المركز العربي للأبحاث ودراسة السياسات
Arab Center for Research & Policy Studies

Case Analysis | 6 May 2026

Hyperwar and the Defence of the Gulf Cities

Jean-Michel Valantin - Nathalie Glais

Hyperwar and the Defence of the Gulf Cities

Series: Case Analysis

6 May 2026

Jean-Michel Valantin

Collaborator with The Red Team Analysis Society and the Small Wars Journal. He is currently working on the militarization of AI and its consequences on warfare. He is exploring the different dimensions of the concept of Hyperwar, in order to anticipate the way AI transforms the links between nation/army/politics. He holds a PhD in Strategic Studies and Defence Sociology.

Nathalie Glais

Associate researcher at the University of Poitiers and at the International Observatory on the Societal Impacts of AI (Canada), and frequent collaborator with Small Wars Journal. She holds a PhD in Social sciences, for which her thesis focused on the interactions between organization governance and algorithmic tools. Her work examines AI as a driver of strategic transformation, reshaping global governance and power relations, especially within urban systems.

The Arab Center for Research and Policy Studies is an independent research institute and think tank for the study of history and social sciences, with particular emphasis on the applied social sciences.

The Center's paramount concern is the advancement of Arab societies and states, their cooperation with one another and issues concerning the Arab nation in general. To that end, it seeks to examine and diagnose the situation in the Arab world - states and communities- to analyze social, economic and cultural policies and to provide political analysis, from an Arab perspective.

The Center publishes in both Arabic and English in order to make its work accessible to both Arab and non-Arab researchers.

The Arab Center for Research and Policy Studies

Al-Tarfa Street, Wadi Al Banat

Al-Dayaen, Qatar

PO Box 10277, Doha

+974 4035 4111

www.dohainstitute.org

Table of Contents

Introduction

The US and Israeli air offensive against Iran began on 28 February 2026.[1] Starting on 1 March, the Iranian Revolutionary Guard launched missile strikes against US military bases in various Persian Gulf countries, as well as against oil and gas infrastructure. These strikes would only intensify, targeting Kuwait, Bahrain, Saudi Arabia, the United Arab Emirates, and Qatar. They targeted oil and gas facilities, data centres, and desalination plants.[2] Thus, the Iran war threatens the very infrastructure necessary for the highly modern and connected cities in the Persian Gulf to function on a daily basis.

The Gulf countries are characterized by the high urbanization of relatively small populations. Across the region, nearly 80% of the total population now lives in urban areas, and their capital cities play a global role.[3] These capitals exert their authority over oil, gas, and chemical industries and infrastructure, the production levels of which are a major driver of global energy, chemical, and agricultural operations.[4] The current structure of these cities is inextricably linked to the massive influx of investment fuelled by oil and gas revenues, and the resulting international financial appeal since the early 1980s.[5] Moreover, the massive emergence of natural gas in the global energy mix since the early 2000s has had profound consequences for urban planning, particularly in Qatar and the UAE, by financing the accelerated modernization of their cities. This state-led modernization has, in turn, oriented urban development around digital technologies and connectivity. This approach is intended to support economic diversification, especially in the financial and fintech sectors, as well as in tourism.

This integration of Gulf cities into the global dynamic of "augmented cities" powered by AI is reflected in the widespread integration of online services into the daily lives of residents of Doha and Abu Dhabi, as well as in major urban development projects like Saudi Arabia's Neom, which aims to integrate both climate change adaptation and large-scale urban AI. Furthermore, these states and cities are positioning themselves as major hubs for the development of AI infrastructure. Thus, the UAE hosts an OpenAI data centre as part of the Stargate project, an initiative aimed at expanding the US company's global network of data centres.

Such modernization rests on the interconnection of land, sea, and air transport systems, the digital management of public services and private enterprises, and the integration of technological and spatial capabilities into the daily functioning of cities. It also relies on critical environmental control infrastructures, in particular air conditioning and desalination plants, which are essential to sustaining viable living conditions in one of the most hostile environments on the planet. However,

---

1 Mark F. Cancian and Chris H. Park, "Assessing the Air Campaign after Three Weeks", CSIS, 25/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1CQz

2 Ellen Clark, Noor Hammad, and Hasna Wajid, "Mapping the Damages: Iranian strikes on the GCC", IISS, 27/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1CUg

3 Brigitte Dumortier, "The Gulf Cities: A composite and Evolving urban Model", European Institute of the Mediterranean, 2015, at: https://acr.ps/hBy1CnR

4 Ahmed al Ashemi, "The Strait of Hormuz is not just an oil chokepoint", *Al Jazeera*, 27/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1D1E

5 Daniel Yergin, *The New Map: Energy, Climate, and the Clash of Nations*, (Penguin Books: London, 2021).

the tech and AI systems at the core of this modernity simultaneously reveal themselves as sources of vulnerability – surfaces of attack that are actively exploited within Iran's strategic approach.[6]
In other words, the capitals and major cities of the Gulf are highly modern urban entities, deeply dependent on cutting-edge infrastructure and technologies. This modernity is reflected most clearly in the systematic use of AI in the governance and operation of a number of cities, which are underway to becoming "smart cities," listed in the international smart city index.[7]

For the past fifteen years or so, oil and gas revenues have been strategically reinvested to diversify the economies of the Gulf Cooperation Council (GCC) countries, particularly through the integration of AI technologies.[8] The companies driving this transformation, primarily of Chinese and US origin, have become deeply embedded in both the economic development and the governance of Gulf cities. Thus, Iranian strikes on three data centres directly threaten the banking, financial, and IT operations of Bahrain, the UAE, and the wider network of countries to which they are connected. However, Iranian drone and missile strikes highlight how oil, gas, digital, and water infrastructure represents both a direct and indirect vulnerability for the region's cities. The war on Iran consequently reveals the profound vulnerability inherent in the ultra-modern cities of the Persian Gulf. This exacerbates the fragility of these cities, even though the Gulf States are equipped with AI-enhanced air defence and cybersecurity systems.

The war on Iran thus exposes how the very development of Gulf cities constitutes a system of vulnerabilities and attack surfaces. It jeopardizes the dynamic of "AI augmentation" that underpins urban governance, including the operation of "smart cities."[9] In a context of persistent regional tensions, these cities must be understood not only as vulnerable strategic infrastructures, but also as cognitive environments where data, platforms, and algorithms shape perceptions and decision-making processes. Therefore, this article examines how the war on Iran inflicts complex impact systems on the cities of the Gulf, which, due to their modernity, offer a multitude of attack surfaces. How are the region's smart cities made especially vulnerable by the modernity and complexity of their design? How can this experience of war help integrate defence considerations into the AI-enhanced architectures of Gulf cities?

II. Cities and Hyperwar in the Gulf

On 28 February 2026, US and Israeli forces decapitated the Iranian government within an hour of launching their offensive. Salvos of missiles struck more than 1,000 targets on the first day alone.[10] The

6 Jean-Michel Valantin, Nathalie Glais, "AI, Warfare, Augmented Cities", *Small Wars Journal*, 4/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1Cry

7 Yergin, *The New Map.*

8 Jean-Michel Valantin, "China, Saudi Arabia and the Arab AI Rise", The Red Team Analysis Society, 31/1/2023, accessed on 29/4/2026 at: https://acr.ps/hBy1Cvf

9 Giorgio Cafiero, "Where the American-Israeli War on Iran Leaves the Gulf Arabs", Stimson Center, 25/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1CyW

10 AJ Labs, "Mapping US and Israeli Attack on Tiran and Teheran retaliatory strikes", *Al Jazeera*, 28/2/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1CZd

pace continued in the following days, accompanied by large-scale cyberattacks against the Islamic Republic.[11] The intensity and speed of the targeting, execution, precision, and strikes illustrate how the integration of AI is redefining contemporary warfare. From a regional geostrategic perspective, the US-Israeli offensive unfolds in a context shaped by the Gulf states' imperative to secure and defend their cities and the critical energy, digital, and water infrastructures on which their urban cohesion and economic development depend. These defence systems are based on the deployment of anti-missile and anti-drone capabilities, alongside increasingly sophisticated cyber defence systems.

These capabilities, largely purchased or leased from the US, are embedded within digital and AI architectures that operate at both the national level and in integration with US military systems, which are omnipresent in the region.[12] Their primary objective is the defence of oil, gas, petrochemical, port, and airport facilities. However, the functioning of Gulf cities, which are the true technological and economic incubators upholding national development, depends on these infrastructures.

Thus, the UAE has equipped itself with THAAD anti-missile batteries, while Qatar and Saudi Arabia have acquired several Patriot missile batteries. These weapon systems are coordinated with SAM (surface-to-air missile) batteries and anti-aircraft guns, as well as with air forces that deploy combat helicopters and fighter jets to intercept drones in flight. These systems and tactics are common to Qatar, Kuwait, Saudi Arabia, Bahrain, the United Arab Emirates, and Oman. It should be noted that Saudi Arabia also fields laser weapon systems, which are particularly effective against drones.[13] The effectiveness of these systems depends on uninterrupted access to air, maritime, and land-based data streams, enabling AI systems to generate early warnings.

The Islamic Revolutionary Guard Corps (IRGC) responded to the US-Israeli assault with widespread airstrikes and drone attacks across the Gulf countries targeting critical infrastructure such as airports and, a week later, desalination plants and airports. The strategic importance of these targets indicate high strategic intelligence. Conversely, the defensive and countermeasure systems deployed against these strikes, including anti-missile batteries, fighter jet and helicopter flights, and counter-drone drones, have been extremely effective. The combined effort of the Gulf States' own defence systems and the US armed forces reportedly intercepted around 90 per cent of incoming Iranian missiles and drones.[14] However, the remaining 10 per cent that reach their targets can inflict significant damage, given that the affected infrastructure – such as desalination plants and Kuwait's main airport – plays a vital role in sustaining both state functions and urban life in the region.

---

11 "Record pace of strikes in Iran bombing campaign: analysis", Airwars, 6/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1CCD

12 Tahir Azad, "The Hypersonic Dilemma: GCC States and the Future of Missile Procurement Post-Iran–Israel War 2025", *Small Wars Journal*, 10/9/2025, accessed on 29/4/2026 at: https://acr.ps/hBy1CGk

13 Arthur Vidal Ribe, "Defending the skies of the Arab Gulf States", IISS, 18/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1CK1

14 Frank A. Rose, "Air and Missile Defense in the Gulf", Arab Gulf States Institute, 18/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1CNI

III The Hyperwar on Infrastructure

Iranian attacks intensified, becoming more precise and accompanied by a particularly sustained cognitive warfare campaign. In cyberspace, Iranian cyber units flooded social media with deepfake images and videos designed to destabilize public opinion.[15] Meanwhile, Iranian strikes targeted oil and gas infrastructure across the Gulf States, as well as desalination plants and US and Saudi military bases holding US military aircraft.[16] Furthermore, reduced traffic through the Strait of Hormuz began to impact the revenues of the Gulf states. In Bahrain and the UAE, Iranian drone and missile strikes have damaged or destroyed oil facilities, as well as three Amazon data centres.[17] In Saudi Arabia, more than 16 attacks have damaged buildings in the suburbs of Riyadh and targeted the Prince Bandar il Sultan base, as well as oil facilities. In Qatar, several strikes have damaged the emirate's massive gas plant, resulting in a 17 per cent reduction in its production.[18]

On 7 and 8 March, strikes hit seawater desalination plants in Iran and Bahrain. While the damage was limited, more than thirty Bahraini villages were affected. Then, on 30 March, Iranian missile and drone strikes inflicted significant damage on one of Kuwait's main desalination plants. This prompted protests from Kuwait, Qatar, and the UAE, as desalination infrastructure is fundamental to sustaining urban life in one of the driest regions on Earth. This precision appears to have been enhanced by Chinese space-based intelligence capabilities, reportedly through the Shanghai-based Chinese company MizarVision, which specializes in geospatial information services.[19] This situation is reminiscent of the 2024 US State Department's denunciation of the support allegedly provided by Chang Guang Satellite Technology Corporation in supplying geospatial intelligence to the Houthi rebels in Yemen during their attacks in the Red Sea.[20]

Several GCC members are investing heavily in the integration and development of AI technologies. AI deployment is according guided by holistic strategies aimed at optimizing the extraction and management of resources such as oil, gas, and liquid helium, across the entire value chain, from upstream production to downstream distribution. It is also increasingly embedded in the daily functioning of cities.[21] From an urban perspective, AI is envisioned as a tool of improving the

15 Ellen Clark, Noor Hammad, Hasna Wajid, "Mapping the Damages: Iranian strikes on the GCC", *IISS*, 27/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1CUg

16 Priyanka Shankar, "Iran "hist" US AWACS, tankers: what else what else has it targeted last month ?", *Al Jazeera*, 27/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1CRp

17 Dennis Murphy, "Why Iran targeted Amazon data centers and what that does – and doesn't – change about warfare", *The Conversation*, 1/4/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1D6B

18 Spenser Kimball, "Iran missile attack on Qatar cause "huge damages" on facility housing huge gas plant", *CNBC*, 18/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1Dai

19 Henry Zwartz and Kathleen Calderwood, "Chinese satellite imagery of Middle East bases is helping Iran, US intelligence says", *ABC*, 5/4/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1C9V

20 Mohammad Salami, "China send Houthis dual use technology to boost influence and undercut the US", The Stimson Centre, 12/8/2025, accessed on 29/4/2026 at: https://acr.ps/hBy1D2U

21 Jean-Michel Valantin, "Petrodollars for AI – Is AI the Future of the Oil and Gas Industry", The Red Team Analysis Society, 7/10/2025, accessed on 29/4/2026 at: https://acr.ps/hBy1CV6

management of energy, water, vehicle, and population flows, as well as electricity consumption, building climate control, thereby shaping how cities in one of the world's most arid regions respond to extreme heat.

Furthermore, disruptions in the Strait of Hormuz, including allegations of mining activities and attacks on tankers attempting transit without clearance, have triggered a broader crisis affecting the export of oil, natural gas, fertilizers, and liquid helium from the Gulf states. This led to a sharp decline in revenues, while these economies are simultaneously facing a cascading set of pressures across multiple sectors. In this context, the sustainability of long-term AI development strategies could be called into question. These risks are further amplified by Iran's strategy of targeting the strategic Gulf infrastructure. Thus, on 30 March, Tehran threatened to strike the data centre associated with OpenAI's Stargate project in the UAE, an initiative that is expected to be accompanied by a $30 billion investment.[22]

IV Gulf Smart Cities in Danger

The strategic deployment of smart cities in the Gulf is generally approached through the lenses of innovation and efficiency, often at the expense of analysing their exposure to emerging forms of conflict such as cyberattacks, disinformation, and hybrid threats. Yet data- and algorithm-driven urban technologies introduce risks that fundamentally challenge existing models of urban governance.[23] This section analyses these vulnerabilities through three contrasting cases: Dubai, a globally optimized city; Riyadh, a strategic city under geopolitical constraints; and Doha, a model of proactive security.

Digital Infrastructures and Cyber Vulnerabilities

Smart cities in the Gulf are often designed as technological showcases, highlighting AI, data integration, and urban optimization. This focus on performance, however, raises a critical question: To what extent do these systems ensure security against cyber threats and risks to populations? Dependence on highly interconnected infrastructures, spanning digital networks, transport systems, energy grids, and decision-making centres, creates systemic vulnerabilities with consequences that can extend well beyond the technical domain.[24]

In Dubai, urban services are integrated via centralized platforms linking transport, energy, and security systems. While this architecture enhances efficiency, it also creates tightly coupled systems,

---

22 Sebastian Moss, "Iran threatens to attack OpenAI's Stargate data center in UAE", Data Centers Dynamics, 7/4/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1CYN

23 Alina Wernick and Anna Artyushina, "Future-proofing the City: A Human Rights-Based Approach to Governing Algorithmic, Biometric and Smart City Technologies", *Internet Policy Review* 12, no. 1 (2023).

24 Vasiliki Demertzi, Stavros Demertzis et Konstantinos Demertzis, "An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities", *Applied Sciences* 13, no. 2 (2023); Yee Ching Tok et Sudipta Chattopadhyay, "Identifying Threats, Cybercrime and Digital Forensic Opportunities in Smart City Infrastructure via Threat Modeling", *Forensic Science International: Digital Investigation* 45 (2023).

in which local disruptions can trigger cascading effects across the city, sometimes beyond the anticipatory capacity of existing control mechanisms.[25] In contrast, Riyadh exemplifies a model in which vulnerability is considered in the design of infrastructure from the outset. Smart city projects are embedded in state strategies that link governance, security, and critical infrastructure management, integrating technological development within an explicit framework of national defence and resilience.[26]

Cyber vulnerability thus transcends the technical realm to become a strategic and political issue. The Shamoon attack against Saudi Aramco in 2012, which paralysed tens of thousands of computer workstations, illustrates how a cyberattack targeting critical infrastructure can affect economic stability, governance capabilities, and public trust, well before the rise of smart cities as we understand them today.[27]

Urban Infrastructure, Security, and Physical Threats

Beyond cyber vulnerabilities, smart cities in the Gulf are exposed to physical and security threats that reveal the fragility of urban environments in a context of persistent regional tensions. Urban infrastructure, including energy systems, transport networks and surveillance devices, constitutes a set of critical assets whose disruption can generate immediate and far-reaching effects on political and economic stability.[28]

This physical vulnerability is particularly evident in Saudi Arabia. In September 2019, drone strikes on the Abqaiq and Khurais oil facilities temporarily disabled nearly half of Saudi Aramco's production, demonstrating that even heavily protected critical infrastructure remains exposed to asymmetric attacks.[29] In Riyadh, this experience accelerated the integration of smart city infrastructure into a broader national security architecture combining early detection, system redundancy, and centralized command centres.[30] Doha, for its part, illustrates a proactive security model geared towards risk management in dense urban environments. The deployment of advanced surveillance systems and crowd management technologies, implemented on a large scale during the 2022 World

---

25 Wael A. Samad and Elie Azar (dir.), *Smart Cities in the Gulf: Current State, Opportunities, and Challenges* (Singapore: Springer Nature, 2018); "The Rise of Gulf Smart Cities", Wilson Center, 2025, accessed on 29/4/2026 at: https://acr.ps/hBy1D2u

26 Samad and Azar, *Smart Cities in the Gulf*, p. 45; Alessandro Accorsi, "Disinformation Warfare in the Middle East", Center for Strategic and International Studies, 13/2/2025, accessed on 29/4/2026 at: https://acr.ps/hBy1D6b

27 Alaa Alsaeed, "The Cyber Attack on Saudi Aramco in 2012", *Asian Journal of Engineering and Applied Technology* 10 (2021).

28 Demertzi et al., "An Overview of Cyber Threats".

29 *2026 Annual Threat Assessment of the U.S. Intelligence Community*, Office of the Director of National Intelligence, 18/3/2026, accessed on 29/4/2026 at:https://acr.ps/hBy1D9S

30 Samad et Azar, *Smart Cities in the Gulf*, p. 45; Rachel George, "The Rise of Gulf Smart Cities", *Wilson Center*, 16/9/24, accessed on 29/4/2026 at: https://acr.ps/hBy1D2u; Mohammed Soliman and Alicia Chavy "Transformational Implications of Moving Toward Smart Cities in the Gulf", Middle East Institute, 12/12/2023, accessed on 29/4/2026 at: https://acr.ps/hBy1C9v;

Cup, demonstrates urban governance designed to absorb security shocks in highly digitized public spaces, which are in turn potentially vulnerable to targeted disruptions.[31]

These two cases reveal a structural trend: the boundary between civilian and security infrastructure is becoming increasingly blurred. Smart cities rely on dual-use technologies that, by integrating governance, surveillance, and defence into a single system, produce hybrid infrastructures whose resilience is becoming a national security issue in its own right.[32]

c. Informational and Cognitive Vulnerabilities

Beyond cyber and physical dimensions, smart cities in the Gulf are exposed to a third form of vulnerability: informational and cognitive. Based on real-time data, interconnected services, and algorithmic decision-making processes, they function as cognitive environments where infrastructure, data, and platforms shape not only urban governance but also the perceptions and behaviours of the population.[33] In Dubai, the flow of information is a critical dimension of urban functioning. In a highly digitized environment geared towards international appeal, disinformation campaigns can undermine public trust, disrupt data-driven decision-making systems, and damage the city's image, thus revealing the dependence of smart cities on the integrity of their information ecosystems.[34]

In Riyadh, cognitive vulnerability takes a distinct form. Digital transformation is accompanied by tighter regulation of information flows, including platform restrictions, legislative frameworks governing online content, and increased social media control.[35] This reflects a conception of information security as a core function of the state. Cognitive vulnerabilities thus result from both external threats – such as disinformation campaigns and the manipulation of public opinion – and from internal data governance choices that can, paradoxically, weaken public trust in digital institutions.[36] Contemporary threats are inherently cross-cutting, combining cyberattacks, disinformation, and AI in integrated influence strategies.[37]

In this context, the resilience of smart cities cannot be limited to the protection of physical and digital infrastructure; it must include the control of information flows, the maintenance of public trust, and

---

31 Council of Europe, *Safety, Security and Service at FIFA World Cup Qatar 2022* (Strasbourg: Council of Europe, 2023); Eleonora Ardemagni. "The Security Side of Qatar's World Cup", *Arab Gulf States Institute in Washington*, 2022, accessed on 29/4/2026 at: https://acr.ps/hBy1Cdc

32 George, "The Rise of Gulf Smart Cities"; Soliman and Chavy "Transformational Implications of Moving Toward Smart Cities in the Gulf".

33 Federico Cugurullo and Ying Xu. "When AIs Become Oracles: Generative Artificial Intelligence, Anticipatory Urban Governance, and the Future of Cities". *Policy and Society* 44, no. 1 (2025): 98-115, p. 100.

34 Marc Owen Jones, *Digital Authoritarianism in the Middle East: Deception, Disinformation and Social Media* (London: Hurst, 2022); Accorsi, "Disinformation Warfare in the Middle East".

35 Jones, *Digital Authoritarianism*, p. 45.

36 Accorsi, "Disinformation Warfare in the Middle East".

37 Christian Von Sikorski and Michael Hameleers, "Disinformation in the Age of Artificial Intelligence (AI): Implications for Journalism and Mass Communication", *Journalism & Mass Communication Quarterly* 102, no. 4 (2025); *2026 Annual Threat Assessment.*

the integrity of algorithmic governance systems.[38] The cyber, physical, and cognitive dimensions thus demonstrate that smart cities in the Gulf are not merely vulnerable technical infrastructures: they are cognitive and strategic environments whose governance requires an integrated risk management approach, capable of combining system protection, information control, and the maintenance of public legitimacy.

III. The Transformation of the Gulf States into Major Powers of Hyperwar

Rethinking the Defence and Security of "Augmented Cities"

The transformation of Gulf cities into "AI-augmented" urban systems necessitates a profound rethinking of their defence and security. Indeed, the war on Iran highlights the extent to which these cities function not only as built environments adapted to harsh natural conditions, but also as surfaces of attack. Failures or disruptions in urban regulatory and control systems expose them to a dual risk: the degradation of the technical infrastructures on which both economic activity and standards of living depend, and increased population exposure to water scarcity and extreme climate conditions. As a result, the broader development model of Gulf states is potentially called into question, given its reliance on vulnerable digital, economic, and water infrastructures.[39] Furthermore, the attacks on Bahraini and Kuwaiti desalination plants must be understood in their full strategic and symbolic complexity. They represent not only strikes against critical infrastructure, but also an attempt to reimpose the hostile environmental conditions of an arid, climate-stressed region onto the very urban systems designed to shield populations from them. This raises a final question: Could the Gulf cities emerge as the future powers of hyperwarfare?

Becoming the Urban Powers of the Hyperwar

The defence and securitization of Gulf cities reveal how these states are evolving into urban powers of hyperwarfare. This transformation began in the early 2020s with significant investments in the military applications of AI, including drones, missiles, space capabilities, and cyberwarfare. Abu Dhabi, the capital of the UAE, is both a smart city, recognized as such by the Smart City Index, and a major hub for investments in defence, AI technologies, and their militarization.[40] This dimension has become particularly salient in the context of the protracted conflict in Yemen since 2015, in which a coalition led by Saudi Arabia and the UAE has been engaged against Houthi forces.

---

38 Wernick and Artyushina, "Future-proofing the City": p. 5; Federico Cugurullo et al., "The Rise of AI Urbanism in Post-Smart Cities: A Critical Commentary on Urban Artificial Intelligence." *Urban Studies* 61, no. 6 (2024): 1168-1182, p. 1170.

39 Sanaam Mahoozi, "Iran and the Arabian Peninsula depend on desalination plants to survive – why water has become a target", *The Conversation*, 13/3/2026,
https://theconversation.com/iran-and-the-arabian-peninsula-depend-on-desalination-plants-to-survive-why-water-has-become-a-target-278142

40 Soner Dogan, "From Soldiers to Algorithms: AI and Autonomous Warfare in the UAE's Military Strategy", Dergi Park, 2026. https://dergipark.org.tr/en/pub/aybukulliye/article/1792824

However, in 2022, the growing mastery of missile and drone technologies by the Yemeni Houthi movement, supported by Iran, resulted in a series of attacks on UAE territory. More than four strikes were carried out using missiles and drones, including at least one against an Emirati oil complex.[41] Such attacks are highly strategic: they strike at the core of the UAE's economic infrastructure while simultaneously threatening broader regional stability, given that the Gulf region accounts for roughly 20 per cent of global daily oil production.[42]

Furthermore, in Qatar in 2026, while strategic foresight studies emphasize the importance of integrating AI into defence systems, this awareness has not yet been translated into concrete military policies. However, on 28 March 2026, the Qatari government signed a defence agreement with the Ukrainian government to benefit from the transfer of skills and technologies to strengthen the emirate's capacity to defend against Iranian drones and missile systems.[43] This partnership is all the more significant given Ukraine's internationally recognized experience in countering Russian attacks, often carried out using Iranian-made Shahed drones.[44] As in Qatar, this expertise has been developed in the defence of both critical infrastructure and urban environments. On 27 March, President Volodymyr Zelensky similarly concluded an agreement with Saudi Arabia, driven by the same strategic considerations. This indicates that a substantial transfer of experience, skills, and technologies is underway between Ukraine, the initial testing ground for hyperwarfare, and the Gulf states, which are now integrating these capabilities at a time when the entire region is sliding into hyperwar.[45]

As illustrated by the actions of the Qatari and Saudi governments, defence imperatives and wartime conditions accelerate the adoption of new technologies, generating strategic advantages, not only in military terms, but also in strengthening social cohesion and the protection of critical infrastructure. As in Ukraine, Iran's multi-domain conflict against its neighbours underscores the vital importance of safeguarding cities across both physical and cyber domains, including digital infrastructure. Moreover, the interplay between US "smart" offensives and Iranian reprisals, particularly strikes on data centres and threats against big tech companies, further emphasize the role of AI n the evolving strategic landscape of the region. Therefore, one short-term consequence of the war is likely to be the strengthening of AI governance by states, and, by extension, by cities, alongside a much deeper integration of defence considerations understood in a multi-domain sense.

---

41 Dr Sidhart Kaushal, "Lessons from the Houthi Missile Attacks on the UAE", RUSI, 3/2/2022, accessed on 29/4/2026 at: https://acr.ps/hBy1CgT

42 Jean-Michel Valantin and Nathalie Glais, "AI, Warfare and Augmented Cities", *Small Wars Journal*, 4/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1Cry

43 Max Hunder and Yulia Diisia, "Ukraine deploys unit to 5 Middle East Countries to operate drones", *Defense News*, 20/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1CkA

44 "Ukraine signs 10-year defence pact with Qatar as it eyes broader Gulf cooperation", *France 24*, 28/3/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1Coh

45 Jean-Michel Valantin, "AI at War (1)- Ukraine", The Red Team Analysis Society, 8/4/2026, accessed on 29/4/2026 at: https://acr.ps/hBy1CrY

Bibliography

Cugurullo, Federico, Federico Caprotti, Matthew Cook, Andrew Karvonen, Pauline McGuirk and Simon Marvin. "The Rise of AI Urbanism in Post-Smart Cities: A Critical Commentary on Urban Artificial Intelligence." *Urban Studies* 61, no. 6 (2024) : 1168 - 1182.

Cugurullo, Federico and Ying Xu. "When AIs Become Oracles: Generative Artificial Intelligence, Anticipatory Urban Governance, and the Future of Cities". *Policy and Society* 44, no. 1 (2025): 98 - 115.

Council of Europe. *Safety, Security and Service at FIFA World Cup Qatar 2022.* Strasbourg: Council of Europe, 2023.

Demertzi, Vasiliki, Stavros Demertzis and Konstantinos Demertzis. "An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities". *Applied Sciences* 13, no. 2 (2023).

Jones, Marc Owen. *Digital Authoritarianism in the Middle East: Deception, Disinformation, and Social Media*. London: Hurst/Oxford University Press, 2022.

Morris, Ian. *War! What is it good for? Conflict and the Progress of Civilization, from primates to robots,* New-York: Farrar, Strauss & Giroux, 2014.

Samad, Wael A. et Elie Azar (dir.). *Smart Cities in the Gulf: Current State, Opportunities, and Challenges.* Singapore: Springer Nature, 2018.

Tok, Yee Ching and Sudipta Chattopadhyay. "Identifying Threats, Cybercrime and Digital Forensic Opportunities in Smart City Infrastructure via Threat Modeling". *Forensic Science International: Digital Investigation* 45 (2023).

Valantin, Jean-Michel, *Hyperguerre, Quand l'IA révolutionne la guerre*, Paris: Nouveau Monde Éditions, 2024.

Von Sikorski, Christian et Michael Hameleers. « Disinformation in the Age of Artificial Intelligence (AI): Implications for Journalism and Mass Communication. » *Journalism & Mass Communication Quarterly* 102, no. 4 (2025).

Wernick, Alina et Anna Artyushina. "Future-proofing the City: A Human Rights-Based Approach to Governing Algorithmic, Biometric and Smart City Technologies". *Internet Policy Review* 12, no. 1 (2023).