



Anatomy of Asymmetry: How a Weaker State Converts Vulnerability into Leverage

Dr Hichem Karoui

**Senior Affiliate Researcher
London Dialogue**

Iran did not need to defeat the United States and Israel in the conventional sense to alter the strategic balance. It needed only to prove that a weaker state could convert vulnerability into leverage, inflict costs faster than its enemies could impose order, and turn endurance into a form of power.

The Logic of Disproportion:

From battlefield weakness to strategic leverage

The central mistake in much Western analysis of war is to assume that material inferiority translates directly into strategic inferiority (Arreguín-Toft 2005). That assumption is rooted in an older model of conflict in which military strength was measured primarily through fleets, aircraft, armour, tonnage, and industrial depth. By those metrics Iran appeared overmatched from the outset. It could not command the air, could not protect all fixed infrastructure, and could not hope to prevail in a symmetrical exchange against the combined technological superiority of the United States and Israel. Yet asymmetry begins precisely where like-for-like comparison ends. A weaker state does not need to match an adversary's strengths if it can instead exploit the adversary's exposure, impatience, and political constraints.

Iran's strategy in 2026 was therefore not built around military victory in the classical operational sense. It was built around strategic disproportionality: the deliberate use of lower-cost tools to generate higher-order political, economic, and psychological effects. The point was not to destroy an American carrier group, annihilate Israeli air power, or hold captured territory. The point was to make every additional day of conflict more expensive for Washington and more destabilising for regional actors than for Tehran (Eisenstadt 2020). In that framework, survival itself became productive. Every strike absorbed, every network



reconstituted, and every disruption to energy flows signalled that the war was not ending on terms favourable to the stronger side.

Cost-imposition rather than platform competition

This is why the key concept here is cost-imposition. Cost-imposition is not simply the infliction of damage (Eisenstadt 2020). It is the shaping of an adversary's decision space by forcing it to spend more resources, assume more risk, tolerate more uncertainty, and justify more sacrifice than it expected. Iran pursued this through a system in which relatively cheap drones, missiles, cyber attacks, deniable proxies, and maritime pressure operated as mutually reinforcing instruments. None needed to be decisive on its own. Their power lay in their integration. Together they denied closure, complicated retaliation, and multiplied the number of fronts on which the stronger power had to defend itself.

In earlier eras, weaker states often sought attrition through insurgency over years or decades. Iran compressed that timeline. It used technologies that were sufficiently accurate to threaten high-value assets and sufficiently affordable to be used in quantity. This combination altered the relationship between cost and effect. Nadimi (2017) noted the Zolfaghar missile failures against ISIS in Syria as an example of missile unreliability. However, the 2026 war showed how a drone that cost tens of thousands could compel the launch of interceptor missiles costing millions. A cyber intrusion requiring modest infrastructure could disrupt port operations tied to billions in trade. A brief disruption in the Strait of Hormuz could send price signals across the global economy before major navies had even stabilised the tactical environment. The mismatch between input and output became the essence of the strategy.

The Architecture of the Iranian System

A networked model of war

Iran's wartime method is best understood not as a collection of separate capabilities but as a system of systems. Drones, missiles, coastal defences, cyber teams, naval units, intelligence organs, and proxy relationships were woven into a broader architecture that created persistent friction (Lindsay 2020). Such a model differs from conventional force planning, where the main objective is often to achieve superiority in a defined domain. Iran did not expect to dominate any single domain. Rather, it sought to make no domain secure enough for its



adversaries to operate freely and predictably. The objective was not mastery but contamination of the operational picture.

This architecture also reflected decades of adaptation under sanctions, isolation, and threat. Unable to rely on imported advanced platforms at scale, Iran invested in indigenisation, dispersal, redundancy, and modularity (Ostovar 2016). Components could be manufactured in distributed facilities, moved covertly, and assembled with flexibility. Command structures were designed not merely for centralised direction but for delegated continuity. Such arrangements matter greatly in a high-intensity confrontation. A state that assumes its command nodes will be struck first has powerful incentives to make replacement and recovery part of its initial design. In this sense, resilience was not an emergency response. It was embedded doctrine.

Absorbing the opening blow

The decapitation strike that opened the war tested whether that doctrine was real. A conventional understanding of coercion would predict disorientation, fragmented command, and loss of initiative after the removal of supreme leadership. Iran's response suggested something else: a political-military apparatus prepared in advance for severe leadership disruption. The continuity of retaliatory operations signalled that the strategic plan did not depend on uninterrupted top-down command. This is a crucial feature of mature asymmetry. The weaker actor assumes the stronger actor will target visible centres of gravity and therefore seeks to ensure that action can continue even when those centres are hit.

The result was a strategic surprise of a different sort. Washington and Jerusalem could destroy, but destruction did not produce submission. The expectation that shock would collapse coordination proved false, as Iran had organised around the probability of shock. This phenomenon is one reason why asymmetry is so often misunderstood by materially stronger states. They confuse the destruction of assets with the destruction of agency. But a decentralised, ideologically hardened, operationally networked state can lose significant assets while preserving its capacity to punish (Arreguín-Toft 2005). Once that fact becomes visible, the stronger state faces a new problem: every additional strike may demonstrate military superiority while doing little to alter the adversary's political will.



Drones and Missiles as Democratic Precision

Quantity, accuracy, and saturation

At the core of Iran's operational toolkit stood the pairing of mass-produced drones with increasingly precise missile forces. Their significance was not merely technical. They represented a shift in the economics of coercion. Precision had once been the preserve of the most advanced militaries, delivered through expensive aircraft, elite intelligence architectures, and highly sophisticated munitions. By 2026 that monopoly had eroded. Iran could now field layered strike packages in which drones served as decoys, sensors, distractions, and attack platforms, while ballistic and cruise missiles targeted critical military and economic nodes. These tactics produced a form of affordable complexity that strained even advanced air defences (Renad Mansour et al. 2025).

The strategic advantage of saturation lies less in guaranteed penetration than in forcing constant expenditure by the defender. Defending against one missile is difficult; defending against mixed salvos arriving from multiple vectors is costlier still. Even successful defence can become strategically disadvantageous if it requires lavish consumption of interceptors, round-the-clock operational tempo, and expanded force protection measures across a broad theatre. Iran understood that defence itself could be turned into a burden. By making attack cheap enough and frequent enough, it transformed sophisticated defensive systems from symbols of dominance into instruments of financial and operational depletion.

Psychological and political effects

These weapons also had effects that extended beyond physical damage. Precision or near-precision strikes against bases, ports, energy installations, and urban peripheries create a constant atmosphere of exposure. They force political leaders to answer difficult questions from publics and allies alike: if the strongest military coalition in the world cannot fully secure critical infrastructure, what exactly does superiority guarantee? The answer matters because strategic credibility depends not only on destruction inflicted but also on protection delivered. Iran's drone-and-missile campaign exploited that relationship. Each successful or partially successful strike undermined the image of impermeability that underpins alliance confidence.



article/01/September/2026/London-Dialogue.

This is the deeper meaning of the so-called second precision revolution. It is not merely that more actors possess accurate weapons. It is that these weapons allow weaker states to intervene directly in the calculus of escalation, economics, and alliance management. They can create distributed vulnerability faster than stronger powers can restore the appearance of control. When repeated over days and weeks, that vulnerability has cumulative consequences. Markets react, insurers reprice risk, shipping reroutes, commanders disperse assets, and governments begin to discuss off-ramps. A weaker actor that cannot seize the battlefield may still seize the tempo of political decision (Mack 1975).

Cyber Disruption and Information Friction

The invisible front

Cyber operations complemented physical attacks by widening the spectrum of uncertainty. Their value in asymmetric war lies in ambiguity, deniability, and scalability. A cyber operation may not destroy a refinery or sink a vessel, but it can delay cargo manifests, cloud maritime tracking, disrupt payment systems or interfere with logistics software (Rid 2020). In a closely coupled global economy, these frictions have a cascading effect. A delayed discharge at one port becomes a bottleneck elsewhere; a network outage in one terminal alters scheduling across shipping chains; uncertainty over data integrity can slow decisions even after systems are restored. The effect is to impose diffuse economic drag that exceeds the apparent narrowness of the intrusion.

Iran's use of cyber tools fits neatly within its broader strategic logic. Physical strikes created fear of interruption; cyber actions made interruption harder to diagnose and recover from. This combination matters because modern states and markets rely not only on physical infrastructure but also on informational trust. Tankers move because systems say they are insured, loaded, routed, and cleared. Energy trades settle because data systems remain legible. Military supply networks depend on software-enabled coordination at every stage. A weaker state that can inject uncertainty into those processes gains leverage that is disproportionate to its computing footprint. It need not dominate cyberspace to make dependence on it painful (Lindsay 2020).



Deniability as strategic lubricant

Another advantage of cyber disruption is that attribution rarely arrives at the speed of political demand. This lag is useful to a middle power under pressure. It complicates retaliation, divides allies over evidence thresholds, and creates room for calibrated escalation. In conventional war, kinetic attacks generate immediate visual narratives. Cyber effects are often murkier. Was a system overloaded, sabotaged, or merely malfunctioning under stress? Did a proxy actor act independently or under instruction? Such questions buy time, and time in asymmetric conflict is often the most valuable commodity. It allows the weaker actor to maintain pressure without always triggering automatic responses.

Information friction also mattered in public narratives (Lindsay 2020). Iran did not need to win a propaganda contest outright. It needed to reinforce a simple proposition: that its enemies could not compel outcomes quickly and cleanly. In that setting, every contradictory statement, every revised casualty estimate, and every unexplained disruption fed the perception of strategic slippage. Asymmetry operates partly through perception management. If a stronger state appears powerful yet ineffective, confidence in its deterrent promises erodes. Cyber operations, precisely because they are difficult to map in real time, help create that atmosphere of contested control.

Proxy Networks and the Geography of Reach

Expanding the theatre without formal expansion

Iran's proxy relationships have often been described lazily as instruments of plausible deniability alone. In reality they function more importantly as geographic extenders (Tabatabai 2020; Paglia and Tourret 2020). They allow Tehran to create pressure points far from its own borders, forcing adversaries to defend a far broader theatre than direct interstate war would otherwise require. Militias, aligned armed movements, and partner organisations do not need to act with perfect discipline or centralised command to be strategically useful. Their very existence obliges stronger powers to allocate surveillance, defensive systems, diplomatic attention, and contingency planning across multiple arenas at once (Al-Banna, Asmaa. 2025).

This distributed pressure undermines one of the key advantages of superior militaries: concentration. The United States and Israel can bring immense force to bear at chosen points,



article/01/September/2026/London-Dialogue.

but proxy-linked escalation creates many points at once. Bases in Iraq and Syria, shipping in the Red Sea and Gulf, diplomatic compounds, partner infrastructure, and regional energy nodes all become potential sites of coercion. The practical effect is to dilute the stronger actor's ability to convert technical superiority into political closure. The theatre becomes too wide, the categories of threat too varied, and the available responses too escalatory or too weak.

Control, looseness, and strategic utility

It is important, however, not to imagine proxy warfare as a puppet-master model. Iran's network is better understood as a spectrum of influence, support, shared interest, and operational coordination. Some actors are closely tied; others are merely aligned in moments of crisis. This looseness can appear to be a liability, but it often functions as a strength. It preserves deniability, reduces the vulnerability of the whole network to decapitation, and allows pressure to emerge from different directions without requiring explicit central orders visible to intelligence services. Such semi-autonomy is especially effective when the aim is not clean command but persistent harassment (Ostovar 2016).

For the stronger power, this approach poses an enduring dilemma. Striking back at every aligned actor risks horizontal escalation and diplomatic backlash. Ignoring them invites more attacks and further credibility loss. This is asymmetry in its purest political form. The weaker state uses layered relationships to generate a menu of dilemmas that have no tidy solution. Each choice by the superior military actor carries costs that can exceed the tactical significance of the immediate threat. The network thus becomes a machine for manufacturing difficult decisions, not merely a means of inflicting damage.

Maritime Coercion and the Economics of Hormuz

Turning geography into strategy

No element of Iran's asymmetric system better demonstrates the fusion of geography and technology than its maritime coercion in and around the Strait of Hormuz. The strait is not merely a map feature. It is a global economic valve through which energy security, insurance calculations, and naval strategy converge (Cordesman 2020). Iran cannot permanently close it against the full force of major navies, but permanent closure was never the necessary objective. Temporary disruption, credible threat, selective targeting, and induced uncertainty were



sufficient to raise prices, alter shipping behaviour, and globalise the war's consequences. In chokepoint politics, risk itself can be weaponised.

Such factors mattered because commercial systems react not only to realised damage but also to perceived hazard. Tanker operators, insurers, commodity traders, and governments do not wait for absolute certainty before adjusting their behaviour. They respond to probabilities, which can move violently under conditions of crisis. By combining anti-ship threats, small-boat harassment, mining risks, surveillance, drone reconnaissance, and missile coverage, Iran created a layered environment that made each transit more uncertain. A superpower navy may be able to escort, clear, retaliate, and patrol. It cannot instantly restore the market psychology of normality once fear has entered pricing.

Economic shock as strategic output

The brilliance, from Tehran's perspective, was that the principal audience for Hormuz coercion was not only the U.S. military. It was global markets and U.S. political leadership. If oil spikes, insurance surcharges rise, Asian importers panic, and allied governments begin urgent consultations, then the war ceases to be a bilateral or even regional affair. It becomes a systemic economic event. That dramatically increases the pressure on Washington to manage not only combat operations but also the wider consequences of prolonged instability. In effect, Iran expanded the list of stakeholders invested in rapid de-escalation, thereby increasing the diplomatic and political weight pushing against an open-ended campaign.

This is a model of coercion especially suited to middle powers located near strategic bottlenecks. It does not require naval dominance. It requires only sufficient capability to make commerce doubt the safety of passage. Once that threshold is crossed, even limited action can generate outsized effects. Here again the asymmetry is stark: modest tactical investments produce global macroeconomic consequences. Stronger states remain militarily superior, but they become hostages to the very interconnected systems from which they derive power. Iran's insight was that vulnerability in a globalised order is not distributed according to military rank alone.



Why the Stronger Side Struggled

The burden of escalation control

A paradox sits at the heart of modern asymmetric war: the stronger actor often has more military options but fewer politically usable ones (Arreguín-Toft 2005). The United States could escalate vertically, strike wider target sets, and devastate additional infrastructure. Yet each move carried risks of regional expansion, global economic disruption, allied anxiety, and domestic political backlash. Iran, by contrast, needed only to keep the conflict costly and unresolved. This asymmetry of objectives matters more than the asymmetry of arsenals. One side seeks decisive compliance; the other seeks durable non-compliance. The latter goal is frequently easier to achieve.

Moreover, superior firepower can produce diminishing returns when the adversary's key assets are dispersed, mobile, concealed, or already amortised. Destroying launchers matters, but if production lines are distributed and replenishment is cheap, tactical success does not guarantee strategic relief. Hitting command nodes matters, but if doctrine encourages local initiative and redundant communications, command disruption may be temporary. Bombing maritime assets matters, but if the economic effect depends mainly on fear and insurance premiums, restoring confidence may take longer than destroying the instruments that undermined it. In short, the stronger side could suppress symptoms faster than it could remove the underlying logic of the threat.

The exhaustion of political will

This is why asymmetry should be understood as a contest over political endurance (Mack 1975). Iran wagered that American tolerance for mounting costs, uncertain outcomes, and widening regional instability would prove lower than its own tolerance for damage and hardship. That wager was grounded not in romantic notions of resistance but in a cold reading of democratic accountability, alliance management, and media cycles. Democracies can sustain major wars, but they require persuasive narratives of progress. When military action is visible yet strategic results remain elusive, support becomes brittle. A weaker state does not need to win public opinion in the adversary's society. It needs only to thicken doubt.



article/01/September/2026/London-Dialogue.

The cumulative effect of Iran's integrated campaign was therefore to redefine what success meant. If the war could not be ended swiftly, if deterrence could not be re-established cheaply, and if every route to escalation threatened larger shocks, then the stronger side faced a choice between costly persistence and unsatisfying restraint. That is the strategic trap asymmetry seeks to build. It leaves the superior power visibly active but substantively constrained. The lesson is sobering. In the age of cheap precision, networked proxies, cyber friction, and chokepoint coercion, weaker states can punish stronger ones without ever matching them platform for platform. They need only understand where the stronger side is exposed, what it cannot tolerate, and how to turn survival into leverage.

Iran's achievement in 2026 was not that it overturned the hierarchy of military power. It was that it revealed the hierarchy to be less decisive than many had assumed. Asymmetric war, in this newer form, is the art of making superiority expensive, patience painful, and control perpetually incomplete.



References

- Renad Mansour, Hayder Al-Shakeri and Haid Haid (2025). The shape-shifting 'axis of resistance'. Middle East and North Africa Programme. Chatham House. DOI: 10.55317/9781784136369
- Arreguin-Toft, Ivan. 2005. *How the Weak Win Wars: A Theory of Asymmetric Conflict*. Cambridge: Cambridge University Press.
- Cordesman, Anthony H. 2020. *Iran and the Changing Military Balance in the Gulf – Net Assessment Indicators*. Washington, DC: Center for Strategic and International Studies (CSIS).
- Eisenstadt, Michael. 2020. "Operating in the Grey Zone: Countering Iran's Asymmetric Way of War." *The Washington Institute for Near East Policy*.
- Al-Banna, Asmaa. 2025. "Maḥwar al-muqāwama ḍidd Isrā'īl: al-kharīṭa, wa-l-imkānāt, wa-l-adwār" [The Axis of Resistance Against Israel: The Map, Capabilities, and Roles]. *Qadaya wa Nadharat*, no. 36 (January), Hadara Center for Studies and Research. <https://shorturl.at/TknFd>
- Lindsay, Jon R. 2020. *Information Technology and Military Power*. Ithaca, NY: Cornell University Press.
- Mack, Andrew. 1975. "Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict." *World Politics* 27 (2): 175–200.
- Nadimi, Farzin. 2017. "Iran Missile Strikes Reveal Potential Military Weaknesses." *PolicyWatch* 2823. Washington Institute for Near East Policy.
- Ostovar, Afshon. 2016. *Vanguard of the Imam: Religion, Politics, and Iran's Revolutionary Guards*. New York: Oxford University Press.
- Paglia, M., and V. Tourret. 2020. "L'Iran et ses « proxys » au Moyen-Orient. Les défis de la guerre par procuration." *Institut Français des Relations Internationales (IFRI)*.
- Rid, Thomas. 2020. *Active Measures: The Secret History of Disinformation and Political Warfare*. New York: Farrar, Straus and Giroux.
- Tabatabai, Ariane M. 2020. *No Conquest, No Defeat: Iran's National Security Strategy*. New York: Oxford University Press.