

INTERNATIONAL RELATIONS, INTERNATIONAL SECURITY AND GEOPOLITICS

DOI: 10.46340/eppd.2026.13.3.1

ARTIFICIAL INTELLIGENCE, ESCALATION DYNAMICS, AND REGIONAL SECURITY IN THE PERSIAN GULF: A RISK-RESILIENCE ANALYSIS

Levan Cholikidze¹, Doctor of Computer Science; Qetevan Kveselava¹,
Academic Doctor of Informatics Engineering; Maia Gamsakhurdia¹,
PhD in International Relations

¹Georgian Technical University, Georgia

Corresponding author: Maia Gamsakhurdia; Email: mgamsakhurdia@eta.edu.ge

Citation: Cholikidze, L., Kveselava, Q., & Gamsakhurdia, M. (2026). Artificial Intelligence, Escalation Dynamics, and Regional Security in the Persian Gulf: A Risk-Resilience Analysis. *Evropský politický a právní diskurz*, 13, 3, 5-15. <https://doi.org/10.46340/eppd.2026.13.3.1>

Abstract

This conference article examines how artificial intelligence (AI) may increase or reduce military escalation and strategic risk in the Persian Gulf. The paper develops a risk-resilience framework that treats AI not as a single technology, but as a cluster of decision-support, surveillance, cyber, autonomous, predictive, and infrastructure-management capabilities. The analysis is based on four recent open-source studies: Al Neyadi's analysis of AI and Gulf energy security, Atalan's assessment of AI infrastructure resilience, Miller and Wright's article on U.S.-China AI competition in the Arab Gulf, and Nasser bin Nasser's UNIDIR study on AI, regional threat perceptions, and weapons of mass destruction risk. These sources are interpreted together with open data from the U.S. Energy Information Administration and the International Energy Agency. The article argues that AI can reduce risk when it improves early warning, infrastructure monitoring, predictive maintenance, maritime domain awareness, and crisis communication. However, AI can also amplify escalation by compressing decision time, widening the target set to include data centres and cloud infrastructure, increasing cyber and information-operation risks, and intensifying great-power technological competition. The Persian Gulf is a particularly important case because energy chokepoints, military rivalry, critical digital infrastructure, and sovereign AI ambitions overlap in a compact and strategically sensitive space. The paper concludes that AI will contribute to regional stability only if it is embedded in governance mechanisms that prioritize human control, model auditability, infrastructure redundancy, cross-border confidence-building, and restraint in the military use of autonomous and predictive systems.

Keywords: artificial intelligence, Persian Gulf, regional security, military escalation, energy security, strategic stability, WMD risk, AI governance, critical infrastructure.

Introduction

Artificial intelligence has become a central variable in contemporary debates on regional security. Earlier security studies often treated AI as a distant technological possibility or as a narrow military

© Cholikidze, L., Kveselava, Q., & Gamsakhurdia, M., 2026. This is an Open Access article, distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International. It gives an opportunity to read, to load, to copy out, to expand, to print, to search, to quote or to refer to the full text of the article in this Journal.

capability, but this view is no longer sufficient. AI now affects surveillance, logistics, intelligence analysis, cyber defense, autonomous systems, public communication, energy management, and the protection of critical infrastructure. In conflict-prone regions, these applications matter because they can alter the speed, scale, and interpretation of state behavior. A radar alert classified by a machine-learning system, a cyber anomaly detected inside an energy facility, a drone swarm monitored by automated tools, or a sudden disruption of cloud services may become part of the same strategic crisis. For this reason, AI must be analyzed as a political and security variable, not merely as a technical innovation.

The Persian Gulf provides a particularly important case for this analysis. The region combines several features that make AI security effects visible. It contains critical energy routes, especially the Strait of Hormuz, which the U.S. Energy Information Administration identifies as one of the world's most important oil chokepoints. In 2024, oil flow through the strait averaged about 20 million barrels per day, equal to roughly one-fifth of global petroleum liquids consumption, while a significant share of global liquefied natural gas trade also passed through the same maritime space (U.S. Energy Information Administration [EIA], 2025). The Gulf also contains persistent military rivalries, particularly involving Iran, the Gulf monarchies, Israel, and the United States. In addition, Gulf states are investing heavily in sovereign AI capability, hyperscale data centers, cloud infrastructure, and digital transformation. These three layers - energy exposure, military tension, and AI ambition - create a complex environment in which AI can become both a stabilizing tool and a new source of vulnerability.

This article asks the following research question: How can artificial intelligence increase or decrease military escalation and strategic risks in the Persian Gulf? The central argument is that AI produces dual effects. It can strengthen resilience by improving warning, forecasting, infrastructure management, maritime monitoring, and crisis response. Yet it can also increase escalation by compressing decision time, producing opaque assessments, encouraging preemptive action, expanding the range of strategic targets, and deepening great-power competition over technology ecosystems. The paper therefore rejects two simplified positions: technological optimism, which assumes that better information automatically produces restraint, and technological pessimism, which assumes that AI inevitably destabilizes regional security. The more accurate conclusion is conditional: AI can support stability only when it is governed, audited, embedded in human decision-making, and supported by resilient infrastructure.

Methodology and Source Base

The paper uses qualitative comparative source analysis. This method is appropriate because many military and intelligence applications of AI remain classified, commercially sensitive, or only partially visible in open sources. Rather than claiming to provide a statistical measurement of AI's impact, the article compares the arguments, assumptions, and policy implications of four recent open-source studies. Al Neyadi (2026) is used to analyze the connection between AI, energy security, and the Iranian conflict. Atalan (2026) is used to examine the vulnerability of AI infrastructure itself, especially data centers, cloud regions, and continuity requirements. Miller and Wright (2025) provide a theoretical lens for understanding AI as technological statecraft in U.S.-China competition in the Gulf. Nasser bin Nasser (2025) adds the regional arms-race, threat-perception, and WMD-risk dimension.

The four sources are not identical in genre. One is an academic journal article, one is a UNIDIR policy report, and two are contemporary policy analyses. This diversity is useful because the subject lies between academic security studies and rapidly evolving policy practice. The article also uses supplementary open sources from the EIA, the IEA, the U.S. Navy, OpenAI, G42, and CSIS in order to situate the four main texts in the broader empirical context. The EIA is especially relevant because the Gulf's security significance cannot be separated from maritime energy flows. The IEA is used to establish the energy-AI nexus: data centers require reliable electricity, while AI can also optimize energy systems. Official and policy sources on Stargate UAE and Task Force 59 illustrate how AI infrastructure and AI-enabled maritime operations are moving from abstract ambition into practical regional security planning.

The analysis proceeds in five steps. First, it defines AI as a risk-resilience technology. Second, it identifies the Persian Gulf's strategic exposure. Third, it analyzes the four core sources. Fourth, it maps escalation and de-escalation pathways. Fifth, it proposes governance and policy options. The method is interpretive and analytical rather than predictive. Its goal is not to forecast a single crisis scenario, but to build a structured framework that can be used by researchers, policymakers, and military planners to evaluate how AI interacts with regional conflict dynamics.

Table 1

Core Source Matrix

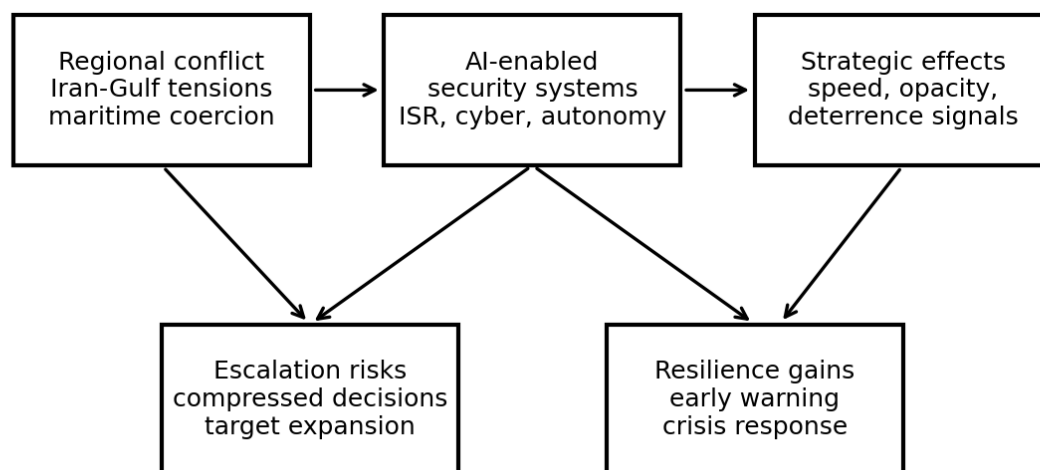
Source	Primary focus	AI mechanism	Escalation relevance	Resilience relevance
Al Neyadi (2026)	AI, energy security, and the Iranian conflict in the Gulf	AI as a tool for forecasting, network resilience, and crisis response	Energy infrastructure becomes more exposed when conflict threatens both oil flows and power-dependent digital systems	AI can improve predictive maintenance, demand forecasting, and continuity planning but cannot substitute for geopolitical restraint
Atalan (2026)	Resilience of Gulf AI infrastructure amid conflict	AI as infrastructure requiring data centers, chips, power, connectivity, and customer confidence	Cloud regions and AI campuses may become strategic targets or sources of investor uncertainty	Trusted infrastructure, redundancy, and continuity planning reduce the vulnerability of sovereign compute strategies
Miller & Wright (2025)	U.S.-China AI competition and technological statecraft in the Gulf	AI as geopolitical leverage across defense and economic domains	AI partnerships may intensify alignment pressure, export-control disputes, and strategic hedging	Gulf states can use AI partnerships to increase strategic autonomy if safeguards and diversification are managed
Nasser bin Nasser (2025)	AI, threat perceptions, arms racing, and WMD-free zone negotiations	AI as a military enabler affecting autonomy, cyber, delivery systems, and arms-control verification	AI can increase misperception, arms-race dynamics, and WMD-related risks	AI can also support verification, risk assessment, and technical arms-control processes

Conceptual Framework: AI as a Risk-Resilience Technology

The article defines AI as a risk-resilience technology. This concept means that the same set of capabilities can either increase insecurity or reduce vulnerability depending on operational design, political context, and governance. AI is a risk technology when it accelerates military decision-making beyond the pace of human deliberation, produces recommendations that commanders cannot fully interpret, expands cyber-attack surfaces, or enables autonomous and semi-autonomous systems to operate in contested environments. AI is a resilience technology when it improves warning, clarifies the operating picture, detects infrastructure anomalies, reduces uncertainty, and helps civilian and military authorities respond to shocks with greater accuracy.

The risk side begins with speed. A Gulf crisis could involve drones, missiles, cyber incidents, maritime harassment, energy disruptions, and information operations occurring almost simultaneously. AI-enabled systems may process these events faster than traditional command structures. Speed can be beneficial, but it can also create pressure to act before political leaders have clarified intent. This is especially dangerous when states interpret ambiguous signals through existing threat perceptions. In a militarized environment, a defensive action may look offensive, a cyber anomaly may look like preparation for a strike, and an AI-generated risk score may be treated as evidence rather than as a probabilistic assessment.

The resilience side begins with information. AI can integrate satellite imagery, maritime automatic identification system data, radar feeds, port activity, cyber logs, energy-grid signals, and open-source



**Figure 1. AI, Conflict, and Regional Security in the Persian Gulf:
Analytical Framework**

Note. Original visualization prepared by the author based on the synthesis of Al Neyadi (2026), Atalan (2026), Miller and Wright (2025), and Nasser bin Nasser (2025).

intelligence. Used carefully, this integration can reduce uncertainty and support de-escalation. For example, if an incident near the Strait of Hormuz can be attributed more accurately and quickly, decision makers may avoid unnecessary retaliation. If AI-based monitoring detects stress in oil terminals, LNG facilities, data centers, or electricity grids before failure occurs, authorities can prepare redundancy and continuity measures. The same technology therefore belongs simultaneously to the logic of escalation and the logic of resilience.

The Persian Gulf as a Strategic Case

The Persian Gulf is not only a regional security environment; it is a global energy and technology-security node. Its geography makes local escalation internationally consequential. According to EIA (2025), about 20 million barrels per day of oil moved through the Strait of Hormuz in 2024, representing approximately 20% of global petroleum liquids consumption. The same source notes that flows through the strait represented more than one-quarter of total global seaborne oil trade and that around one-fifth of global LNG trade also transited the strait, largely from Qatar. These figures mean that an incident involving mines, drones, missiles, tanker seizures, cyber disruption, or port attacks can affect not only regional actors but also Asian markets, European energy calculations, global shipping insurance, and inflation expectations.

The importance of Hormuz also explains why AI is relevant to regional security. Modern maritime security depends increasingly on data fusion, pattern recognition, unmanned systems, and rapid anomaly detection. The U.S. Navy's Task Group 59.1, launched in 2024, focuses on the operational deployment of unmanned systems teamed with manned operators to strengthen maritime security across the Middle East region (United States Navy, 2024). Such initiatives show that AI-enabled maritime domain awareness is already part of the Gulf security environment. However, these systems also introduce new questions: Who controls the data? How reliable are automated classifications? What happens when an unmanned platform is jammed, spoofed, captured, or misidentified? How can states prevent AI-assisted surveillance from being interpreted as preparation for offensive action?

The Gulf is also becoming a major AI infrastructure space. OpenAI (2025) announced Stargate UAE as the first international deployment of its Stargate AI infrastructure platform, including a 1 GW cluster in Abu Dhabi, with 200 MW expected to go live in 2026. G42 (2025) similarly describes Stargate UAE as a 1 GW compute cluster within a wider 5 GW UAE-U.S. AI Campus. These projects demonstrate that Gulf AI ambition is not rhetorical. It has a physical footprint in data centers, electricity contracts, cooling systems, cyber defenses, fiber routes, advanced chips, and international technology partnerships. Therefore, AI does not only analyze conflict; it becomes part of the conflict environment. In a severe regional crisis, data centers and cloud regions may be considered economically and strategically important infrastructure.

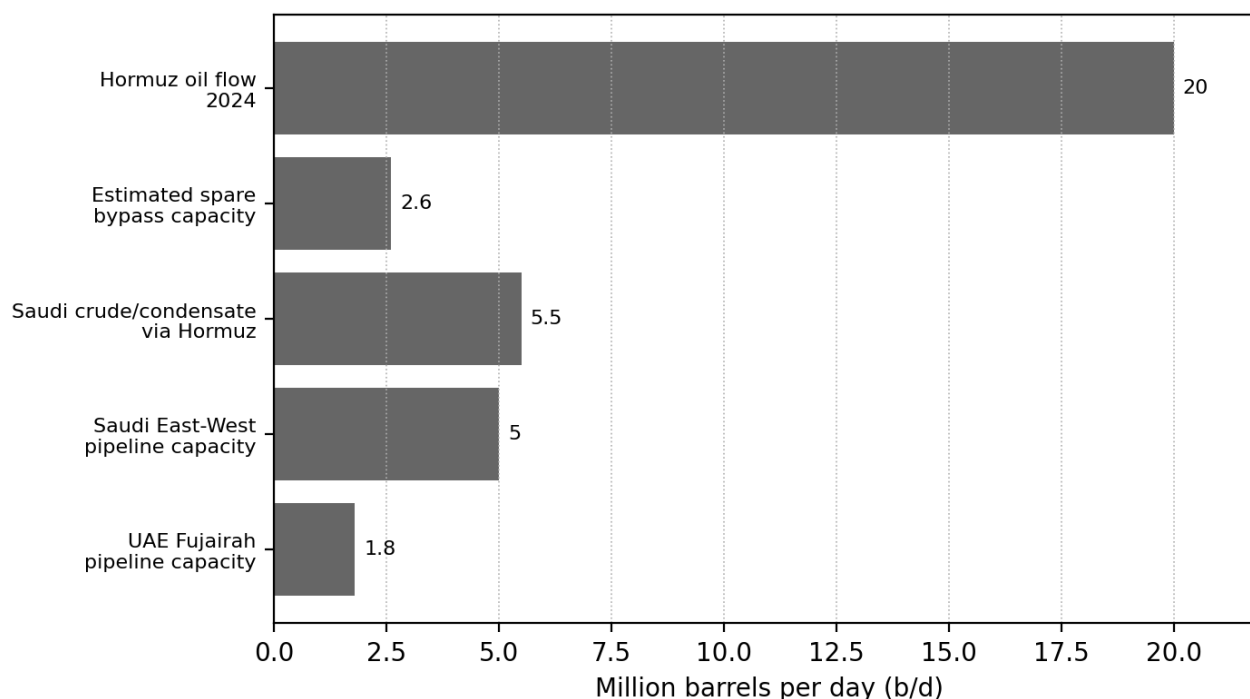


Figure 2. Energy Exposure Around the Strait of Hormuz

Note. Original chart prepared from EIA (2025) indicators. Values are expressed in million barrels per day where applicable.

Analysis of the Four Core Sources

AI and Energy Security: Al Neyadi (2026)

Al Neyadi (2026) offers the most direct connection between AI, energy security, and Gulf conflict dynamics. The study argues that missile and naval threats to refineries, LNG terminals, and the Strait of Hormuz intersect with the region's rapid expansion of AI-driven infrastructure. This is a significant analytical move because it refuses to treat energy security and digital transformation as separate policy domains. In the Gulf, AI infrastructure requires stable electricity, cooling, networks, and physical security. At the same time, AI can support the protection and optimization of energy systems. The result is an interdependence: energy enables AI, while AI may help secure energy.

For escalation analysis, the key insight is that the target set expands. Traditional Gulf security studies focused on tankers, ports, offshore platforms, pipelines, refineries, airbases, and missile-defense systems. Al Neyadi's argument suggests that data centers, fiber-optic networks, energy-intensive cooling systems, and cloud dependencies must also be included. A strike that damages a port or refinery may also disrupt digital services. Conversely, an attack on a cloud region or data center may affect energy-sector operations, logistics, banking, public services, and emergency coordination. This creates a wider and more complex crisis environment.

The resilience implication is equally important. AI can improve predictive maintenance, demand forecasting, smart-grid management, supply-chain visibility, and crisis decision support. These capabilities can reduce the strategic impact of disruption. However, Al Neyadi's analysis also implies a limitation: AI cannot remove the political causes of escalation. It can reduce uncertainty and improve response capacity, but it cannot substitute for diplomacy, deterrence management, or regional risk-reduction mechanisms. This distinction is essential for a balanced academic conclusion.

AI Infrastructure as Critical Security Infrastructure: Atalan (2026)

Atalan (2026) shifts attention from AI applications to AI infrastructure. This is one of the most important contributions for a Persian Gulf case study because AI is often discussed as software, models, or algorithms, while the real-world system depends on data centers, chips, electricity, cooling, cloud

redundancy, physical protection, and insurance. Atalan argues that Gulf AI strategy must move from capital and scale toward resilience, continuity, and trusted infrastructure. This reframing is highly relevant because Gulf states seek to become global AI hubs at the same time that regional conflict exposes the vulnerability of large fixed infrastructure.

The article's significance lies in showing that AI infrastructure can become a strategic object. If data centers, cloud regions, or AI campuses are perceived as part of national power, they may be exposed to coercion. They can be attacked physically, targeted through cyber operations, undermined through supply-chain pressure, or affected by investor perceptions of risk. AI infrastructure also depends on imported advanced chips and global technology partnerships. In a crisis, export controls, sanctions, disrupted shipping, or insurance restrictions may affect the ability to build or operate sovereign compute systems.

From a resilience perspective, Atalan's logic points toward redundancy. Gulf AI strategies require not only powerful data centers but also distributed backups, hardened power supply, trusted connectivity, incident response, and transparent security standards. A state that concentrates AI infrastructure in a small number of visible facilities may increase efficiency but also create high-value targets. Therefore, the resilience question is not whether the Gulf can build AI capacity, but whether it can keep that capacity operating during military tension, cyber incidents, energy shocks, or maritime disruption.

Technological Statecraft and Great-Power Competition: Miller and Wright (2025)

Miller and Wright (2025) provide the strongest theoretical framework among the four core sources. They argue that military AI should be conceptualized as technological statecraft, especially in the Gulf, where AI has the potential to reshape regional security and economic order. Their article places Gulf AI within the broader transition from U.S. predominance toward a more multipolar and contested international system. The United States remains central to Gulf security doctrine, while China is a major economic partner and technology actor. AI therefore becomes a domain in which Gulf states seek capability, autonomy, and bargaining power.

This argument matters for escalation dynamics because AI partnerships are not politically neutral. Access to advanced chips, cloud infrastructure, data governance frameworks, military AI systems, and cybersecurity standards can pull Gulf states toward competing technology ecosystems. Export-control disputes, concerns about technology leakage, and pressure to align with U.S. or Chinese standards may influence defense procurement and strategic trust. AI may therefore intensify alliance politics even when Gulf states prefer strategic diversification.

At the same time, technological statecraft can produce resilience through strategic autonomy. Gulf states are not passive recipients of outside technology. They use AI partnerships to diversify economies, modernize defense institutions, and increase bargaining power. If managed carefully, this autonomy may reduce overdependence on any single external patron. If managed poorly, it may create fragmented systems, incompatible standards, intelligence-sharing concerns, and suspicions about dual-use technology transfer. Miller and Wright's contribution is therefore crucial: AI is not only a battlefield technology; it is a diplomatic, economic, and alliance instrument.

AI, Threat Perceptions, and WMD Risk: Nasser bin Nasser (2025)

Nasser bin Nasser (2025) broadens the analysis from conventional conflict to regional threat perceptions, arms-race dynamics, and WMD-related risks. The UNIDIR report is valuable because it treats AI as a technology that can influence both the development of military capabilities and the political interpretation of those capabilities. This is especially important in the Middle East, where distrust, secrecy, proxy conflict, missile programs, and nuclear concerns interact with conventional military competition.

AI may increase WMD-related risk in several ways. It can improve the precision, navigation, and autonomy of delivery systems. It can accelerate research and development in sensitive scientific domains. It can support cyber operations against command, control, communications, and intelligence systems. It can also intensify suspicion if states believe that rivals are using AI to gain a rapid strategic advantage. In this context, the problem is not only the actual capability but also the perceived capability. Threat perceptions can drive arms-race behavior even when information is incomplete.

However, the UNIDIR report also indicates that AI can support risk reduction. AI tools may assist verification, monitoring, anomaly detection, and technical assessment in arms-control processes. In a future Middle East WMD-Free Zone negotiation framework, AI could help process large data sets, identify inconsistencies, and support confidence-building. The challenge is governance. A verification tool that one

side sees as neutral may be seen by another as intrusive intelligence collection. Therefore, AI-enabled arms control would require transparency, agreed standards, and institutional trust.

Escalation Pathways

The combined analysis of the four sources suggests four main escalation pathways in the Persian Gulf. The first is decision-speed compression. AI systems can accelerate detection, classification, and recommendation. In a missile or drone incident, decision makers may receive AI-generated assessments quickly, but those assessments may contain uncertainty that is difficult to communicate. A probabilistic warning can become politically powerful when leaders face pressure to respond. The risk is not simply that machines decide; it is that humans may over-trust machine outputs under time pressure.

The second pathway is target expansion. As Gulf economies digitize and AI infrastructure becomes strategically valuable, the target set expands from traditional military and energy assets to data centers, cloud regions, undersea cables, chip supply chains, and AI operations centers. This does not mean that every actor will attack these assets directly. It means that their vulnerability becomes relevant in coercive signaling, cyber competition, insurance markets, and crisis planning. Atalan (2026) and Al Neyadi (2026) are especially important here because they show that AI infrastructure and energy infrastructure are increasingly interdependent.

The third pathway is opacity and misperception. AI systems may produce outputs that are difficult to explain. In a crisis, a state may not know whether a rival's unusual deployment reflects human intent, algorithmic error, automated response, deception, or defensive precaution. This uncertainty can produce worst-case interpretation. In the Gulf, where air, sea, cyber, and proxy domains interact, misperception can move quickly from local incident to regional confrontation.

The fourth pathway is great-power entanglement. Miller and Wright (2025) show that AI competition in the Gulf is also U.S.-China competition. A crisis involving AI infrastructure, chip exports, cyber intrusion, or data-center security may therefore involve external powers even if the original dispute is regional. The danger is that local escalation could be interpreted through the lens of global technological rivalry. This is particularly important for Gulf states that seek to balance security reliance on the United States with economic ties to China.

Table 2

AI-Related Escalation Pathways and Mitigation Options

Risk pathway	Mechanism	Possible Gulf effect	Risk-reduction measure
Decision-speed compression	AI accelerates detection and recommendation in missile, drone, maritime, or cyber incidents.	Leaders may respond before intent is clarified.	Human authorization, confidence thresholds, and crisis consultation windows.
Target expansion	AI infrastructure depends on fixed data centers, power, cooling, and connectivity.	Data centers and cloud regions become coercive targets.	Critical-infrastructure designation, redundancy, and hardened continuity planning.
Cyber and data manipulation	AI systems depend on data integrity and secure networks.	Data poisoning or spoofing can create false warning or operational disruption.	Model audit, secure data pipelines, red-team testing, and incident reporting.
Great-power entanglement	AI partnerships connect Gulf security to U.S.-China technological competition.	Local incidents may be interpreted through global rivalry.	Transparent technology safeguards and balanced strategic communication.
Arms-race and WMD-related risk	AI can improve delivery systems, research speed, and threat assessment.	Rivals may assume rapid hidden capability gains.	AI risk dialogue, verification tools, and nonproliferation norms.

High AI reliability	Fast but opaque risk compression	Resilient crisis management
Low AI reliability	High escalation likelihood	Managed but fragile resilience
	Low governance coordination	High governance coordination

Figure 3. AI Risk-Resilience Outcomes in a Gulf Crisis

Note. Qualitative matrix developed by the author to synthesize the risk-resilience logic of the four core sources.

De-escalation and Resilience Pathways

The same sources also point to important de-escalation pathways. First, AI can improve early warning. In maritime security, AI-assisted systems can identify suspicious movement, detect spoofed signals, correlate drone activity with vessel behavior, and help authorities distinguish routine activity from hostile preparation. Earlier warning creates more time for political consultation and reduces the chance of surprise. However, early warning stabilizes only when it is accompanied by disciplined interpretation and communication.

Second, AI can improve infrastructure resilience. Predictive maintenance in pipelines, refineries, LNG terminals, electricity grids, and data centers can reduce failure during periods of stress. The IEA (2025) notes that AI is already used in the oil and gas industry to optimize operations, detect leaks, predict maintenance needs, and improve safety. In a Gulf context, these capabilities can help operators prioritize repairs, anticipate overloads, and maintain continuity during crises. They can also support emergency planning for hospitals, ports, financial systems, and military logistics.

Third, AI can improve crisis response. In a complex regional event, decision makers must process military reports, shipping data, cyber alerts, energy-market signals, diplomatic messages, and public narratives. AI can help organize these inputs and identify contradictions. It can also support scenario analysis and resource allocation. The benefit is not that AI replaces judgment, but that it helps human institutions avoid information overload.

Fourth, AI can support confidence-building and arms-control verification. Nasser bin Nasser (2025) emphasizes the relevance of AI for threat perceptions and the Middle East WMD-Free Zone initiative. If institutional trust exists, AI can help analyze compliance data, detect anomalies, and support technical dialogue. This role is especially important because the Middle East lacks a dense regional security architecture. Carefully governed AI tools could help create shared situational awareness, but only if their data sources, assumptions, and limits are transparent enough to be politically acceptable.

Discussion: Conditions Under Which AI Stabilizes or Destabilizes

AI stabilizes Gulf security only under specific conditions. The first condition is human control. Human control does not mean slow decision-making; it means that commanders and civilian leaders understand what an AI system is recommending, what data it used, what uncertainty remains, and what consequences may follow. Human review is especially important for actions that could be interpreted as offensive, such as strikes, cyber operations, electronic warfare, or maritime interdictions.

Table 3

AI as a Resilience Instrument in the Persian Gulf

Resilience domain	AI contribution	Expected benefit	Governance limitation
Energy resilience	Predictive maintenance, demand forecasting, grid management, leak detection	Lower probability of cascading failure during conflict	Requires electricity, cyber security, and operator trust
Maritime security	AI-assisted ISR, unmanned systems, anomaly detection, route risk analysis	Better warning and more complete maritime domain awareness	Risk of misidentification or provocative surveillance
Crisis management	Data fusion, scenario analysis, logistics prioritization, public communication support	Reduced information overload and faster coordination	Risk of overreliance on opaque recommendations
Arms control and verification	Pattern detection, satellite-image analysis, compliance support, anomaly identification	Improved technical monitoring and negotiation support	May be viewed as intrusive or intelligence-driven without agreed rules

The second condition is auditability. AI systems used in regional security should be tested, documented, and reviewed. In crisis environments, an unexplained output can become a strategic liability. Auditability helps institutions determine whether a warning was based on reliable data, biased training, sensor error, adversarial manipulation, or excessive model confidence. This is particularly relevant to the Gulf because the operating environment includes heat, dust, maritime clutter, electronic interference, spoofing, and dense commercial traffic.

The third condition is infrastructure redundancy. Sovereign AI requires more than national ambition. It requires electricity, cooling, cyber defense, physical security, backup sites, trusted suppliers, and resilient connectivity. The IEA (2025) shows that data-center electricity demand is growing rapidly, while OpenAI (2025) and G42 (2025) indicate the scale of future Gulf AI infrastructure. In a region exposed to missiles, drones, cyber operations, and maritime disruption, AI infrastructure must be planned as critical national infrastructure.

The fourth condition is diplomatic signaling. AI-enabled surveillance and unmanned systems can be stabilizing if they increase transparency, but destabilizing if they look like preparation for attack. Gulf states and external partners need crisis communication channels that include AI and cyber incidents. A drone malfunction, data-center outage, cyber false alarm, or algorithmic misclassification should not automatically become a military escalation trigger. Governance must therefore include technical hotlines, incident-notification protocols, and shared language for AI-related uncertainty.

Policy Recommendations

First, Gulf states should adopt AI security doctrines that clearly separate decision support from automated use of force. Any AI system used for targeting, cyber retaliation, or maritime interdiction should remain subject to human authorization. The doctrine should specify acceptable uses, prohibited uses, and review procedures. Such clarity would reduce the risk of accidental escalation and increase the credibility of restraint. International experience offers useful reference points. NATO's revised AI strategy emphasizes lawfulness, responsibility and accountability, explainability and traceability, reliability, governability, and bias mitigation as principles for responsible defense use (North Atlantic Treaty Organization [NATO], 2024). For civilian and critical-infrastructure applications, the NIST AI Risk Management Framework similarly stresses trustworthiness, design-stage risk management, and evaluation across the life cycle (National Institute of Standards and Technology [NIST], 2023). These frameworks cannot be transferred mechanically to the Persian Gulf, but they provide language for doctrine, audit, testing, and procurement.

Second, AI infrastructure should be included in national critical infrastructure protection plans. Data centers, cloud regions, semiconductor supply chains, cooling systems, backup generators, fiber routes, and cyber operations centers should be protected with the same seriousness as ports, refineries, LNG terminals, and airbases. This recommendation follows from Atalan's (2026) infrastructure emphasis and Al Neyadi's (2026) energy-AI linkage.

Third, regional maritime domain awareness should be strengthened through AI-enabled but human-supervised systems. Unmanned surface, aerial, and underwater systems can help monitor chokepoints and protect shipping, but their deployment should be accompanied by procedures for identification, deconfliction, and incident reporting. The experience of Task Force 59 and Task Group 59.1 demonstrates the operational relevance of unmanned and AI-enabled systems, but operational speed must be matched with political risk management.

Fourth, Gulf states should develop a regional AI incident dialogue. Existing security dialogues often focus on missiles, nuclear issues, maritime incidents, and conventional deterrence. AI adds new categories: model failure, cyber-physical manipulation, data poisoning, cloud disruption, and autonomous-system incidents. Even if a comprehensive regional security architecture remains politically difficult, technical working groups could begin with narrow issues such as AI in maritime safety, energy infrastructure monitoring, and cyber incident notification.

Fifth, external partners should avoid forcing Gulf states into rigid technology blocs. Miller and Wright (2025) show that Gulf states seek agency and strategic autonomy amid U.S.-China competition. Excessive pressure could encourage hedging, secrecy, or fragmented systems. A more effective approach would combine security safeguards, export-control clarity, trusted-vendor standards, and transparent cooperation. This would reduce technology-leakage concerns while respecting Gulf states' development ambitions.

Sixth, arms-control and nonproliferation institutions should prepare for AI-enabled verification and AI-related risk. Nasser bin Nasser (2025) suggests that AI can both increase and reduce WMD-related risks. Regional and international institutions should therefore study how AI affects delivery systems, cyber operations, biological research, nuclear safety, and verification. The goal should not be to ban all AI use in security contexts, which is unrealistic, but to establish norms that reduce destabilizing applications while allowing defensive and verification functions.

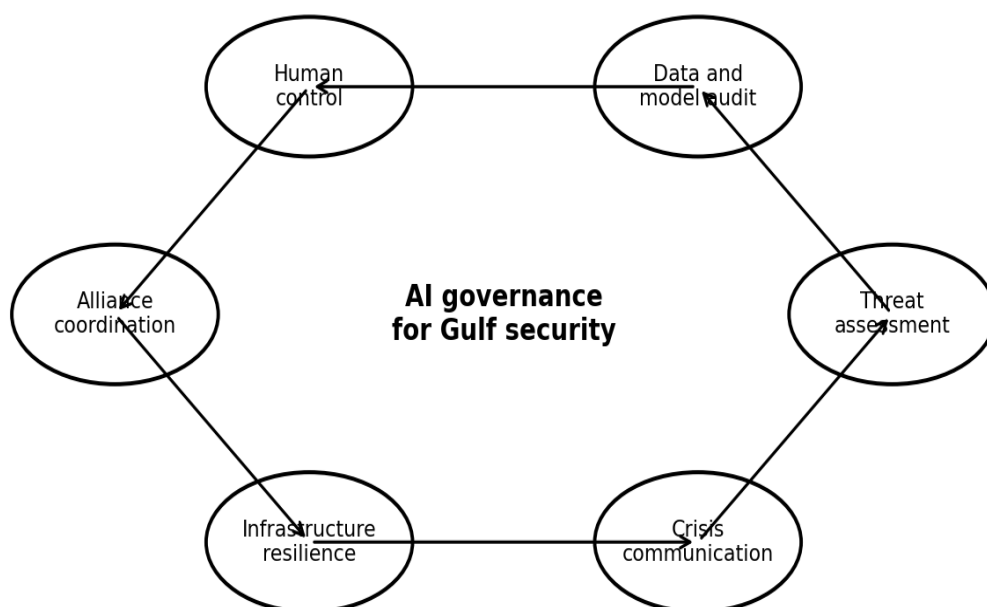


Figure 4. Governance Cycle for Risk Reduction and Resilience

Note. Original policy-cycle diagram prepared by the author.

Conclusion

AI will not determine the future of Persian Gulf security by itself. It will interact with geography, energy dependence, military rivalry, alliance politics, infrastructure investment, and regional threat perceptions. The four core sources analyzed in this article show that AI has dual effects. It can strengthen resilience through early warning, predictive maintenance, energy optimization, maritime surveillance, crisis response, and verification support. It can also increase escalation by compressing decision time, expanding strategic targets, intensifying cyber and information risks, deepening great-power competition, and affecting WMD-related threat perceptions.

The Persian Gulf is a critical case because energy chokepoints and AI infrastructure now overlap. The Strait of Hormuz remains central to global energy security, while Gulf states are attempting to build sovereign AI capacity and become global technology hubs. This creates a new strategic equation: the security of oil, gas, electricity, data centers, cloud systems, and AI models can no longer be analyzed separately. A disruption in one layer may cascade into others.

The article's main conclusion is conditional. AI can reduce military escalation and regional risk only if it is embedded in governance structures that prioritize human control, auditability, redundancy, resilience, and crisis communication. Without these safeguards, AI may magnify insecurity by accelerating decisions, obscuring responsibility, and creating new high-value targets. Therefore, the policy task for Gulf states and their partners is not simply to acquire more AI capability, but to design AI systems and institutions that remain reliable under crisis conditions. In the Persian Gulf, the strategic value of AI will depend less on technological sophistication alone and more on whether the region can convert technological power into disciplined, transparent, and resilient security governance.

Acknowledgements: none.

Conflict of Interests: none.

References:

- Al Neyadi, S. S. S. (2026, May 8). Artificial Intelligence and Energy Security in the Gulf: Strategic Implications of the Iranian Conflict. *TRENDS Research & Advisory*.
<https://trendsresearch.org/insight/artificial-intelligence-and-energy-security-in-the-gulf-strategic-implications-of-the-iranian-conflict/>
- Allen, G. C., Adamson, G., Heim, L., & Winter-Levy, S. (2025). The United Arab Emirates' AI ambitions: Key Implications for Maintaining U.S. AI leadership. *Center for Strategic and International Studies*.
<https://www.csis.org/analysis/united-arab-emirates-ai-ambitions>
- Atalan, Y. (2026, May 4). The Gulf's AI Strategy Needs Resiliency. *Arab Gulf States Institute in Washington*.
<https://agsi.org/analysis/the-gulfs-ai-strategy-needs-resiliency/>
- G42. (2025, May 22). *Global Tech Alliance Launches Stargate UAE*.
<https://www.g42.ai/resources/news/global-tech-alliance-launches-stargate-uae>
- International Energy Agency. (2025). *Energy and AI*. <https://www.iea.org/reports/energy-and-ai>
- Miller, R., & Wright, S. (2025). US-China AI Competition in the Arab Gulf: Diverging Uses of Technological Statecraft on the Regional Level. *Alternatives: Global, Local, Political*.
<https://doi.org/10.1177/03043754251377866>
- Nasser bin Nasser. (2025). The Impact of Artificial Intelligence on Regional Security, Threat Perceptions and the Middle East WMD-Free Zone. *UNIDIR*.
<https://doi.org/10.37559/MEWMDFZ/2025/ZoneAI>
- National Institute of Standards and Technology. (2023). *Artificial Intelligence risk management framework (AI RMF 1.0)*. U.S. Department of Commerce. <https://www.nist.gov/itl/ai-risk-management-framework>
- North Atlantic Treaty Organization. (2024, July 10). *Summary of NATO's revised artificial intelligence (AI) strategy*.
<https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/07/10/summary-of-natos-revised-artificial-intelligence-ai-strategy>
- OpenAI. (2025, May 22). *Introducing Stargate UAE*. <https://openai.com/index/introducing-stargate-uae/>
- U.S. Energy Information Administration. (2025, June 16). *Amid regional conflict, the Strait of Hormuz Remains Critical Oil Chokepoint*. <https://www.eia.gov/todayinenergy/detail.php?id=65504>
- United States Navy. (2024, January 16). *Task Force 59 launches new unmanned task group 59.1*.
<https://www.navy.mil/Press-Office/News-Stories/Article/3645647/task-force-59-launches-new-unmanned-task-group-591/>