

#08

September 2025

Emerging Defence Technologies in the Middle East: Strategic Implications and Regional Security Dynamics

Sara Bazoobandi

DIGITAL
COOPERATION
WITH GLOBAL PARTNERS
POLICY
STUDY

G I G A

German Institute for Global and Area Studies
Leibniz-Institut für Globale und Regionale Studien

Author

Dr. Sara Bazoobandi is a Research Fellow at the GIGA and non-resident fellow at the Institute for Security Policy at Kiel University, the Italian Institute for International Political Studies, and the Arab Gulf States Institute. Her research focuses on political economy, emerging defence technologies, and artificial intelligence governance in the Middle East.

About the Digital Transformation Lab (DigiTraL)

GIGA's Digital Transformation Lab (DigiTraL) is funded by the Federal Foreign Office and analyses the political drivers and real-world consequences of the digital transformation taking place around the world. The Global South in particular is an important actor in and shaper of this transformation. In the first phase (2021-2023) of the project, the focus was on digital diplomacy and on analysing the question of what new opportunities, challenges and instruments the digital transformation offers for German foreign policy. The second phase (2024-2025) concentrates on analysing the opportunities that digitalisation offers for Germany's cooperation with global partners. Central questions include: Where do individual countries and regions in the Global South stand with regards to digitalization? Where are the points of contact for (tech) partnerships with Germany? Where are new developments arising (e.g. emerging threats from digital disinformation, related reactions, and interventions in the Global South)? What cooperative relationships exist in the field of digitalization in the Global South, and how can the German government and other actors in Germany best respond to this? The current phase of DigiTraL is headed by Dr. Iris Wiczorek, Senior Research Fellow at the GIGA Institute for Asian Studies.

For more information, please have a look [here](#).

Emerging Defence Technologies in the Middle East: Strategic Implications and Regional Security Dynamics

Sara Bazoobandi

Abstract

The recent conflicts in Ukraine and the Middle East have starkly demonstrated that modern warfare demands digital transformation. As Ukrainian officials warned, in modern-day conflicts countries must “digitise or die.” This imperative resonates across the Middle East, where regional powers are each pursuing their own distinct models of technological transformation. This policy study examines how emerging defence technologies are fundamentally reshaping strategic dynamics and security architectures across the Middle East, with particular focus on the pursuit of technological sovereignty by Iran, Turkey, Saudi Arabia, and the United Arab Emirates. Three key domains are analysed: drone warfare evolution; artificial intelligence integration; and, cyberwarfare capabilities. Demonstrated is how these developments are transforming traditional power balances and military doctrines. Regional powers are transitioning from foreign military dependency to indigenous production capabilities by taking distinct strategic approaches. The proliferation of autonomous weapon systems (AWS), AI-enhanced cyber operations, and modular drone technologies has changed the defining factors for “military capabilities,” enabling both state and non-state actors to project power at unprecedented speed. These developments are creating new both competition and collaboration opportunities across the region. As regards European security interests, strategic challenges and opportunities are respectively identified. Findings indicate that future conflicts will increasingly feature digitalised warfare and AWS integration, fundamentally altering engagement parameters and challenging international security frameworks.

Policy Recommendations

- European powers should expand and strengthen their strategic technology partnerships with Gulf states. There is substantial potential for leveraging the UAE’s EDGE Group (a state-owned, advanced-technology conglomerate) and Saudi Arabia’s SAMI (the country’s military-industries development programme) to create mutually beneficial defence-technology partnerships.
- Europe must strengthen its collective cyber defence against Iranian threats. The German government and European peers should take active measures to counter such threats through enhanced response mechanisms. The European Union needs to establish a dedicated regional cyberthreat intelligence unit to handle real-time information-sharing and joint development of AI-powered cyber defence systems. Germany’s strong cybersecurity sector positions it well to lead such an initiative.

- European states must invest in comprehensive counter-drone systems. Germany should leverage its industrial base to develop anti-swarm technologies and AI-powered air-defence systems. Modular drones have transformed the nature of warfare in Ukraine and the Middle East; European countries need similar capabilities both for defence and to maintain technological competitiveness in this realm globally.
- Iran’s reverse-engineering capabilities and technology-acquisition networks should be countered by thorough export controls on AI development tools, advanced semiconductors, and machine-learning software. This requires European coordination across all relevant industries to monitor related technology transfers.
- European states should actively engage in the field of AI with Gulf nations, particularly Saudi Arabia and the UAE, given their substantial investments in its development. Europe’s human-centric AI governance framework, emphasising transparency, accountability, and ethical deployment, provides a valuable model for Gulf states seeking to develop their own AI capabilities. European policymakers should work with regional partners through specific diplomatic channels and technical exchanges to promote AI governance frameworks that balance ethical considerations with each region’s strategic priorities.

Outline

Introduction	5
From Import Dependence to Technological Sovereignty	6
Drone Warfare Evolution: Transforming Military Doctrine	11
Software-Defined Warfare: How Technological Advancement Is Reshaping Global Military Capabilities	14
AI Ambitions: How Gulf States’ Investments Can Transform Regional Military Power	16
Cyber Arms Race: AI and Digital Warfare	17
Conclusion	20
Bibliography	21
Glossary	26

Introduction

The Middle East's strategic landscape is being fundamentally reshaped by rapid advancements in defence technologies, as regional powers increasingly invest in indigenous military capabilities to address evolving security challenges. From artificial intelligence and autonomous weapon systems (AWS) to cyberwarfare and innovative missile technologies, these emerging capabilities are altering the traditional balance of power and creating new dimensions of competition and cooperation across the region. Some of the Middle East's regional powers – namely, Iran, Turkey, Saudi Arabia, and the United Arab Emirates – have in recent years become among the most dynamic and resource-capable actors regionally, ones actively pursuing defence modernisation as instruments of influence and power projection.

The Gulf states began their efforts to develop domestic defence industries in the early years of the new century, with Saudi Arabia and the UAE leading initiatives to reduce their dependence on foreign military supplies; these two countries continuing to lead such developments. This shift reflects broader strategic visions of regional hegemony and technological sovereignty, driven by mounting security concerns amid Iran's growing influence, proxy conflicts across the region, and evolving threat landscapes. These industrialisation programmes represent both a defensive response to regional instability and a desire for offensive capabilities helping project power, positioning these nations as autonomous security actors rather than dependent clients of external powers.

Saudi Arabia and the UAE lead the Gulf Cooperation Council (GCC) states' modernisation efforts in this regard, pursuing comprehensive transformation from foreign dependence to domestic manufacturing. Both governments have initiated sizable programmes aimed at advancing self-reliance while developing industries capable of international sales, too. Iran seeks to bolster its defence capabilities through its "jihad of knowledge" doctrine, prioritising scientific innovation as regards military applications despite severe economic constraints and international sanctions (Bazoobandi 2024). Turkey leverages its NATO membership and indigenous engineering capacity to develop AWS and export-oriented defence technologies. These initiatives serve dual purposes: achieving military independence and diversifying national economies through technology-sector development, with each actor adapting to their unique geopolitical circumstances and resource constraints.

The advancements pursued here by Middle Eastern powers directly impact European security. As these technologies spread and are adopted by various actors, they risk creating new asymmetric capabilities between regional players – potentially influencing conflicts in ways that carry broader implications for Europe itself. These developments are particularly significant given the major conflict happening in Ukraine, which has demonstrated how the digitalisation of defence sectors is essential for modern military effectiveness. As Ukraine's Deputy Minister of Defence for Digital Development emphasised in early 2025, the choice facing modern militaries is clear: "Digitise or die" (Chernohorenko 2025). European manufacturers have been actively developing and refining their defence systems through real combat applications in Ukraine, while simultaneously facing supply-chain challenges as China imposed export restrictions on critical microelectronics components, particularly those used in drone technologies (Kyiv Post 2024). The Ukraine War has also accelerated the development of AWS, showcasing their transformative potential as game-changing military technologies that extend far beyond traditional applications in combat settings.

This research examines how emerging defence technologies, particularly digitalisation and AWS, are reshaping policy dynamics and security architectures across the Middle East, including as regards the development strategies underpinning this trajectory and the mechanisms by which those strategies are conceived and executed. As regional powers increasingly integrate these advanced capabilities into their military doctrines, fundamental questions arise on their implications for regional stability, power projection, and the broader international security environment. Addressed is how these technologies influence regional competition and alliance structures, as well as their prospects for altering existing power dynamics with close consideration given to the broader implications for European security calculations.

Given the rapidly evolving nature of these technologies and their proliferation across different domains, precise definition of “defence digitalisation” is essential to ensure conceptual clarity throughout. The term is defined, accordingly, as the digital transformation of military forces. This involves implementing sophisticated information technology systems, protecting communication networks, and designing intuitive operational interfaces throughout all aspects of the armed forces’ infrastructure. These foundations facilitate enhanced operational efficiency, superior decision-making capabilities, and significant competitive advantages in contemporary warfare environments.

From Import Dependence to Technological Sovereignty

Regional powers across the Middle East have embarked on ambitious programmes to establish indigenous defence-manufacturing capabilities, marking a significant shift from decades of heavy foreign military dependency. This reflects their broader aspirations to technological sovereignty, economic diversification, and enhanced regional influence amid evolving security challenges, while embodying the strategic visions of political leaders seeking to position their nations as autonomous actors. The pursuit of domestic military capabilities represents not merely a response to supply-chain vulnerabilities or sanctions regimes but also a comprehensive reimagining of national security architectures in ways prioritising self-reliance and strategic autonomy.

Iran and Turkey have historically maintained substantial military forces, reflecting their roles as major regional powers with extensive territorial boundaries and strategic geopolitical positions. Both nations have long recognised the importance of robust defence capabilities, though their approaches to military modernisation have evolved significantly over time. Iran’s defence trajectory underwent dramatic transformation following the 1979 Islamic Revolution. Prior to that, the Shah’s regime had been a major purchaser of Western military technology, with substantial arms deals including advanced fighter aircraft, naval vessels, and sophisticated weapons systems from the United States and European suppliers. The subsequent revolution and international sanctions prompted Iran to pivot towards indigenous development, ultimately establishing the foundations for today’s self-reliance doctrine. As a NATO member since 1952, Turkey, conversely, has consistently invested in defence manufacturing, traditionally balancing Western technology acquisition with the gradual development of domestic capabilities. Turkish defence modernisation accelerated significantly in the 1990s and first decade of the new century, as driven by internal security challenges, regional conflicts, and the political vision of strategic autonomy within the Western alliance framework.

Iran has prioritised self-sufficiency in defence technology. This is underpinned by the “jihad of knowledge” doctrine that systematically channels scientific advancement towards military applications. The Defence Industries Organisation, operating under the Ministry of Defence, coordinates indigenous production across multiple sectors, while the Islamic Revolutionary Guard Corps (IRGC) maintains its own research and development apparatus through organisations like the Aerospace Force and the Electronic Industries Company (EIC). Iran’s ballistic-missile programme, managed primarily by the IRGC’s Aerospace Force in collaboration with entities like Shahid Hemmat Industrial Group, has produced systems ranging from short-range Fateh missiles to intercontinental Sejil variants. The country’s drone capabilities have also evolved through the work of institutions like the Iran Aircraft Manufacturing Industrial Company and various IRGC-affiliated workshops, producing systems from those used for surveillance to armed variants like the Shahed series. Electronic warfare has become more sophisticated due to the involvement of organisations such as the EIC and academic partnerships with academic institutions like Sharif University of Technology, enabling Iran to develop its cyber capabilities and communication-disruption systems in support of both defensive postures and regional proxy operations. Notably, academics from universities in the UK, Australia, and the US have collaborated on research related to drone technology with Sharif University, despite the institution being under international financial sanctions and widely known for its close ties to Iran’s military establishment (Yerushalmy and Bhuiyan 2024).

Iran Aircraft Manufacturing Industrial Company has developed multiple domestic aircraft platforms, including passenger and cargo variants and specialised military applications, while simultaneously engaging in the extensive reverse engineering of Western fighter-aircraft components. The organisation has been particularly active in reverse engineering components from legacy American fighter jets that remain in Iranian service, including various ones from the pre-revolutionary era. It has also been involved in complex international procurement networks designed to circumvent sanctions and obtain access to Western aviation technology. These operations allegedly involved multiple intermediary companies across Asia and Europe, utilising transshipment routes through various countries to acquire restricted components that are critical for the development of indigenous technologies (Iran Watch 2022).

Turkey has emerged as a significant player in indigenous defence production, leveraging its NATO membership and strategic geographic position to develop exportable military technologies while reducing foreign dependency. Baykar, a privately-owned company, revolutionised Turkey’s drone capabilities with the TB2 and the larger Akinci systems, which have established the country as a major unmanned aerial vehicle (UAV) exporter. Azerbaijan, Indonesia, and Mali have reportedly purchased these drones to date. In 2025, Baykar acquired Piaggio Aerospace, an Italian company, where TB2 and Akinci UAVs will be produced in future (Army Recognition 2025).

ASELSAN, Turkey’s largest defence electronics company, develops radar systems, electronic-warfare equipment, and communication technologies. Founded in 1975, it went on to produce avionics for the F-16 programme in the late 1980s, participate in NATO’s Stinger missile production, and now has offices from the Balkans and Central Asia (i.e. Azerbaijan and Kazakhstan) to Jordan and GCC countries.

Turkish Aerospace Industries leads aircraft development, including the indigenous TF-X fighter-jet programme, while Roketsan specialises in missile systems and rocket technologies. The Scientific and Technological Research Council of Turkey coordinates work in this domain through its Defence Industries Research and Development Institute, fostering innovation

across academia and industry. The country’s defence exports have grown substantially of late, with collaboration extending to with the likes of Saudi Arabia through the concluding of technology-transfer agreements that bolster regional partnerships while advancing Turkey’s strategic influence.

Turkey has emerged as a global power in the field of drone production, becoming a market leader with a 37.9 per cent share thereof. This transformation occurred with remarkable speed, with the country experiencing an export surge whereby 43 of its 47 total transfers between 1995 and 2023 took place within just four years (2020–2023) (Campbell 2024).

Also striking is how the scope of Turkey’s influence extends far beyond its home region: it has supplied drone systems to more than 15 countries across four continents to date, establishing itself as an international defence supplier.

Table 1. Top Armed Drone Recipients (1995–2023)

Rank	Country	Transfers*Received	Primary Suppliers
1	United Kingdom	9	US, Turkey
2	Nigeria	7	Turkey, China
3	UAE	7	Turkey, China
4	Algeria	6	Turkey, China
5	Pakistan	5	Turkey, China
6	Saudi Arabia	5	Turkey, China
7	Ethiopia	4	Turkey
8	Kyrgyzstan	4	Turkey
9	Morocco	4	Turkey
10	Ukraine	4	Turkey

Note: * The term “transfers” refers to completed and ongoing foreign military sales, direct commercial sales, leases, gifts, and secondary proliferation. The Center for a New American Security Drone Proliferation Dataset identified 633 drone transfers between 1995 and 2023.

Source: Center for a New American Security, Drone Proliferation Dataset.

Iran and Turkey represent fundamentally different approaches to indigenous defence development, as shaped by their distinct geopolitical circumstances and respective strategic orientations. Iran’s path has been defined by international sanctions and a self-reliant model built, as noted, around the “jihad of knowledge” doctrine that requires heavy reliance on reverse engineering and sanctions-circumvention networks. Turkey’s approach, however, has been facilitated by its NATO membership and Western partnerships. The country has gradually built indigenous capabilities while maintaining access to international markets and technology-transfer opportunities. While Iran has developed sophisticated asymmetric capabilities primarily for regional influence and proxy support, Turkey has successfully created commercially viable, exportable defence technologies that enhance both its strategic autonomy and economic diversification.

In contrast to both Iran’s sanctions-driven isolation and Turkey’s alliance-based development, Saudi Arabia and the UAE represent a third model: resource-rich states utilising their vast financial capabilities to rapidly build indigenous defence industries through strategic partnerships, technology transfers, and ambitious “Vision” programmes that combine economic diversification with military modernisation. The UAE’s EDGE Group and Saudi Arabian Military

Industries (SAMI) represent the most significant entities driving defence technology development in these two countries. Both entities represent their respective governments' commitment to transforming from defence importers to indigenous producers and exporters in support of regional security objectives while diversifying away from oil dependence.

The UAE has invested heavily in developing its defence industry, focusing on advanced technologies and partnerships. By collaborating with international firms and investing in research and development, it seeks to enhance its military capabilities and reduce dependence on foreign suppliers. The country has strategically pursued partnerships with the world's leading defence-technology providers to enhance its military capabilities and regional influence.

EDGE Group, created in 2019 by merging several existing state-owned organisations including key defence entities, functions through four divisions: equipment manufacturing; weaponry development; digital-warfare technologies; and, operational-support services. EDGE has localised over 80 per cent of its 220+ products and solutions to UAE manufacturing, operating 170 facilities across Abu Dhabi while investing heavily in local suppliers to boost in-country value. HALCON, EDGE's smart-weapons subsidiary, has contributed significantly to these localisation efforts by directing over AED 100 million in orders to 26 UAE-based manufacturers (EDGE 2025). Some of the most significant technical innovations by EDGE include: the Garmoosha unmanned aircraft system, with a 120-kilogram cargo capacity over a range of 150 kilometres and with 8 hours endurance; the QX series of intelligent loitering weapons featuring AI targeting and endurance of between 1.5 hours to 16 hours (Oliver 2024); and, precision-guided Rash munitions (EDGE 2023).

As noted, the Ukrainian conflict has served as a crucial testing ground for emerging defence technologies, with unmanned ground vehicles (UGVs) like those developed by Estonia-based Milrem Robotics proving their battlefield effectiveness in real combat conditions. This operational validation has significantly influenced GCC leaders' investment decisions, as they recognise the strategic value of partnering with companies whose technologies have demonstrated combat-proven capabilities rather than theoretical R&D promises. The success of these systems in Ukraine's challenging operational environment has accelerated Gulf states' pursuit of similar technologies, driving partnerships with European firms that offer battle-tested solutions for contemporary warfare challenges.

Originally founded in Estonia, Milrem was bought in 2023 by EDGE. Together with Spain's EM&E Group (defence-technology provider) and Belgium's Thales (aerospace and cyber systems), these organisations have now formed a partnership to pursue commercial opportunities in the UAE. Their collaboration aims to combine EM&E's weapon station (SECUTOR, a remotely operated platform that can be mounted on vehicles, vessels, or stationary structures) and Thales' 70mm rocket systems with Milrem's UGVs (THEMIS), creating an enhanced platform specifically designed for UAE requirements – particularly anti-drone operations (Zawya 2025). Milrem's platforms have been deployed in Ukraine for diverse missions including cargo transport, casualty evacuation, anti-tank operations, indirect and direct fire support, intelligence-gathering, communications relay, and engineering tasks. It is worth noting that UGVs and First Person View systems are designed to maximise the effectiveness of counter-drone operations without requiring human ground forces (White 2025). Milrem has also established partnerships with Saudi Arabia's Wahaj, a precision-engineering company, as well. This strategic positioning enables both of these Middle Eastern countries to acquire battle-tested systems while establishing partnerships that enhance regional significance and defence capacity through access to operationally tested technologies (Defensehere 2024). For Europe, these

partnerships represent vital opportunities to sustain and expand their defence-related industrial base while fostering technological innovation that benefits both regional security and economic competitiveness globally.

SAMI, launched in 2017, aims to join the ranks of the world's top-25 defence manufacturers while achieving domestic production of half the kingdom's military purchases by 2030 (Astute Group 2025). The company has experienced an extraordinary expansion since its founding, rising to 98th worldwide by 2022 following a nearly 3,000 per cent growth in revenues. SAMI (2025) obtained nearly USD 2 billion in bank funding dedicated to domestic production, facility construction, and company acquisitions. Global alliances encompass partnerships with Singapore's ST Engineering for enhanced supply-chain development (Zawya 2022), collaboration with Lockheed Martin on cutting-edge defence technologies (Technical Report 2025), and an agreement with Boeing (Times Aerospace 2022) establishing a specialised company focused on helicopter maintenance and support services for Saudi military aircraft.

SAMI faces significant obstacles, including difficulty finding skilled technicians, higher costs for locally manufactured products compared to foreign alternatives, and competition from EDGE. The Saudi government has invested USD 1.4 billion in incentives to support the local defence sector (Issa 2022). Defence Minister Prince Khalid bin Salman visited Turkey in 2024 to strengthen defence ties amid regional tensions arising amid the latest Gaza War and potential expansion of the conflict in the aftermath of the Iran–Israel conflict (Arab News 2024). Saudi Arabia, the world's fifth-largest military spender, allocated 21 per cent of total government expenditure and 7.1 per cent of the country's gross domestic product to this domain in 2025 (Helou 2025). The country is seeking greater military self-sufficiency after experiencing supply-chain disruptions in the past.

The US has sporadically motivated Saudi Arabia to invest in domestic defence production and the seeking of new allies. The US halted precision-guided munitions sales to Saudi Arabia in 2016 to pressure it over its war in Yemen, highlighting the risks of foreign dependence (Stewart and Strobel 2016). In 2021, within days of his inauguration, President Joe Biden announced a halt to the sale of offensive weaponry to Saudi Arabia (Dent and Rumley 2024). Though the embargo was lifted in August 2024 with a USD 750 million weapons shipment, the experience reinforced Riyadh's need for indigenous production capabilities (Pamuk, Zengerle, and Holland 2024).

SAMI has signed three memoranda of understanding with Turkish defence companies, including Baykar and ASELSAN. These aim to: transfer indigenous defence technology to Saudi Arabia; develop drone production capabilities on Saudi soil; and, produce advanced defence technologies locally (Al Arabiya 2024). The Saudi–Turkish partnership serves multiple purposes: it demonstrates to Washington that Saudi Arabia has alternative suppliers and it is relatively non-threatening to the North American country since Turkey is a NATO member.

Saudi Arabia is also among the top-six global drone recipients (see Table 1 above), reflecting a comprehensive approach to military-capability enhancement via strategic procurement. The kingdom has pursued diversified sourcing by acquiring drone systems from both Turkey and China, demonstrating the deliberate avoidance of dependency on a single supplier while gaining access to different technologies and operational capabilities. These investments also align with the capability-building objectives outlined in "Vision 2030," Saudi Arabia's national-transformation programme that seeks to reduce oil dependency and develop indigenous defence-manufacturing capabilities as part of broader economic diversification. Furthermore, Saudi Arabia's drone acquisitions are critical to maintaining regional balance, as it strives to

counterbalance Iran's own growing drone capabilities and expanding influence in the neighbourhood. The kingdom will continue diversifying military procurement away from Western powers, prioritising partners willing to commit to local manufacturing and technology transfers. However, it will also maintain boundaries to preserve its core strategic alliance with the US (Shahbazov 2024).

Both Saudi Arabia and the UAE have appointed trusted elites to head their defence-industry conglomerates (e.g. SAMI and EDGE), formed of royal family members, tribal leaders, and high-ranking military officers. This has led, though, to corruption scandals involving active-duty officers and princes, particularly in Saudi Arabia (*The Guardian* 2024). While the two nations have made significant strides towards their desired outcomes, a number of challenges remain – including technological gaps, workforce development, and the integration of complex systems. Continued investment and international partnerships will be crucial for sustaining growth in indigenous defence capabilities.

These respective initiatives by Iran, Turkey, Saudi Arabia, and the UAE carry profound implications for both regional stability and the international security architecture. Regionally, the proliferation of advanced military capabilities is reshaping the traditional balance of power, with these nations increasingly able to project force independently and support proxy conflicts through domestically produced systems, as evidenced by Iran's drone supplies to regional allies and Turkey's UAV deployments across multiple theatres. This is serving to fragment established supplier–client relationships, in the long-run potentially reducing Western leverage over regional conflicts while creating new dynamics of technological competition and cooperation among Middle Eastern powers themselves.

Internationally, these developments challenge the traditional dominance of established defence exporters, forcing European and American manufacturers to compete with increasingly sophisticated regional alternatives that often come with fewer political strings attached. For Europe specifically, these initiatives present both opportunities and challenges: while partnerships with Gulf states – like the UAE's collaboration with Milrem – offer vital revenue streams and technological validation for European defence industries, the growing independence of regional military capabilities also reduces European influence over regional security decisions and potentially complicates conflict-resolution efforts. Moreover, the proliferation of advanced military technologies from these emerging producers to third parties could undermine European security interests globally.

Drone Warfare Evolution: Transforming Military Doctrine

Drone technology is deemed able to unleash a revolution in combat affairs, one that would affect not only military doctrine, organisation, and force but also both regional and international stability. By making long-range precision strikes more realistic, drones can eliminate close combat from the battlefield, which would relieve states from the need to deploy ground troops (Hammes 2013). Drones have lowered the entry barrier for acquiring and employing advanced military capabilities, enabling both state and non-state actors to produce or purchase them with relative ease (Calcara et al. 2022). Small nations can now develop indigenous drone programmes or procure sophisticated systems from major suppliers, while non-state groups in-

cluding terrorist organisations, insurgent movements, and even criminal cartels have demonstrated their ability to weaponise commercial drones or acquire military-grade systems through various channels (HOZINT 2021).

Ukraine’s rapid expansion of drone manufacturing during its conflict with Russia, Iran’s provision of Shahed drones both to the latter and to various proxy groups, Ansar Allah in Yemen using drones to attack shipping in the Red Sea, and Islamic State of Iraq and the Levant’s early adoption of commercially available quadcopters for surveillance and attack are all vivid examples of how drone technology has shifted the traditional frameworks of military power and capability distribution. Against this backdrop, the historical links between wealth and power in the international order might be weakened or disrupted by the advancement of drone technology, as asymmetric capabilities become more accessible to a broader range of actors regardless of their financial status or industrial base. The development and deployment of drones technology carry dramatically lower financial and human costs, make it more politically feasible for states to “keep shooting forever,” and thereby threaten enduring peace and stability worldwide (Zegart 2021).

With this advancement, forward deployments of troops and hardware capabilities will become increasingly vulnerable, and all states will have to restructure their armed forces away from expensive and complex military platforms in favour of new, less sophisticated, and cheaper drone technologies. This shift represents a fundamental aspect of defence digitalisation, as focused on the integration of related technologies, AWS, and network capabilities into military operations. It is therefore not surprising that state efforts to develop defence technology in countries like Iran, Turkey, and the UAE are largely focused on drone technology (see Table 2 below). Such efforts clearly demonstrate these nations’ understanding of the critical value of investing in unmanned systems. For them, drones represent both an accessible entry point into advanced military technology and a means of projecting power that aligns with the digital transformation of modern warfare.

Table 2. Global Armed Drone Suppliers Ranking (1995–2023)

Rank	Country	Total Transfers	Market Share (%)
1	Turkey	47	37.9
2	China	34	27.4
3	United States	12	9.7
4	Iran	8	6.5
5	Israel	6	4.8
6	South Africa	3	2.4
7	UAE	3	2.4
8	Belarus	1	0.8
9	Russia	1	0.8

Source: Center for a New American Security, Drone Proliferation Dataset.

Although drones do not automatically provide offensive superiority, they are increasingly considered a “poor man’s air force” (Waters 2018). Their effectiveness depends heavily on the

enemy's air-defence capabilities and operator skill levels. Rather than empowering weaker actors, drones actually favour stronger, well-resourced forces that can provide necessary support systems (radar, communications, and similar) (Calcara et al. 2022). Many analysts and policymakers have sought to assess whether armed drones can shift the offence–defence balance in the air. The rapid global advancement and proliferation of autonomous and semi-autonomous drone systems has fundamentally altered the landscape of modern warfare, creating a paradigm shift that challenges traditional military doctrines. This technological revolution has been particularly pronounced in regional conflicts, where nations like Iran and Turkey have emerged as pioneering adopters and deployers of these systems.

Militaries worldwide are rapidly adapting their strategic thinking to incorporate lessons learned from drone-centric conflicts. For Europe, the experience of full-scale war in Ukraine has been a major trigger for revising its defence doctrine. The emphasis has shifted towards distributed operations, electronic-warfare capabilities, and counter-drone technologies. The current trajectory of drone warfare suggests that future conflicts will be increasingly characterised by the integration of AWS across all combat domains, fundamentally reshaping how military forces are organised, trained, and deployed. The proliferation of AWS has also raised critical questions about command-and-control structures, rules of engagement, and the ethical implications of delegating life-and-death decisions to algorithmic systems. Issues concerning the use of drones in targeted killings and civilian casualties is a critical component of this debate. Indeed, the lack of international consensus on appropriate regulations complicates accountability and oversight. As these technologies continue to evolve, there seems to be a need for the incorporation of measures balancing the operational advantages of AWS with human oversight and accountability.

Table 3. Loitering Munitions Suppliers (1995–2023)

Rank	Country	Total Transfers
1	Israel	22
2	Iran	17
3	United States	6
4	Poland	4
5	Australia	2
6	Germany	1
7	Turkey	1
8	UAE	1

Source: Center for a New American Security, Drone Proliferation Dataset.

Iran's development of the Shahed series exemplifies the global evolution of this category of loitering-munitions weaponry. Iranian systems have evolved into sophisticated platforms capable of long-range strikes, surveillance, and coordinated swarm attacks. Their proliferation to proxies across the Middle East has created a force-multiplication effect that extends Iran's strategic reach without direct military engagement. As Table 3 above demonstrates, Iran occupies a strategic position in the global drone ecosystem through its dual-capability approach, ranking fourth among armed drone suppliers while simultaneously holding second position as regards loitering-munitions transfers globally. This standing provides Iran with a significant

asymmetric advantage, as the country has achieved a combined total of 25 transfers comprising 8 armed drone systems and 17 loitering munitions, creating a comprehensive portfolio that enhances both conventional and unconventional warfare (Campbell 2024). Iran serves hereby as the primary supplier to proxy forces and allied nations throughout the Middle East region, leveraging drone technology as a tool for regional power projection and influence. Iran maintained a consistent supply rate across the period 2012–2021, indicating a deliberate and sustained strategy and allowing the country to strengthen relationships with recipient nations and non-state actors alike.

Software-Defined Warfare: How Technological Advancement Is Reshaping Global Military Capabilities

Within the broader landscape of drone technology, a particular category of system that has gained significant strategic importance of late is the aforementioned AWS. “Autonomous” describes a technology’s capacity to achieve its objectives independently or with limited human oversight while operating in challenging and uncertain conditions (Defense Advanced Research Projects Agency 2025). These represent the most advanced iteration of unmanned platforms, distinguished by their ability to select and engage targets without direct human control once activated. The technological advancement to fully autonomous systems represents a fundamental shift in military capabilities, as AWS can operate at machine speed rather than being constrained by human reaction times and decision-making processes, reducing the cognitive burden on operators. The evolution from remotely piloted aircraft to increasingly autonomous systems represents more than incremental progress; it constitutes a revolution in military capability. Modern drone systems now incorporate AI, machine-learning algorithms, and advanced sensor packages that enable them to operate with minimal human intervention. They can, accordingly, identify, track, and engage targets while making tactical decisions in real time.

AWS leverage dual-use civilian technologies that are increasingly available on the commercial marketplace. AI, robotics, and sensor technologies are advancing rapidly in civilian applications, creating a pathway for military adaptation that bypasses traditional proliferation controls. This has made AWS accessible not just to major military powers but potentially to small states and even non-state actors as well. This challenge becomes particularly acute when considering that autonomy in weapons systems is fundamentally a software problem rather than a hardware one. While sophisticated AWS will require military-grade components and systems integration, the core capability of autonomous decision-making can be implemented through software that is easily copied, stolen, or reverse engineered. Converting existing remote-controlled combat drones to autonomous operation using pattern-recognition algorithms is already technically feasible with current technology. Widespread proliferation may accelerate, as something difficult to control through traditional export restrictions or monitoring mechanisms (Altmann and Sauer 2017). States are likely reluctant to allow inspection of AWS software; even if they did, cheating would be easy via rapid software changes immediately after. This verification challenge means that conventional arms-control approaches are inadequate for managing AWS. Moreover, the latter fundamentally alter the tempo of military operations. They can be produced cheaply and in large numbers, making them economically attractive for offensive operations. Most importantly, their swarm capabilities make defending against them extremely difficult.

Further, the emergence of modular drones represents another significant dimension of how traditional security paradigms are now changing, challenging conventional assumptions about the complexity and cost barriers associated with advanced military systems. The threshold for acquiring sophisticated weaponry is constantly being lowered, enabling actors with limited resources to access tools that were previously exclusive to major military powers. Modular drones exemplify this revolution. These sophisticated yet compact devices, often comprising merely a chip with embedded software and sometimes a camera while being smaller than a “bar of soap” (Bondar 2025), have proven their remarkable autonomous capabilities on the battlefield. Their ability to perform critical functions such as surveying the environment, conducting target recognition, and engaging them without direct human flight control has fundamentally altered the nature of combat. The conflict in Ukraine has provided extensive validation of these modular drones. Several regional powers have emerged as key producers and distributors of this technology, fundamentally altering how military capabilities are transferred to non-state actors. Iran and the UAE have positioned themselves at the forefront of this transformation, manufacturing and supplying component-based drone systems to various groups across multiple conflict zones. Unlike traditional arms transfers that required substantial logistical infrastructure and formal government-to-government agreements, these countries have developed distribution networks that can rapidly deliver required components to non-state recipients while maintaining plausible deniability regarding the end users and operational applications of these AWS (Defence Intelligence Agency 2024; Krieg 2025).

Equally significant, events in Ukraine have demonstrated how non-defence infrastructure can be rapidly adapted and integrated into warfare. The conflict has highlighted the dual-use potential of civilian technologies, particularly in the domain of satellites. Commercial variants of the latter, originally designed and operated by private companies for profit-making purposes such as communication, broadcasting, and data transmission, have found unexpected military applications. These systems have been repurposed to now support communications, intelligence-gathering, and coordination on the battlefield too. There are, indeed, a number of companies across the Middle East who are currently developing commercial satellite capabilities (Mordor Intelligence 2024) that could potentially be leveraged for defence purposes in future. Al Yah Satellite Communications Company’s (Yahsat) satellite-based services include broadband, video broadcasting, and mobile solutions; Space42 uses AI-powered space technology and plans to build the region’s first commercial satellite-manufacturing facility.

This convergence of affordable autonomous technologies and adaptable civilian infrastructure has fundamentally reshaped affairs, demonstrating that future conflicts will increasingly rely on defence digitalisation and the creative repurposing of commercial technologies. As regards Europe’s own security interests, these developments present both openings and vulnerabilities that require careful strategic consideration. The proliferation of dual-use satellite capabilities in the Middle East offers new partnership opportunities for European nations in technology transfer and intelligence cooperation, while simultaneously demonstrating the prospective pitfalls inherent to modern digital infrastructures. The ease with which civilian devices can be militarised is particularly concerning, as it highlights how adversaries could weaponise seemingly benign commercial technologies.

AI Ambitions: How Gulf States' Investments Can Transform Regional Military Power

AI has also been pivotal in transforming military operations, by creating new paradigms for intelligence-gathering, decision-making, and tactical execution. Modern combat environments generate enormous volumes of data from satellites, drones, sensors, and communication intercepts, far exceeding human capacity to effectively process them. AI systems now serve as multipliers, enabling military forces to synthesise complex information streams, identify patterns, and respond to threats with unprecedented speed and precision. These technologies have shifted warfare from primarily human-driven operations to hybrid systems where AI augments human decision-making across reconnaissance, targeting, and operational planning. AI-driven capabilities include specialised methods and systems designed to address distinct operational challenges, ranging from identifying hostile equipment in aerial-surveillance footage to analysing various types of unstructured text-based intelligence data. Modern AI applications have also transformed acoustic intelligence by introducing automated sound classification and identification capabilities that operate with remarkable accuracy and rapid response times. Sound-based intelligence-gathering represents a long-established military practice that has been significantly enhanced by AI. This methodology traces back to submarine-detection systems developed during the Second World War. These advanced systems can process audio information instantaneously, enabling the detection and differentiation of sound signatures that would be extremely difficult or even impossible for human operators to distinguish reliably.

The abovementioned ease with which civilian satellite infrastructure can be militarised represents a critical aspect of defence digitalisation. The accelerating convergence of space technology and AI is a major driver of this transformation. The Ukraine War has provided an unprecedented real-world laboratory for testing and validating emerging technologies that leverage the synergies between space-based systems and AI capabilities, fundamentally transforming both sectors. It has enabled spacecraft to autonomously classify imagery, detect anomalies, and prioritise data transmission based on defined parameters (Stroescu and Franchi 2025). This convergence is reshaping global military doctrine by enabling seamless integration across land, sea, air, space, and online. AI-powered satellite systems now provide real-time intelligence fusion, allowing commanders to process vast amounts of multispectral data instantaneously and make informed decisions across multiple theatres simultaneously (Ogden et al. 2024). More recently, various episodes of war between Iran and Israel has demonstrated how space-based AI can enhance battlefield awareness through autonomous target recognition and predictive threat assessments: "AI-assisted satellite imagery analysis and communications intercepts helped identify and prioritise high-value Iranian targets" (Alam 2025).

Several GCC countries have launched their own AI initiatives by now. Qatar and the UAE began their respective programmes in 2017, followed by Bahrain and Saudi Arabia two years later. By 2023, both Qatar and the UAE had begun developing comprehensive regulatory frameworks, reflecting the region's growing commitment to responsible AI governance (Lean Tech 2024). The GCC nations have emerged as major global investors in AI: during President Donald Trump's recent Middle East tour, the UAE pledged USD 200 billion in additional investments hereto, Saudi Arabia committed USD 600 billion over four years, and Qatar earmarked USD 1.2 trillion for AI and related technologies (PWC 2025). It is estimated that generative AI applications could result in annual turnover figures of between USD 21–35 billion for the GCC region (McKinsey 2024).

Saudi Arabia leads regional AI investment through its Public Investment Fund, which is reportedly in discussions to establish a USD 40 billion fund in partnership with Silicon Valley firms like Andreessen Horowitz. The country is aiming to become the world's third-largest AI provider behind the US and China, with USD 23 billion allocated for strategic partnerships and a USD 10 billion venture capital fund. Saudi Arabia has also secured partnerships with Groq, Amazon Web Services, AMD, and Nvidia for AI infrastructure development. The collaboration with Nvidia encompasses the development of 500 megawatts of AI processing facilities over a five-year timeline (Turak 2025). The country has also begun working with Qualcomm on edge computing and Arabic-language processing models. Major technology corporations including Google, Oracle, Salesforce, Uber, and DataVolt have committed to combined investments of USD 80 billion, with the latter independently allocating USD 20 billion to AI-related data centre construction in the US (Bhat 2025).

In 2024, the UAE announced plans for setting up a specialised investment fund focused on AI and semiconductor technologies, with over USD 100 billion in assets to be placed under its management (Fast Company 2024). The country has systematically developed its AI infrastructure and established the world's first ministerial position dedicated to this domain. Arabic–English AI assistants are integrated across government departments to optimise service delivery (Bhat 2025).

The AI investments by GCC countries carry profound implications for military applications and regional strategic positioning. The convergence of AI and defence capabilities enables these countries to overcome their military dependence on imported technology and equipment. AI-powered systems can enhance everything from AWS platforms to predictive intelligence analysis and real-time battlefield decision-making. These investments can create technological foundations readily adapted to military communications, surveillance, and AWS operations. As the GCC countries establish themselves as major AI developers rather than merely technology consumers, their growing capacity to produce indigenous solutions is reducing their dependence on Western military technologies while simultaneously enabling them to export this know-how to regional partners, fundamentally altering the balance of power in the Middle East and positioning the Gulf states as emerging-technology powers of global reach.

Cyber Arms Race: AI and Digital Warfare

The integration of AI with cyberwarfare capabilities has fundamentally transformed the landscape of global security, opening new pathways for state-level conflict beyond traditional geographic boundaries. This represents a paradigm shift in how states conduct information warfare and infrastructure attacks. AI algorithms now enable them to craft sophisticated social-engineering campaigns, automate reconnaissance activities, and develop zero-day exploits with unprecedented speed and precision. Machine learning is fundamentally changing malware creation, leading to the development of malicious programmes that possess the ability to learn, modify themselves, and escape traditional countermeasures. State and non-state actors are now able to create AI-powered systems generating adaptive malware that transforms its underlying code to avoid detection. AI has also fundamentally enhanced the impact of social-manipulation attacks, rendering them significantly more precise and convincing (Kinight 2025). AI-driven cyberthreats represent a major danger to vital infrastructure in arenas such as utilities, financial services, healthcare, and transportation. By evading standard safeguards, AI

enables more persistent, far-reaching, and destructive compromises (Lipsker 2025). For cyber defence, AI has become equally transformative. Advanced threat-detection systems leverage machine learning to identify anomalous network behaviour, predict attack patterns, and respond to threats within milliseconds. These systems can process vast amounts of network-traffic data, correlate seemingly unrelated events, and provide early-warning capabilities that human analysts could never achieve independently (Mohamed 2025).

Studying the dynamics of competition here – that is, how nation-states engage in digital warfare and cyber-enabled rivalry – is an evolving field. The strategic motivations driving key regional players, the methods and tools employed, and the implications of such competition for broader security architectures must all be considered. Regional powers leverage cyber capabilities to advance their geopolitical objectives, challenge adversaries, and establish dominance within their respective spheres of influence. Cyber resilience is established through distinct pathways, ones shaped by states' unique strategic environments, threat perceptions, and available resources. Transformation into a digitally connected economy has exposed regional players to heightened cyber threats. The proliferation of smart cities, AI integration, online government- and private sector services, and 5G infrastructure has made many countries in the Middle East attractive targets. Naturally, those that are more digitalised (such as Saudi Arabia, Turkey, and the UAE) are more vulnerable due to their expanded digital surfaces and economic dependence on interconnected systems. Iran, despite its more limited digital infrastructure, remains vulnerable for strategic reasons. In recent years, its state institutions have experienced significantly more external attacks than the private sector, reflecting the country's adversarial international position and the targeting of regime-critical infrastructure by foreign actors.

As noted, AI is being increasingly weaponised for sophisticated phishing campaigns, large-scale misinformation operations, and critical infrastructure-related espionage. In response, most regional governments have established comprehensive national cybersecurity frameworks that are meant to unite agencies, industry stakeholders, and private sector entities to create a coordinated defence strategy. With its "National Cyber Security Strategy," the UAE has established a multilayered defence framework that integrates AI-powered threat detection with strategic partnerships and regulatory frameworks (Al Hammadi 2025). Saudi Arabia has also developed a comprehensive cybersecurity framework that leverages AI for threat detection, incident response, and infrastructure resilience (Library of Congress, 2024). Further, Saudi investments in AI-driven cybersecurity aim at strengthening partnerships with international technology companies to develop indigenous capabilities on the protection of critical infrastructure. Turkey recently promulgated a new cybersecurity law that creates a Cybersecurity Directorate under presidential oversight, with broad authority over the collection of digital data when approved by court order. Under this law, a cybersecurity council chaired by President Recep Tayyip Erdogan and including intelligence and security officials centralises state control over related policy. Critics argue that this could lead to the suppression of investigative journalism by criminalising reporting on data leaks unless the authorities confirm incidents themselves (Committee to Protect Journalists, 2025). Iran's cybersecurity laws primarily serve as instruments of domestic censorship and social control rather than comprehensive protection frameworks. The Iranian Cyber Police, established in 2011, actively enforce restrictions on virtual private networks, which many Iranians use to circumvent Internet censorship – demonstrating the regime's prioritisation of information control over cybersecurity. Regulations penalise offences like hacking, data theft, and computer forgery, but they lack robust personal data-

protection provisions and fail to establish comprehensive technical standards for safeguarding critical infrastructure or private sector entities (Mirshahi, 2024).

These regional initiatives consistently prioritise the protection of critical sectors, particularly energy, telecommunications, finance, and transportation. The UAE exemplifies the taking of a collaborative approach by distributing cybersecurity responsibilities beyond governmental agencies to harness collective sectoral expertise, thereby enhancing awareness and building comprehensive societal resilience (Al Kuwaiti and Anwar, 2025). However, these legal frameworks simultaneously fortify state surveillance apparatus and content-restriction mechanisms, revealing that maintaining political control over digital domains often supersedes the protection of citizens' digital rights and civil liberties.

These governments are simultaneously investing in offensive cyberwarfare capabilities to project power and advance strategic objectives. Iran exemplifies this trend, leveraging AI-powered tools to conduct more precise social-engineering campaigns, develop adaptive malware, and orchestrate complex information-warfare operations against regional adversaries and Western targets alike. In recent years, then, Iran has emerged as a sophisticated cyber power. OpenAI documented three instances in 2024 where actors including Iranian groups exploited ChatGPT for malicious purposes. Alongside Chinese, North Korean, and Russian peers, they used the platform across various cyber operations. The Iranian group Crimson Sandstorm specifically leveraged the AI tool to create phishing emails, including fake communications from international development agencies, demonstrating how AI enhances their English-language capabilities for influence campaigns. These incidents highlight the growing trend of Iran-sponsored actors weaponising commercial AI platforms (Tkeshelashvili and Saade, 2024). The Iranian government has furthermore deployed AI-enabled facial-recognition technology imported from China as part of its enforcement efforts against women who do not comply with mandatory veiling laws.

Although potentially lacking direct access to cutting-edge technologies for developing and training sophisticated AI systems, Iran has a proven track record of reverse engineering and acquiring know-how through illicit means. A long history of successfully reverse engineering advanced military hardware, including drones and missile systems, alongside its established capabilities in cyber espionage and technology theft suggest that Tehran could potentially combine Chinese-supplied technology with stolen intellectual property to advance its AI development. This hybrid approach of leveraging legitimate partnerships with allies, combined with covert acquisition of Western technologies and indigenous reverse-engineering efforts, could enable Iran to circumvent international sanctions and technological restrictions to build more sophisticated AI capabilities than its isolated position might otherwise allow.

These developments also carry profound implications for Europe, as adversarial cyber capabilities have increasingly targeted its countries – prominently among them Germany. Iran exemplifies this threat (Bundesamt für Verfassungsschutz Cyberabwehr, 2023): state-backed cyber groups like APT35 (Charming Kitten) and APT34 (OilRig) have systematically targeted European organisations, demonstrating Tehran's willingness to extend its offensives beyond the Middle East (Hajdari, 2025). This is forcing EU member states to fundamentally reassess and strengthen their defensive postures in the face of state-sponsored cyber threats increasingly blurring the lines between espionage, sabotage, and warfare.

Conclusion

The transformation of the Middle East's strategic landscape as a result of emerging defence technologies represents a fundamental shift away from traditional power structures. Iran, Saudi Arabia, Turkey, and the UAE have each pursued distinct paths towards technological sovereignty beyond historical dependence on foreign military suppliers. The development of these countries' national cyber doctrines is influenced by multiple factors including geopolitical positioning, economic constraints, technological access, domestic security priorities, and alliance structures. The digitalisation trajectories of these respective regional powers demonstrate an accelerating trend towards both offensive and defensive operations, though the pace and direction of development varies significantly based on each state's strategic priorities and capabilities. Some nations pursue indigenous technology development through reverse engineering and proxy networks, others invest heavily in international partnerships and technology acquisition. All of these states seek to centralise national cyber capabilities under direct state control. Regional competition is, as such, creating new forms of digital deterrence, escalation dynamics, and strategic interdependencies that are fundamentally reshaping traditional concepts of sovereignty, security, and influence in the Middle East.

Three domains have been central to this remaking of regional security dynamics: First, drone warfare has transformed military capabilities, enabling both state and non-state actors to project power with unprecedented accessibility and cost-effectiveness. Second, the integration of AI with military systems has accelerated decision-making processes while creating new possibilities for AWS that by and large operate beyond traditional human control. Third and finally, the convergence of cyberwarfare capabilities with AI technologies has opened up new realms of conflict beyond geographic boundaries, challenging conventional concepts of sovereignty and deterrence. The broader implications of emerging defence technologies extend beyond military modernisation. These developments are challenging established supplier–client relationships, potentially reducing Western leverage, and creating new dynamics of competition among the Middle East's regional powers. The proliferation of advanced military capabilities is enabling these nations to support proxy conflicts, project force independently, and establish alternative partnerships that challenge traditional alliances.

As regards Europe's own security interests, there are opportunities and challenges alike. While partnerships with Gulf states offer sizeable prospective revenue streams for Europe and its defence industries, the former's growing independence simultaneously reduces the latter's role in security decisions and complicates conflict-resolution efforts. The targeting of European countries by Iranian cyber operations demonstrates, moreover, how these technological advancements are generating immediate and tangible security threats that demand urgent attention. The current trajectory of these developments suggests that future conflicts will increasingly be characterised by digital warfare, AWS, and cyber-enabled information operations that fundamentally alter the pace, nature, and geographic scope of military engagement in ways that will continue to greatly challenge European security frameworks and international stability.

Bibliography

- Al Arabiya (2024) *Saudi defense firm SAMI signs 3 MOUs with Turkish companies*, Al Arabiya. Available at: <https://english.alarabiya.net/News/saudi-arabia/2024/07/04/saudi-defense-firm-sami-signs-3-mous-with-turkish-companies-> (Accessed: 19 July 2025).
- Al Hammadi, A. (2025) *UAE: Ministry of Interior leverages Artificial Intelligence to fight cyber and economic crimes*, Gulf News. Available at: <https://gulfnews.com/technology/uae-ministry-of-interior-leverages-artificial-intelligence-to-fight-cyber-and-economic-crimes-1.500226766#> (Accessed: 1 September 2025).
- Al Kuwaiti, M.H. and Anwar, H. (2025) *The power of partnership: How the UAE is securing cyberspace*, *World Economic Forum*. Available at: <https://www.weforum.org/stories/2025/06/uae-securing-cyber-space/#:~:text=The%20UAE%20has%20developed%20a%20powerful%20national%20cybersecurity%20model%20that,cyber%2Dresilience%20at%20every%20level> (Accessed: 1 September 2025).
- Alam, F. (2025) *How AI shaped the Iran-Israel 12-day war*, *The Daily Star*. Available at: <https://www.thedailystar.net/opinion/views/news/how-ai-shaped-the-iran-israel-12-day-war-3927726> (Accessed: 14 July 2025).
- Altmann, J. and Sauer, F. (2017) 'Autonomous Weapon Systems and Strategic Stability', *Survival*, 59(5), pp. 117–142. Available at: <https://doi.org/doi.org/10.1080/00396338.2017.1375263>.
- Arab News (2024) *Saudi defense minister meets president of Turkiye's Defense Industry Agency*, Haluk Gorgun, Arab News. Available at: <https://www.arab-news.com/node/2543126/saudi-arabia> (Accessed: 20 July 2025).
- Army Recognition (2025) *Turkish company Baykar to produce TB2 and Akinci UAVs in Italy after acquiring Piaggio Aerospa*, *Armyrecognition.com*. Available at: <https://armyrecognition.com/news/army-news/2025/turkish-company-baykar-to-produce-tb2-and-akinci-uavs-in-italy-after-acquiring-piaggio-aerospace> (Accessed: 28 August 2025).
- Astute Group (2025) *SAMI aims for top 25 with new CEO at HELM*, *Astute*. Available at: <https://www.astutegroup.com/news/defence/sami-aims-for-top-25-global-defence-primers/> (Accessed: 18 July 2025).
- Bazoobandi, S. (2024) *Development of the Knowledge-Based Economy in Iran*, *AGSI*. Available at: <https://agsi.org/analysis/development-of-the-knowledge-based-economy-in-iran/> (Accessed: 28 August 2025).
- Bhat, D. (2025) *Can the Gulf buy its way to AI supremacy?*, *Rest of the World*. Available at: <https://restofworld.org/2025/gulf-ai-investment-us-china-race/>.
- Bondar, K. (2025) *Ukraine's Future Vision and Current Capabilities*, *Center for Strategic and International Studies*. Available at: <https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare> (Accessed: 9 July 2025).
- Bundesamt für Verfassungsschutz Cyberabwehr (2023) *Warnhinweis zu Cyberspionage gegen Kritiker des iranischen Regimes in Deutschland*, *verfassungsschutz.de*. Available at: <https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/cyberabwehr/2023-01-bfv-cyber-brief.html> (Accessed: 3 September 2025).

- Calcara, A. *et al.* (2022) 'Why Drones Have Not Revolutionized War The Enduring Hider-Finder Competition in Air Warfare', *International Security*, 46(2), pp. 130–171. Available at: https://doi.org/10.1162/isec_a_00431.
- Campbell, M. (2024) *Drone Proliferation Dataset*, *Center for a New American Security*. Available at: <https://www.cnas.org/publications/reports/drone-proliferation-dataset> (Accessed: 29 August 2025).
- Chernohorenko, K. (2025) *Digitize or die: Ukraine's war is a wake-up call for 20th century militaries*, *Breaking Defense*. Available at: <https://breakingdefense.com/2025/07/digitize-or-die-ukraines-war-is-a-wake-up-call-for-20th-century-militaries/> (Accessed: 15 July 2025).
- Committee to Protect Journalists (2025) *New Turkish law criminalizes 'false' reporting on cybersecurity-related data leaks*, *CPJ.org*. Available at: <https://cpj.org/2025/03/new-turkish-law-criminalizes-false-reporting-on-cybersecurity-related-data-leaks/> (Accessed: 2 September 2025).
- Defence Here (2024) *Milrem Robotics showcases robotic vehicles in Saudi Arabia*, *Defence Here*. Available at: <https://defensehere.com/en/milrem-robotics-showcases-robotic-vehicles-in-saudi-arabia/> (Accessed: 10 July 2025).
- Defence Intelligence Agency (2024) *Iran enabling Houthi attacks across the Middle East*, *DIA.mil*. Available at: https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Iran_Houthi_Final2.pdf (Accessed: 29 August 2025).
- Defense Advanced Research Projects Agency (2025) *Assured Autonomy*, *DARPA*. Available at: <https://www.darpa.mil/research/programs/assured-autonomy> (Accessed: 9 July 2025).
- Dent, E. and Rumley, G. (2024) *How the U.S. Used Arms Sales to Shift Saudi Behavior*, *Washington Institute for Near East Policy*. Available at: <https://www.washingtoninstitute.org/policy-analysis/how-us-used-arms-sales-shift-saudi-behavior> (Accessed: 21 July 2025).
- EDGE (2023) *RASH - 1 M*, *EDGE Group*. Available at: <https://edgegroup.ae/solutions/rash-1-m> (Accessed: 21 July 2025).
- EDGE (2025) *EDGE Champions 'Made in the UAE' Defence Capabilities at MIITE 2025*, *EDGE Group*. Available at: <https://edgegroup.ae/news/edge-champions-made-uae-defence-capabilities-miite-2025> (Accessed: 21 July 2025).
- Fast Company (2024) *Abu Dhabi unveils AI investment firm, aims \$100 billion AUM*. Available at: <https://fastcompany.com/news/abu-dhabi-unveils-ai-investment-firm-aims-100-billion-aum/> (Accessed: 29 August 2025).
- Hajdari, U. (2025) *Iranian hackers target Albania in retaliation for hosting dissidents*, *Politico*. Available at: <https://www.politico.eu/article/iran-hackers-target-albania-servers-in-retaliation-hosting-dissidents/>.
- Hammes, T.X. (2013) *Droning America: The Tech Our Enemies Can Buy*, *War on Rocks*. Available at: <https://warontherocks.com/2013/10/droning-america-the-tech-our-enemies-can-buy/> (Accessed: 4 July 2025).
- Helou, A. (2025) *Saudi Arabia increases defense spending to \$78B in 2025*, *Breaking Defense*. Available at: <https://breakingdefense.com/2025/02/saudi-arabia-increases-defense-spending-to-78b-in-2025/> (Accessed: 19 July 2025).

- HOZINT (2021) *The Use Of Weaponized Consumer Drones By Drug Cartels*, HOZINT.com. Available at: <https://www.hozint.com/2021/10/mexico-the-use-of-weaponized-consumer-drones-by-drug-cartels/> (Accessed: 29 August 2025).
- Iran Watch (2022) *Iran Aircraft Manufacturing Industries (HESA)*, Iran Watch. Available at: <https://www.iranwatch.org/iranian-entities/iran-aircraft-manufacturing-industries-hesa> (Accessed: 28 August 2025).
- Issa, T.M. (2022) *Saudi Arabia spent \$1.4 bln in incentives to boost local military sector in 2021-22*, Al Arabiya. Available at: <https://english.alarabiya.net/News/saudi-arabia/2022/12/12/Saudi-Arabia-spent-1-4-bln-in-incentives-to-boost-local-military-sector-in-2021-22> (Accessed: 12 September 2025).
- Kinight, A. (2025) *AI-Driven Cyber Espionage: Navigating the Rising Threat*, GreyDynamics.com. Available at: <https://greydynamics.com/ai-driven-cyber-espionage-navigating-the-rising-threat/> (Accessed: 1 September 2025).
- Kongkini, E. (2025) *ASELSAN: Turkish Defence Corporation Marks 50 Years*, GreyDynamics.com. Available at: <https://greydynamics.com/aselsan-turkish-defence-corporation-marks-50-years/#h-1-history> (Accessed: 28 August 2025).
- Krieg, A. (2025) *UAE drones have given rise to a new arms economy*, LSE Blog. Available at: <https://blogs.lse.ac.uk/businessreview/2025/06/09/uae-drones-have-given-rise-to-a-new-arms-economy/> (Accessed: 29 August 2025).
- Kyiv Post (2024) *Chinese Radio, Drone Export Restrictions Starting Sept. 1*, Kyiv Post. Available at: <https://www.kyivpost.com/post/38142> (Accessed: 10 July 2025).
- Lean Tech (2024) *AI Initiatives in GCC Countries: Transforming the Future*, Leantech.sg. Available at: <https://www.leantech.sg/ai-initiatives-in-gcc-countries-transforming-the-future/> (Accessed: 16 July 2025).
- Library of Congress (2024) *Saudi Arabia: National Cybersecurity Authority Issues New Regulations, Instructions, and Procedures to Enhance Cybersecurity Readiness*, LOC.gov. Available at: <https://www.loc.gov/item/global-legal-monitor/2024-02-04/saudi-arabia-national-cybersecurity-authority-issues-new-regulations-instructions-and-procedures-to-enhance-cybersecurity-readiness/> (Accessed: 2 September 2025).
- Lipsker, L. (2025) *Artificial Intelligence and State-Sponsored Cyber Espionage: The Growing Threat of AI-Enhanced Hacking and Global Security Implications*, NYU Journal of Intellectual Property and Entertainment Law. Available at: <https://jipel.law.nyu.edu/artificial-intelligence-and-state-sponsored-cyber-espionage/> (Accessed: 1 September 2025).
- McKinsey (2024) *The state of gen AI in the Middle East's GCC countries: A 2024 report card*, Mckinsey.com. Available at: <https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-gen-ai-in-the-middle-east-s-gcc-countries-a-2024-report-card> (Accessed: 29 August 2025).
- Mirshahi, S. (2024) *قوانین امنیت سایبری، برای محافظت از دولت‌ها یا مردم؟ [cyber security laws, protecting people of governments?]*, Asre Ertebat. Available at: <https://asreertebat.com/قوانین-امنیت-سایبری-برای-محافظت-از-دولت-ها-یا-مردم-؟> (Accessed: 2 September 2025).
- Mohamed, N. (2025) 'Artificial intelligence and machine learning in cybersecurity: a deep dive into state-of-the-art techniques and future paradigms', *Knowledge and Information Systems*, 67, pp. 6969–7055. Available at: <https://doi.org/10.1007/s10115-025-02429-y>.

- Mordor Intelligence (2024) *Middle East Satellite-based Earth Observation Top Companies*, Mordor Intelligence. Available at: <https://www.mordorintelligence.com/industry-reports/middle-east-satellite-based-earth-observation-market/companies> (Accessed: 10 July 2025).
- Office of the Under Secretary of Defense for Policy (2023) *DOD DIRECTIVE 3000.09 AUTONOMY IN WEAPON SYSTEMS*, United States Department of Defence. Available at: <https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf> (Accessed: 10 July 2025).
- Ogden, T. et al. (2024) *The Role of the Space Domain in the Russia-Ukraine War*, Centre for Emerging Technology and Security. Available at: <https://cetas.turing.ac.uk/publications/role-space-domain-russia-ukraine-war>.
- Oliver, D. (2024) *UAE's drones gives it the Edge*, times aerospace. Available at: <https://www.timesaerospace.aero/features/defence/uaes-drones-gives-it-the-edge> (Accessed: 21 July 2025).
- Pamuk, H., Zengerle, P. and Holland, S. (2024) <https://www.washingtoninstitute.org/policy-analysis/how-us-used-arms-sales-shift-saudi-behavior>, Reuters. Available at: <https://www.reuters.com/world/us-lift-ban-offensive-weapons-sales-saudi-arabia-sources-say-2024-08-09/> (Accessed: 19 July 2025).
- PWC (2025) *The potential impact of Artificial Intelligence in the Middle East*, PWC. Available at: <https://www.pwc.com/m1/en/publications/potential-impact-artificial-intelligence-middle-east.html> (Accessed: 29 August 2025).
- Shahbazov, F. (2024) *Forging Defense Partnership: Turkey's Role in Saudi Arabia's Arms Industry Expansion*, Gulf International Forum. Available at: https://gulif.org/forging-defense-partnership-turkeys-role-in-saudi-arabias-arms-industry-expansion/?utm_source=chatgpt.com (Accessed: 15 April 2025).
- Stewart, P. and Strobel, W. (2016) *U.S. to halt some arms sales to Saudi, citing civilian deaths in Yemen campaign*, Reuters. Available at: <https://www.reuters.com/article/world/us-to-halt-some-arms-sales-to-saudi-citing-civilian-deaths-in-yemen-campaign-idUSKBN1422M5/> (Accessed: 19 July 2025).
- Stroescu, A. and Franchi, A. (2025) *CONVERGING EARTH AND SPACE: AI-DRIVEN TN/NTN CONNECTIVITY*, European Space Agency. Available at: https://connectivity.esa.int/sites/default/files/ESA_AI_Driven_TN_NTN_Connectivity.pdf.
- Technical Report (2025) *Saudi SAMI-AEC and Lockheed Martin cooperate on unmanned systems, AI*, Technicalreport.com. Available at: <https://www.tacticalreport.com/daily/63468-saudi-sami-aec-and-lockheed-martin-cooperate-on-unmanned-systems-ai> (Accessed: 21 July 2025).
- The Guardian (2024) *Al-Yamamah arms deal report comes to light ending anti-corruption campaigners' battle*, The Guardian. Available at: <https://www.theguardian.com/world/2024/mar/24/al-yamamah-arms-deal-report-discovery-anti-corruption-mod-ao-britain-saudi-arabia> (Accessed: 15 July 2025).
- Times Aerospace (2022) *SAMI announces joint venture agreement with Boeing*, times aerospace. Available at: <https://www.timesaerospace.aero/news/maintenance/sami-announces-joint-venture-agreement-with-boeing> (Accessed: 21 July 2025).

- Tkeshelashvili, M. and Saade, T. (2024) *Decrypting Iran's AI-Enhanced Operations in Cyberspace*, *Institute for Security and Technology*. Available at: <https://securityandtechnology.org/blog/decrypting-irans-ai-enhanced-operations-in-cyberspace/>.
- Turak, N. (2025) *Saudi AI firm Humain is pouring billions into data. Will it pay off?*, *CNBC*. Available at: <https://www.cnn.com/2025/08/27/saudi-arabia-wants-to-be-worlds-third-largest-ai-provider-humain.html> (Accessed: 29 August 2025).
- Waters, N. (2018) *The Poor Man's Air Force? Rebel Drones Attack Russia's Airbase in Syria*, *Bellingcat*. Available at: https://www.bellingcat.com/news/mena/2018/01/12/the_poor_mans_airforce/ (Accessed: 4 July 2025).
- White, A. (2025) *Why Ukraine's all-drone, multi-domain attack could be a 'seminal' moment in warfare*, *Breaking Defense*. Available at: https://breakingdefense.com/2025/01/why-ukraines-all-drone-multi-domain-attack-could-be-a-seminal-moment-in-warfare/?utm_campaign=BD%20Daily&utm_medium=email&_hsmi=344081824&utm_content=344081824&utm_source=hs_email (Accessed: 10 July 2025).
- Yerushalmy, J. and J. Bhuiyan (2024) *Academics in US, UK and Australia Collaborated on Drone Research with Iranian University Close to Regime*, *The Guardian*. Available at: <https://www.theguardian.com/world/2024/feb/14/academics-in-us-uk-and-australia-collaborated-on-drone-research-with-iranian-university-close-to-regime> (Accessed: 23 September 2025).
- Zawya (2022) *SAMI signs multiple agreements with Singaporean Group ST Engineering*, *Zawya.com*. Available at: <https://www.zawya.com/en/press-release/companies-news/sami-signs-multiple-agreements-with-singaporean-group-st-engineering-aidvmf40> (Accessed: 21 July 2025).
- Zawya (2025) *Thales, Milrem Robotics and EM&E Group sign a MoU for strategic cooperation in the United Arab Emirates*, *Zawya.com*. Available at: <https://www.zawya.com/en/press-release/companies-news/thales-milrem-robotics-and-em-and-e-group-sign-a-mou-for-strategic-cooperation-in-the-united-arab-emirates-v5w2n2ku> (Accessed: 15 July 2025).
- Zegart, A. (2021) 'Cheap fights, credible threats: The future of armed drones and coercion', in T.S. Sechser, N. Narang, and C. Talmadge (eds) *Emerging Technologies and International Stability*. London: Routledge.

Glossary

APT34 (OilRig) – An Iranian state-sponsored cyber espionage group that primarily targets Middle Eastern governments and organisations in the financial, government, energy, and telecommunications sectors.

APT35 (Charming Kitten) – An Iranian state-sponsored group known for conducting sophisticated phishing campaigns and cyber espionage operations against government officials, journalists, and activists.

EDGE Group – A state-owned advanced technology conglomerate based in the UAE, created in 2019 through the merger of several existing defence entities. It operates through four divisions: equipment manufacturing; weaponry development; digital-warfare technologies; and, operational-support services.

EM&E's SECUTOR weapon station – A remote system developed designed for integration with UGVs, with various combat applications.

Fateh missiles – A series of short-range ballistic missiles developed by Iran, with a range typically between 200–300 km, designed for precision strikes against tactical targets.

First Person View systems – Drone control with an onboard camera that provide real-time video transmission to the operator.

F-16 programme – A multinational fighter-aircraft manufacturing and maintenance programme involving the General Dynamics (now Lockheed Martin) F-16 Fighting Falcon, one of the most widely used fighter jets globally.

Houthis – Officially known as Ansar Allah, a Yemeni armed political and religious movement that has been involved in the country's ongoing civil war and has conducted attacks on shipping in the Red Sea using drone and missile technology.

ISIL – Islamic State of Iraq and the Levant, also known as ISIS or Daesh, a militant Islamist group and early adopter of commercially available drone technology for surveillance and attack purposes.

Milrem Robotics – Originally an Estonian company (later acquired by EDGE Group) specialising in UGV development.

SAMI (Saudi Arabian Military Industries) – Launched in 2017 as part of "Vision 2030" to develop indigenous defence-manufacturing capabilities and reduce dependence on foreign suppliers.

Sejjil missiles – Medium-range (estimated 2,000–2,500 km) ballistic missiles, representing some of Iran's most advanced solid-fuel missile technology.

Shahed drones – A series of Iranian-manufactured UAVs, including both surveillance and armed variants, notably used in Ukraine and conflicts across the Middle East in being supplied to various proxy groups and allied nations.

TB2 and Akinci systems – UAVs developed by Turkish company Baykar. The TB2 is a medium-altitude, long-endurance drone. The Akinci is a larger and more capable drone designed for complex missions.

TF-X fighter-jet programme – Turkey's indigenous fifth-generation fighter-aircraft development programme, the "Turkish Fighter eXperimental," aimed at developing a domestically produced stealth fighter.

Thales' 70mm rocket systems – Precision-guided and designed for integration with various platforms, including helicopters and UGVs.

THeMIS – A UGV developed by Milrem and designed as a modular platform capable of performing diverse missions, including cargo transport, casualty evacuation, anti-tank operations, and intelligence-gathering.

Imprint

The DigiTraL Policy Study is an Open Access publication and can be read on the Internet and downloaded free of charge. According to the conditions of the Creative-Commons license Attribution-No Derivative Works 3.0, this publication may be freely duplicated, circulated, and made accessible to the public. The particular conditions include the correct indication of the initial publication as DigiTraL Policy Study and no changes in or abbreviation of texts. The DigiTraL Policy Study is edited and published by the GIGA. The views and opinions expressed are solely those of the authors and do not necessarily reflect those of the institute. Authors alone are responsible for the content of their articles. GIGA and the authors cannot be held liable for any errors and omissions, or for any consequences arising from the use of the information provided. The GIGA is thankful for the institutional support provided by the Free and Hanseatic City of Hamburg (Ministry of Science, Research and Equalities) and the Federal Republic of Germany (Federal Foreign Office).

Editor DigiTraL Policy Study: Dr. Iris Wiczorek
Editorial Department: Petra Brandt, Dr. James Powell

GIGA | Neuer Jungfernstieg 21
20354 Hamburg
Germany

info@giga-hamburg.de
<http://www.giga-hamburg.de>