for a complete analysis. In this case, software acts as the instrument that simultaneously bridges Realist external threats with normative loops affecting leaders' decision-making. Alliance formation occurs in a largely covert manner alien to traditional theories regarding state cooperation, and exists within a complex nexus of history, power, and technology. The central argument of this paper is that covert digital security

partnerships, specifically the sale of Pegasus and developing cooperation in the field of AI, serve as a mechanism to overcome significant normative constraints. This process allows for linkage to advance within an irregular process poorly explained by traditional frameworks of alliance formation.

The enhanced explanatory power gained through a synthesis of neoclassical realism and constructivist logic allows for better understanding of Arab-Israeli relations in the 21st century. The core realist logic of power maximization and balancing behavior against the shared threat posed by Iran remains true, but exists within a normative ecosystem that affects the rational choice calculations made by leaders. Given that foreign policy choices are mediated through a field of normative concerns, the costs imposed on Arab states through cooperation with Israel are particularly high. The non-attributable and classified nature of covert digital security partnerships forms a normative bypass mechanism through which quiet alliance formation takes place. Sales of spyware like Pegasus have built a foundation for security partnerships between Israel and partner states, given the unique capability provided by Pegasus to police the domestic normative cycle being highly valued by Arab States. Burgeoning partnerships in the field of AI further this process by linking tech-ecosystems between states and providing a qualitative military advantage against external threats. The dual-use nature of complex AI infrastructure obfuscates the depth of these partnerships and helps guard against normative blowback.

The escalating depth of ties between Israel and Arab States despite roadblocks in the Abraham Accords process caused by Israeli conduct in Palestine demonstrates the complex nature of alliance formation in Arab-Israeli relations. In lieu of traditional diplomatic approaches that have

been made difficult due to normative backlash against them, quiet security partnerships have progressed in a unique manner driven by advanced technology. While the Middle East serves as an excellent case study for this process, it is one that is happening across the world. Global security linkages are becoming increasingly complex and multi-dimensional, and are doing so rapidly. Further research is essential to developing a theoretical understanding of how alliances are being formed in the digital age. Scholars must embrace more eclectic approaches to confront the reality of the modern world. In a world where weapons can be a subscription, and AI picks where bombs are dropped, the traditional schools of international relations theory are simply too myopic and segmented to produce accurate results.

References

Abraham, Y. (2024, April 3). ‘Lavender’: The AI machine that directed a large part of the assassination bombings in Gaza. +972 Magazine. https://www.972mag.com/lavender-ai-israeli-army-gaza/

Afrose, S. (2025). Algorithmic Surveillance and Digital Occupation: Pegasus Spyware and Artificial Intelligence Targeting Systems in Kashmir and Palestine.

Al Naimi, S. M. (2022). Economic diversification trends in the Gulf: The case of Saudi Arabia. Circular Economy and Sustainability, 2(1), 221-230.

Amnesty International. (2021, July 18). The Pegasus Project. https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

Amnesty International. (2021, July 2). UAE: Nearly a decade of unjust imprisonment for 'UAE 94' dissidents. https://www.amnesty.org/en/latest/news/2021/07/uae-nearly-a-decade-of-unjust-imprisonment-for-uae-94-dissidents-2/

Amnesty International. (2025, February 6). Saudi woman imprisoned for tweeting in support of women's rights released after four-year ordeal. https://www.amnesty.org/en/latest/news/2025/02/saudi-woman-imprisoned-for-tweeting-in-support-of-womens-rights-released-after-four-year-ordeal/

Benchemsi, A. (2012). Morocco: Outfoxing the opposition. Journal of democracy, 23(1), 57-69.

Bents, E. R. (1995). The Sale Of US Military Aircraft to Saudi Arabia (No. AFITCICIA95009).

Bergman, R., & Mazzetti, M. (2022). The battle for the world’s most powerful cyberweapon. The New York Times Magazine, 28.

Bondar, K. (2024). Understanding the Military AI Ecosystem of Ukraine. Center for Strategic and International Studies (CSIS).

Bovet Emanuel, P. (2025). Exploring Decision Advantages: Improving Speed, Precision and Efficiency inMilitary Targeting by Applying Artificial Intelligence (Doctoral dissertation, Försvarshögskolan (FHS)).

Breznitz, D. (2002). The military as a public space: the role of the IDF in the Israeli Software Innovation System (pp. 130-48). Samuel Neaman Institute for Advanced Studies in Science and Technology.

Business & Human Rights Resource Centre. (2021, July 18). Al Jazeera journalists allegedly hacked using NSO Group spyware. https://www.business-humanrights.org/en/latest-news/al-jazeera-journalists-allegedly-hacked-using-nso-group-spyware/

Dana, T. (2023). The new (dis) order: The evolving UAE-Israel security alliance. Journal of Palestine Studies, 52(3), 62-68.

Darwich, M. (2022). The view from Riyadh: A neoclassical realist perspective of Saudi foreign policy towards Iran in the post-2011 Middle East. In Saudi Arabia and Iran (pp. 14-32). Manchester University Press.

DeVore, M. R. (2012). Exploring the Iran-Hezbollah relationship: A case study of how state sponsorship affects terrorist group decision-making. Perspectives on terrorism, 6(4/5), 85-107.

EDGE Group. (n.d.). Technology & innovation. Retrieved December 3, 2025, from https://edgegroupuae.com/technology-innovation

Elhajji, M., Alsayyari, A. S., & Alblawi, A. (2020, March). Towards an artificial intelligence strategy for higher education in Saudi Arabia. In 2020 3rd International Conference on Computer Applications & Information Security (ICCAIS) (pp. 1-7). IEEE.

Galal, A. (2023). Mapping the supply of surveillance technologies to Africa Morocco country report. Editor: Tony Roberts.

Gause, F. G. (2016). The Future of US-Saudi relations: The kingdom and the power. Foreign Affairs, 95(4), 114-126.

Gökalp, D. (2020). The UAE's humanitarian diplomacy: Claiming state sovereignty, regional leverage and international recognition. CMI working paper.

Gusterson, H. (2024). It's all Lavender in Gaza. Anthropology Today, 40(6), 1-2.

Helsing. (2024, June 14). Helsing AI agent successfully completes Saab Gripen E test flight. Helsing Newsroom. https://helsing.ai/newsroom/helsing-ai-agent-successfully-completes-saab-gripen-e-test-flight

Human Rights Watch. (2014, December 4). UAE: Terrorism law threatens lives, liberty. https://www.hrw.org/news/2014/12/04/uae-terrorism-law-threatens-lives-liberty

Human Rights Watch. (2025, March 7). UAE: Ahmed Mansoor's 15-Year Sentence Upheld. https://www.hrw.org/news/2025/03/07/uae-ahmed-mansoors-15-year-sentence-upheld

Israel Aerospace Industries (IAI). (n.d.). Strategic agreement between EDGE and IAI. Retrieved December 3, 2025, from https://www.iai.co.il/strategic-agreement-between-edge-and-iai

Johnston, T., Lane, M., Casey, A., Williams, H. J., Rhoades, A. L., Sladden, J., ... & Haberman, R. (2020). Could the Houthis be the next Hizballah Iranian proxy development in Yemen and the future of the Houthi movement (No. RR2551).

Kamrava, M. (2012). The Arab Spring and the Saudi-led counterrevolution. Orbis, 56(1), 96-104.

Kareem, K. (2024). A comprehensive analysis of pegasus spyware and its implications for digital privacy and security. arXiv preprint arXiv:2404.19677.

Katzenstein, P. J. (Ed.). (1996). The culture of national security: Norms and identity in world politics. Columbia University Press.

Marczak, B., Anstis, S., Crete-Nishihata, M., Scott-Railton, J., & Deibert, R. (2020). Stopping the press: New york times journalist targeted by saudi-linked pegasus spyware operator.

Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018). Hide and seek: Tracking NSO group's Pegasus spyware to operations in 45 countries.

Matthiesen, T. (2014). The Local and the Transnational in the Arab Uprisings. The Protests in Saudi Arabia's Eastern Province. The Silent Revolution: The Arab Spring and the Gulf States, 105-143.

Memish, Z. A., Altuwaijri, M. M., Almoeen, A. H., & Enani, S. M. (2021). The Saudi Data & Artificial Intelligence Authority (SDAIA) vision: leading the kingdom's journey toward global leadership. Journal of epidemiology and global health, 11(2), 140-142.

Military Times. (2025, October 1). US military starts drawing down mission in Iraq, officials say. https://www.militarytimes.com/news/pentagon-congress/2025/10/01/us-military-starts-drawing-down-mission-in-iraq-officials-say/

Monshipouri, M., Dorraj, M., & Fields, J. (2025). The Gaza War and the Future Of the Abraham Accords. Middle East Policy.

Morsy, A. (2019). Alliances and Threats in the Middle East: Neoclassical Realism and the Balance of Interest. POMEPS Studies 34: Shifting Global Politics and the Middle East, 81-85.

Munck, R., & Pozzi, P. (2019). Israel, Palestine, and Latin America: Conflictual Relationships. Latin American Perspectives, 46(3), 4-12.

Nassar, Y. (2024). Israel's War on Gaza. Al-Muntaqa: New Perspectives on Arab Studies, 7(2), 111-123.

NVIDIA. (2024, June 3). Saudi Arabia and NVIDIA to build AI factories to power the next wave of intelligence for the age of reasoning. NVIDIA News. https://nvidianews.nvidia.com/news/saudi-arabia-and-nvidia-to-build-ai-factories-to-power-next-wave-of-intelligence-for-the-age-of-reasoning

Offenhauer, P. (2008). Israel's Technology Sector.

Omer, N. (2025, March 18). AI As a Force Multiplier in the Middle East Defense Systems. Innov8 (Kurdistan Innovation and Technology Organization). https://innov8.krd/2714

Ottaway, D. (2009). The King and us: US-Saudi relations in the wake of 9/11. Foreign Aff., 88, 121.

Putnam, R. D. (2017). Diplomacy and domestic politics: the logic of two-level games. In International organization (pp. 437-470). Routledge.

Rakipoğlu, M. (2017). Revisiting the saudi position during the Iran-Iraq war through the lens of balance of threat theory. Ortadoğu Etütleri, 9(1), 118-134.

Rose, G. (1998). Neoclassical realism and theories of foreign policy. World politics, 51(1), 144-172.

Rousseau, J. P. (2017). The history and impact of unit 8200 on Israeli hi-tech entrepreneurship (Bachelor's thesis, Ohio University).

Salman, Y. (2025). Light unto the Nations Through Arms Sales: Israel's Arms Diplomacy Goals, Achievements, and Limitations. Contemporary Review of the Middle East, 12(2), 209-229.

Schweller, R. L. (2014). Unanswered threats: A neoclassical realist theory of underbalancing. In The Realism Reader (pp. 265-271). Routledge.

Scott-Railton, A., Marczak, B., Razzak, N. A., Deibert, R., & Crete-Nishihata, M. (2018, September 18). Hide and seek: Tracking NSO Group's Pegasus spyware to operations in 45 countries. Citizen Lab. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Smith, C., & Knights, M. (2025). How Iran aligned militias seized Iraq: irregular warfare, lawfare and regime change. Small Wars & Insurgencies, 36(4), 659-697.

Sylvia, N. O. A. H. (2024). The Israel Defense Forces' Use of AI in Gaza: A Case of Misplaced Purpose. Royal United Services Institute (RUSI).

Teledyne FLIR Defense. (2023, December 12). Teledyne FLIR Defense names Riyadh-based managing director for Middle East and North Africa. Teledyne FLIR Defense News. https://defense.flir.com/about/news/teledyne-flir-defense-names-riyadh-based-managing-director-for-middle-east-and-north-africa/

The Media Line Staff. (2024, May 22). UAE's EDGE acquires stake in Israeli firm to boost drone detection technology. The Media Line. https://themedialine.org/headlines/uaes-edge-acquires-stake-in-israeli-firm-to-boost-drone-detection-technology/

The New Arab Staff. (2024, May 29). Saudi Arabia plans official ties with Israel, leaked document suggests. The New Arab. https://www.newarab.com/news/saudi-arabia-plans-official-ties-israel-leaked-document

United Arab Emirates, Cabinet of Ministers. (2017). UAE National Strategy for Artificial Intelligence 2031. Mohamed bin Zayed University of Artificial Intelligence. Retrieved December 3, 2025, from https://staticcdn.mbzuai.ac.ae/mbzuaiwpprd01/2022/07/UAE-National-Strategy-for-Artificial-Intelligence-2031.pdf

United Nations. (2024, June 10). COI report: Detailed findings on military operations in the OPT (10 Jun 2024). https://www.un.org/unispal/document/coi-report-detailed-findings-on-military-operations-in-opt-10jun24/

Walt, S. M. (1985). Alliance Formation and the Balance of World Power. International Security, 9(4), 3–43. https://doi.org/10.2307/2538540

Warrick, K. (2022, November 7). Israel-UAE Defense Cooperation Grows Under the Abraham Accord. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/israel-uae-defense-cooperation-grows-under-abraham-accord

Warrick, K. (2022, November 7). Israel-UAE Defense Cooperation Grows Under the Abraham Accords. The Washington Institute for Near East Policy. https://www.washingtoninstitute.org/policy-analysis/israel-uae-defense-cooperation-grows-under-abraham-accords

Wendt, A. (1992). Anarchy is what states make of it: the social construction of power politics. International organization, 46(2), 391-425.

Zitser, J. (2023, May 7). Israeli start-up secures $22m to develop AI-powered drone detection technology. The Jerusalem Post. https://www.jpost.com/business-and-innovation/article-742509