مركز البيان للدراسات والتخطيط
Al-Bayan Center for Studies and Planning

2026/6/27

Iraq and the New Calculations of War
A Precautionary Reading of Iraqi National Security Threats, Armament Options, and Rebuilding Deterrence (2026-2035)

Dr. Amer Abd Rasan Jaafar Al-Moussawi

● Research Paper

Al-Bayan Center Studies Series

Research Paper

2026/6/27

Iraq and the New Calculations of War

A Precautionary Reading of Iraqi National Security Threats, Armament Options, and Rebuilding Deterrence (2026-2035)

Series of publications of Al-Bayan Center for Studies and Planning
Research Department / Security and Military Studies

Publication / Research Paper

Topic / Security and Defense / Domestic and Foreign Policy

Dr. Amer Abd Rasan Jaafar Al-Moussawi / Former Chief of Experts at the National Security Advisory and Former Deputy Head of the Intelligence Service

---

About

Al-Bayan Center for Planning and Studies is an independent, nonprofit think tank based in Baghdad, Iraq. Its primary mission is to offer an authentic perspective on public and foreign policy issues related to Iraq and the region.

Al-Bayan Center pursues its vision by conducting independent analysis, as well as proposing workable solutions for complex issues that concern policymakers and academics.

www.bayancenter.org
info@bayancenter.org
Since 2014

Abstract

This paper argues that the war on Iran, which began on February 28, 2026, and ended later, revealed a structural shift in the nature of contemporary warfare, with direct implications for the Iraqi national security environment. The war demonstrated that modern conflicts are no longer confined to traditional confrontations between states, but have increasingly taken the form of data-centric, attritional hybrid operations characterized by the intensive use of drones. In this new environment, cost asymmetry, flexibility of command structures, speed of adaptation, and intelligence integration have become factors that may rival, or perhaps exceed, the importance of conventional military superiority.

The paper also analyzes how this war revealed the limits of relying on rapid coercive victory, the rising importance of low-cost autonomous systems, the strategic value of data and intelligence integration, as well as the vulnerability of critical infrastructure to multi-domain attacks. Furthermore, the paper examines Iraq's exposure to the secondary and tertiary effects of this conflict, including energy disruptions, financial pressures, indirect strikes, the regional arms race, and the potential resurgence of technologically adaptive extremist

actors in Syria and on the western approaches to Iraq.

The study proposes an Iraqi precautionary framework for the period 2026-2035, based on building a multi-layered air defense, developing a national drone capability, establishing a national data architecture, integrating intelligence work, protecting critical infrastructure, developing strategic deception capabilities, and nurturing young talent in the fields of artificial intelligence, cyber capabilities, and modern security studies. The paper concludes that future Iraqi deterrence will not depend solely on the quality of weapons Iraq acquires, but rather on its ability to build a resilient state that possesses an institutional structure capable of learning, adapting, and enduring in the era of smart, networked, and open-ended warfare.

Introduction

The recent war on Iran since February 28, 2026, has revealed a highly important strategic reality: the Middle East (and perhaps the world) is no longer facing a conventional war whose outcomes are measured solely by the number of air sorties or the intensity of bombardment, but rather a radical transformation in the very nature of conflict itself. Field

developments, Iran's continued ability to respond despite surgical strikes, escalating pressures on energy markets, and the maritime corridors crisis all indicate that modern wars have come to be characterized by operational ambiguity, political uncertainty, and technological and logistical attrition, rather than rapid resolution or swift victory.[1]

The significance of this transformation has been reinforced by conflicting US statements regarding the course of the war. Conflicting positions emerged from US President Donald Trump regarding whether the war was nearing its end or was still in its early stages, reflecting, in a strategic reading, the growing difficulty of predicting the outcomes of modern wars, even for the world's greatest military power, going beyond mere passing media confusion. This issue takes on particular importance for Iraq; as the inability of the prominent international actor to decisively estimate the end of the war means that countries located within the zone of direct regional repercussions will be more vulnerable to the risks of exposure and miscalculation,

1. International press reports indicate a near-halt of navigation in the Strait of Hormuz and the accompanying disruption in global energy markets and high levels of economic uncertainty; see: Oil prices rise and markets fall after US seizure of ship hits Strait of Hormuz, The Guardian, April 20, 2026, available at the link: https://www.theguardian.com/business/2026/apr/20/oil-prices-rise-markets-fall-us-iran-ftse-100-gas-strait-of-hormuz.

unless they take the initiative to update their security and military doctrine on more flexible and proactive foundations.[2]

The current experience also shows that destroying part of the command structure, or targeting sensitive military and security sites, does not necessarily mean achieving the political objectives of the war, particularly the goal of regime change. US intelligence assessments, published by the American press, indicated that the Iranian regime, despite being weakened, remained cohesive and might even lean toward greater radicalism with the rising role of the Revolutionary Guard. Furthermore, published data so far does not show any mass transition within the Iranian security apparatus toward an organized opposition, or a decisive split in the power structure. This establishes a fundamental lesson for Iraq, namely that the survival of the state in modern wars is linked not only to the size of the blow it receives, but also to the flexibility of its institutional structure and its ability to reshape and adapt under pressure.[3]

2. International media reports addressed the conflicting US statements regarding the course of the war, including statements by the US President on whether the war is nearing its end or is still in its early stages; available at this link: https://www.pbs.org/newshour/politics/a-timeline-of-trumps-shifting-statements-about-how-long-the-iran-war-will-last.

3. As US intelligence assessments, reported by the American press, indicated that the military strikes targeting the Iranian leadership and security infrastructure did not lead to a decisive weakening of the regime or

For Iraq, this scene is read not merely as regional monitoring, but through the lens of redefining Iraqi national security. The war proved that the threats Iraq might face during the coming decade will come not only from conventional armies, but from hybrid, decentralized, drone-heavy, highly attritional, and multi-theater wars. It also proved that conventional deterrence is no longer sufficient, and that systems that do not update their armament, intelligence, and data doctrines will become exposed before lower-cost and more flexible adversaries.[4]

First: The War on Iran as a Laboratory for Future Wars

The recent war provided a practical model for what can be termed "Precise Mass," where precision is no longer exclusive to high-cost platforms but has become capable of mass quantitative production through low-cost and densely deployed systems. In this context, aggregated data from defense and analytical sources indicate that the United Arab Emirates was the most exposed to attacks, facing approximately 2,200-2,250 drones and more than 500 missiles during the war period, while Kuwait ranked second with about 850 drones and nearly 350-

a collapse in its cohesion, but rather that the Revolutionary Guard may increase in influence in light of the escalating conflict; see: The Washington Post, U.S. intelligence says Iran's regime is consolidating power, March 16, 2026.

4. See: The Washington Post, the same previous source.

370 missiles. This clearly reflects the transition of warfare from the logic of "a few superior platforms" to the logic of a "dense, smart, low-cost mass," confirming the shift in the balance of power from qualitative superiority to the capacity for quantitative saturation and long-term attrition.[5]

Reuters data regarding the Ukrainian interceptor drone "STING" confirms this trend; as a relatively low-cost system can become part of an effective defensive equation against "Shahed" drones, illustrating that the economics of war are turned upside down when relatively cheap tools can overcome more costly defenses in the field, or when states are forced to use expensive interception methods against low-priced targets. This equation shows that the problem is no longer purely technological, but has become industrial, financial, and operational all at once.[6]

5. As data issued by military analyses and research centers indicate that the United Arab Emirates faced approximately 2,256 drones and 563 missiles, while the State of Kuwait was exposed to about 852 drones and 369 missiles during the recent war, with similar figures recorded in other sources indicating that the UAE was the largest target of the attacks compared to the rest of the Gulf states; see: Long War Journal, Iran's war against regional states: UAE bore the brunt, April 18, 2026.
6. Reuters. (2026, March 17). Inside the Ukrainian interceptor drones wanted around the Gulf. Reuters. https://www.reuters.com/business/aerospace-defense/inside-ukrainian-interceptor-drones-wanted-around-gulf-2026-03-17/.

More dangerously, Iran did not manage its defense with a purely traditional centralized logic, but within a more flexible and decentralized structure, described by some experts in published coverage as a "mosaic strategy," allowing for the continuation of the ability to fight even with a partial disruption in command or communication. The intention here is not to call for a literal imitation of this model, but to point out that organizational flexibility and the multiplicity of operational nodes may become, in certain environments, more effective than rigid centralization, which could collapse if its top node is targeted. This is a highly important Iraqi lesson in an environment where geography and asymmetric threats overlap, and the space of vulnerable infrastructure expands.[7]

Second: What Does This War Mean for Iraq Security-wise?

Iraq lies at the center of the region's most sensitive geography, and it faces the danger not of a single war, but rather the risk of turning into a permanent arena for the repercussions of others' wars. The strikes that hit energy facilities, airports, and ports in the Gulf, along with the shipping disruptions in the Strait of Hormuz, send a direct signal regarding the vulnerability of critical infrastructure when confrontations shift to the level

7. See: The Washington Post, the same previous source.

of complex and simultaneous attacks. Iraq, with its oil fields, refineries, ports, power stations, water, and telecommunication facilities, will be highly vulnerable to this type of targeting if these assets are not integrated into an explicit and comprehensive definition of national security, based on physical protection, cyber fortification, and raising proactive readiness in the face of regional escalation scenarios.[8]

Likewise, the exposure of the Iraqi depth to the model of the recent hybrid war does not pertain to direct military attacks alone, but extends to include economic pressure, psychological disruption, communication disruption, targeting of symbols, and market destabilization. This threat becomes more acute in light of the overlap between the state and non-state actors, between the security and economic files, and between the center and the peripheries. Consequently, any modern Iraqi vision of national security should treat the energy, water, telecommunications, transport, and financial sectors as security arenas vulnerable to targeting and disruption, rather than just traditional service sectors.[9]

8. The Guardian, Oil prices rise and markets fall after US seizure of ship hits Strait of Hormuz, April 20, 2026.
9. Cybersecurity and Infrastructure Security Agency. (n.d.). Be Air Aware™. U.S. Department of Homeland Security. https://www.cisa.gov/topics/physical-security/be-air-aware (CISA).

Thirdly, the current war has proven that advanced conflict tools are no longer exclusive to major powers. Drone capabilities, commercial satellite imagery, flexible communication technologies, and cyber warfare tools have become available in varying degrees to smaller actors, including armed groups and trans-border networks. This means that Iraqi national security is threatened not only from the outside, but also from within and from soft border areas, if it is not built upon an integrated deterrence, monitoring, and tracking system capable of distinguishing between conventional and non-conventional action, and identifying its launch sites with high accuracy.

Third: The Most Important Lesson... Failure of the Bet on Rapid Military Resolution

One of the most prominent lessons of the war is that technological superiority does not necessarily equate to political victory. Published assessments showed that the American and Israeli strikes, despite their intensity and breadth, did not lead to the collapse of the Iranian regime or the dissolution of its coercive apparatuses. In fact, some analyses went so far as to suggest that the Revolutionary Guard emerged from the war more centralized within the power structure, which means

that violent targeting may weaken the adversary materially without producing the desired political outcome.

This lesson matters to Iraq on two levels. First, defending the state relies not only on possessing weapons, but on the cohesion of the political and institutional structure and its ability to continue functioning under pressure. Second, any Iraqi armament doctrine built on the logic of a short war or rapid resolution will be a flawed doctrine. What is required is a doctrine capable of managing attrition, protecting the national depth, maintaining operations, and preserving the state's capacity to function in the midst of strikes and disruptions.[10]

Fourth: What Needs to Change in Iraqi Armament Plans?

Iraq needs a fundamental reconsideration of its armament philosophy. The issue is no longer just buying the "best" weapon, but building an integrated system capable of endurance, resilience, and expansion:

- First: Building a multi-layered air defense dedicated to drones and short- and medium-range missiles, rather than limiting the bet to high-cost strategic systems. Modern NATO documents confirm that effective air and

10. See: The Washington Post, the same previous source.

missile defense must be integrated, multi-domain, and rapid in decision-making, and must also include small, slow, and low-altitude targets as well.[11]

- Second: Establishing a national Iraqi drone force that is not limited to importation, but includes tactical reconnaissance drones, low-cost attack drones, local production or assembly capabilities, and specialized units for squadron management. However, the essence of this force lies not only in its technical possession, but in subjecting it to the complete and exclusive control of the state's central security decision-making, thereby ensuring the monopoly on the legitimate use of this weapon and preventing any deployment outside the institutional framework. This requires, unequivocally, the imposition of full sovereignty over low-altitude airspace, so that no unofficial entity-including armed factions-is permitted to possess or operate drones outside the state's system, or to use them in a manner that exposes Iraq to the risks of being dragged into regional conflicts or threatening neighboring countries. It is also necessary

11. North Atlantic Treaty Organization. (2025, February 13). NATO integrated air and missile defence policy. https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/02/13/nato-integrated-air-and-missile-defence-policy (NATO).

to prevent the transformation of Iraqi airspace into a transit corridor for drones belonging to other countries or non-governmental platforms, by building an effective detection, interception, and jamming system, and linking it to a unified central command and control. At the same time, this force should be built on a calculated measure of operational flexibility that allows for rapid response to wartime conditions through disciplined field-level delegation of authority and accelerated decision mechanisms, without undermining the principle of unity of command and control. The challenge lies not in possessing drones per se, but in regulating their use sovereignly, preventing their politicization or evasion of control, and transforming them from a potential source of threat into a disciplined national deterrence tool. Modern Western trends, as expressed by Kathleen Hicks in the Replicator initiative, focus on platforms that are "small, smart, cheap, and many," rather than on the expensive standalone piece alone. For Iraq, this means shifting from the logic of the "symbolic platform" to the logic of "dense networked capability" linked to a centralized command that is smart and flexible at the same time.[12]

12. Hicks, K. (2023, September 6). Deputy Secretary of Defense Kath-

- Third: Establishing a national databank for aerial and cyber threats, because modern warfare is decided by data as much as it is decided by iron and fire. This includes a unified database for target patterns, trajectories, frequencies, and communication profiles, while integrating it among military intelligence, national security, the intelligence service, and air defense, and employing artificial intelligence for early warning and pattern discovery. This approach has become aligned with CISA warnings regarding drone threats to infrastructure, and with NATO trends in integrated situational awareness.[13]
- Fourth: Rebuilding defense industries on realistic foundations, through partial localization of the manufacturing of drones and simple smart munitions, calculated technological partnerships, linking universities and research centers to military and security needs, and involving the disciplined private sector in certain phases of manufacturing and assembly. Continuous reliance

leen Hicks' remarks: "Unpacking the Replicator initiative" at the Defense News Conference. U.S. Department of Defense. https://www.defense.gov/News/Speeches/Speech/Article/3517213/deputy-secretary-of-defense-kathleen-hicks-remarks-unpacking-the-replicator-ini/ (U.S. Department of Defense).

13. See: Cybersecurity and Infrastructure Security Agency CISA, the same previous source.

on imports creates political and technical vulnerability, especially in a country situated between two main schools in this field: the Turkish school with its organized industrial-export character, and the Iranian school with its dense, low-cost, and flexible character.[14]

Fifth: Rebuilding the Iraqi Intelligence Mindset in the Era of Smart Warfare

The required transformation is no longer just military, but has become a shift in the philosophy of information collection, management, and utilization. Modern war is not managed by weapons alone, but is managed first and foremost by data. The governing rule today is no longer: who possesses the greater power, but rather: who possesses the most accurate information, processes it the fastest, and deceives his adversary with higher intelligence. This aligns with the general trend in modern warfare, where drones, artificial intelligence, commercial imagery, flexible communications, and cyber tools integrate into a single structure for decision and strike.[15]

For this reason, Iraq needs to transition from the concept of

14. Baykar Technologies. (2026, January 31). Baykar remains global UCAV export leader in 2025. https://baykartech.com/en/press/baykar-remains-global-ucav-export-leader-in-2025/ (Baykar Tech).
15. See: The Washington Post, the same previous source.

"information gathering" to the concept of building a dynamic national databank that includes drone flight patterns and trajectories, communication and linking frequencies, maps of potential threats, and adversary behavior in real time. Furthermore, this system must be built by integrating HUMINT, OSINT, low-cost sensing, commercial data, and available satellite imagery, rather than falling into the illusion that modern intelligence means complex technology alone. The value of the system lies not in the tool itself, but in the linking, analysis, and timing.[16]

Moreover, introducing artificial intelligence into pattern discovery, threat prediction, image analysis, and real-time decision support is no longer an institutional luxury, but an operational necessity. What is required here is not the elimination of the human role, but multiplying his capacity and reducing his response time. Therefore, it is necessary to transition from the multiplicity of agencies to a unified intelligence mind by establishing a national information fusion center that links National Security, Intelligence, Military Intelligence, and Air Defense within a common operational picture, allowing for the building of a unified situational

16. See: Cybersecurity and Infrastructure Security Agency CISA, the same previous source.

awareness, and higher coordination in threat management and decision-making.[17] Precautionary defense begins with early and accurate information, not just late interception.

Strategic deception-from misleading movement patterns to creating fake targets and broadcasting deceptive signals-has also become an inherent part of modern warfare. The battle is not limited to detecting the enemy, but extends to disrupting his awareness and spoiling his decisions. Consequently, energy, water, telecommunications, and all critical infrastructure must be redefined as primary intelligence targets, because targeting them in the context of modern warfare may be more impactful than striking a direct military target, given the resulting widespread functional paralysis that affects both the state and society simultaneously.[18]

Sixth: The Most Dangerous Scenarios for Iraq - An Expanded Intelligence Reading

In light of current data, particularly the continued closure of the Strait of Hormuz and the disruption of an important part of global energy shipping, Iraq faces not just conventional

17. See: North Atlantic Treaty Organization. (2025, February 13). NATO, the same previous source.
18. See: Cybersecurity and Infrastructure Security Agency CISA, the same previous source.

repercussions of war, but a matrix of complex and accelerating threats with deep economic, security, and strategic dimensions.

The first scenario is represented by the transformation of the conflict into a state of open regional attrition, where the impact is no longer confined to the direct confrontation arena but has extended to affect the arteries of the global economy. The closure of the Strait-through which a large portion of global oil exports passes-has led to sharp disruption in energy markets, increased insurance and maritime transport costs, and growing commercial risks, which directly reflects on the Iraqi economy as a rentier economy dependent on oil exports. In this context, Iraq faces a complex equation:

- On one hand, oil prices may rise, boosting revenues in the short term;
- On the other hand, risks multiply regarding the continuity of export and safety of supplies, in addition to higher shipping and insurance costs, and potential disruptions to supply chains.
- Furthermore, the continuation of this situation imposes increasing pressure on public finances, with an expanding need for security and military spending to protect vital facilities and export lines, at a time when the

capacity for stable economic planning is eroding.

Thus, the threat is no longer confined to the "war" itself, but lies in the transformation of the region's economic geography into an arena of protracted conflict, wherein Iraq becomes part of the attrition equation, whether as a direct party or a recipient of its repercussions.[19]

The second scenario is the possibility of the war's return and the escalation of indirect strikes within Iraq, whether via airspace, facilities, soft arenas, or unofficial actors. The attacks on oil infrastructure and military bases, which were officially condemned by the Iraqi Government and the Presidency of the Republic, show that this danger is no longer hypothetical.[20]

As for the most dangerous scenario from an intelligence perspective, it is the return of Takfiri threats in a more developed form. With major powers preoccupied with the war, and the erosion of some traditional centers of influence in the Levant, the capabilities of Takfiri groups in Syria (including ISIS and its likes) may grow, benefiting from security vacuums,

19. See: The Guardian, April 20, 2026, the same previous source.
20. Presidency of the Republic of Iraq. (2025, July 15). Statement by the Presidency on rocket and drone attacks targeting critical infrastructure in the Kurdistan Region and Kirkuk. https://www.presidency.iq/en/Details.aspx?id=5655 (presidency.iq).

asymmetric tactics, and low-cost drone technologies that have proven their impact in modern wars. In such a scenario, Iraq could face a new wave of infiltration across its western borders, complex security, media, and cyber operations, and an attempt to reproduce the 2014 model but with more advanced tools. This is not an inevitability, but a precautionary hypothesis that should be treated with high seriousness.[21]

Added to this is the risk of an unequal regional arms race, as Iranian attacks in the Gulf have prompted increased attention to interception solutions and counter-drone systems, including growing interest in low-cost Ukrainian interceptor aircraft. This could pressure Iraq into entering a costly arms race if it does not manage its priorities rationally and gradually.[22]

Finally, there is a dangerous challenge represented by the erosion of internal deterrence. If the Iraqi security decision-making structure remains divided, slow, or unintegrated, any modern threat-whether a small drone, a sleeper cell, or a focused cyber campaign-will exploit this fragmentation quickly. Hence, the most dangerous aspect of the upcoming phase may not be the war itself, but what comes after it in

21. See: The Washington Post, the same previous source.
22. See: Reuters. (2026, March 17), the same previous source.

terms of vacuums, repositioning, and the birth of new threats in the shadows.[23]

Seventh: The Required Iraqi Precautionary Vision - From Conventional Security to Data-Driven and Proactive Security

In light of the previous transformations, Iraq does not need to clone the experiences of others, but rather to build a purely Iraqi precautionary approach that is based on understanding its complex environment and balancing conventional and emerging threats. This approach begins with intelligence proactivity rather than military reaction, meaning discovering the threat before it forms, dismantling networks before they move, and reading transformations in Syria and the western borders early on. The upcoming battle will not be fought at the borders only, but before reaching them.[24]

This vision also requires building a unified security mind instead of institutional fragmentation, through a national information fusion center, and real integration between the army, national security, intelligence, military intelligence, and air defense, resulting in a unified security decision built

23. See: North Atlantic Treaty Organization. (2025, February 13). NATO, the same previous source.
24. See: The Washington Post, the same previous source.

on a common operational picture. Data must be the pillar of national deterrence, including a national databank for aerial, cyber, and field threats, pattern analysis, and the employment of artificial intelligence in prediction and response.[25] In terms of armament, there must be a transition toward low-cost smart defense instead of financial attrition, in light of the equation: the adversary spends less, and the defender spends more.

It is also necessary to precaution against the return of Takfiri threats with new technologies by securing borders through smart means, not just human forces, penetrating these groups through intelligence, and anticipating their formation rather than waiting for their movement. Similarly, oil, electricity, water, and telecommunications should be included within the definition of the first line of defense, rather than being considered separate service sectors.[26]

This vision is completed by localizing security and military technology as much as possible, building strategic deception and disruption capabilities, and, most importantly, investing in young cadres. Iraq possesses a latent wealth of top-

25. See: North Atlantic Treaty Organization. (2025, February 13). NATO, the same previous source.
26. See: Cybersecurity and Infrastructure Security Agency CISA, the same previous source.

ranking graduates, science university alumni, and talents in programming, engineering, and communications, but these energies remain outside the strategic deployment of the state. Therefore, it becomes essential to launch a national program to attract and nurture young elites in the fields of artificial intelligence, cybersecurity, drone systems, data analysis, and modern military and security sciences, because weapons can be bought, but the mind that manages war cannot be bought; it is built and nurtured. This is a pivotal point if Iraq wishes to build a cognitive infrastructure for national security in the coming decade.[27]

Eighth: The Specific Challenge of Drones in the Iraqi Environment

Regarding drones, Iraq must precaution with the logic of a state, not the logic of a weapons deal. By virtue of geography, Iraq is situated between Turkey, a major player in drone export and industrial development, and Iran, which has accumulated extensive experience in producing low-cost drones and their supply networks. Furthermore, the drone threat has come to encompass both states and non-state actors alike. Therefore, the correct question is not: should we buy drones? Rather, it

27. See: The Washington Post, the same previous source.

is: how do we build a low-cost air sovereignty system, both offensive and defensive, that is capable of resilience and expansion?[28]

On the acquisition side as a weapon, Iraq does not need to start with large, complex drones, but rather with a graduated hierarchy of capabilities: a layer for permanent reconnaissance and surveillance, a tactical layer to support units on the borders, in the desert, and at facilities, and a limited layer for precision strikes when necessary within a strict central decision framework. The mistake is purchasing expensive platforms as a symbol of power, whereas the correct approach is building a dense, flexible, and rapidly replaceable system, aligned with modern Western trends that focus on speed, flexibility, and network integration.[29]

On the side of precaution against them as a threat, the best approach for Iraq is not "weapon against weapon," but rather a multi-layered C-UAS system: monitoring, then discrimination, then tracking, then disabling or interception, and finally post-

28. See: Baykar Technologies. (2026, January 31), the same previous source.
29. Hicks, K. (2023, September 7). Hicks discusses Replicator initiative. U.S. Department of Defense. https://www.defense.gov/News/News-Stories/Article/article/3518827/hicks-discusses-replicator-initiative/ (U.S. Department of Defense).

incident management. NATO documents and CISA guidelines emphasize that effective defense against modern aerial threats should be 360-degree, multi-domain, flexible, and rapid in decision-making, and must include small, slow, and low-altitude threats as well, not just missiles. Moreover, protecting infrastructure from drone threats has become an independent file in modern US guidelines.[30]

Practically, Iraq requires nine parallel tracks:

1. A unified national command for drones and counter-drones;
2. A national priority map for protection that includes holy shrines, decision-making centers, air bases, radars, oil fields, refineries, dams, power stations, telecommunication lines, prisons, and the Central Bank;
3. A low-altitude detection network;
4. Disciplined electronic warfare and jamming;
5. Low-cost interception;
6. Supplier diversification and non-dependence;
7. Partial localization of assembly, maintenance, and software;

30. See: North Atlantic Treaty Organization. (2025, February 13). NATO, the same previous source.

8. A national databank for aerial threats; and finally,
9. Legal and regulatory protection of low-altitude airspace.

The need for these tracks has become more urgent in light of proven attacks on oil infrastructure in Iraq, and in light of international warnings regarding the risks of drones to critical infrastructure.[31]

31. See: (presidency.iq) Presidency of the Republic of Iraq. (2025, July 15)., the same previous source.

Conclusion: Iraq Facing the Test of Strategic Awareness

The war on Iran reveals not only a regional conflict, but the birth of a new equation of war: no rapid victory is guaranteed, technological superiority alone is insufficient, and no defense is possible without industrial, data, and intelligence flexibility. Most importantly, it revealed that regimes possessing structural resilience and the ability to distribute strikes and reshape decision-making are capable of enduring even under harsh blows.[32]

For Iraq, the deepest lesson is that national security in the coming decade (2026-2035) will not be safeguarded solely by high-cost tanks and aircraft, but by drones, data, artificial intelligence, jamming and control of the electromagnetic spectrum, and the capacity for long-term endurance. Therefore, the Iraqi strategic question is no longer: what weapon do we buy? Rather, it has become: how do we build a defense system for the state that possesses an intelligence mind, a database, and a flexible architecture, capable of survival, deterrence, and adaptation in the era of smart warfare and open-ended attrition?

32. See: The Washington Post, the same previous source.

In this era, whoever fails to read the transformations of war early on will later pay the price in their sovereignty, resources, and internal stability. As for the state that invests today in knowledge, data, young talents, and institutional integration, it does not merely buy its security, but builds it.

For an Active state and a participating society

www.bayancenter.org
info@bayancenter.org