About the Author:

Beatrice Elizabeth Skurvydaite

About the publication:

3 Main Points:

To what extent did Operation Absolute Resolve demonstrate a scalable model for bypassing sophisticated A2/AD systems through multi-domain non-kinetic fires? The paper argues that tightly integrated cyber and electronic warfare can generate short-term access in permissive or weakly networked defences, yet such effects are highly conditional and context-dependent. Against resilient architectures like Iran's,

non-kinetic fires function best as force multipliers, not standalone solutions.

Highlight Sentence:

"Strategic Security Illusion: the Venezuelan case reflects systematic vulnerability rather than context-specific weaknesses in integration, maintenance, and operational doctrine."

Definition:

Electronic Warfare = military action that exploits electromagnetic (EM) energy—both actively and passively—to provide situational awareness and create offensive and defensive effects.

The Conditional Power of Non-Kinetic Warfare

Introduction

Modern warfare is increasingly defined less by the volume of fire exchanged and more by the ability to control information, its perception, and access across domains (Long, 2026). As sophisticated competitors invest heavily in Anti-Access/Area Denial (A2/AD) architectures, otherwise known as systems preventing military entry, Western militaries have sought to develop and test approaches aimed at preserving operational access while reducing reliance on prolonged kinetic attrition.

In early January 2026, U.S. forces executed Operation Absolute Resolve (OAR). The rapid, precision raid into Venezuelan territory culminated in the capture of President Nicolás Maduro without sustained kinetic suppression against the integrated air defences. Despite the presence of advanced systems of Russian origin, including S-300 variants and Buk-M2 systems, the Venezuelan air defences largely failed to detect, target, or engage more than 150 U.S. aircraft (Kajal, 2026; Baker, 2026). The interaction showed the dominance of electronic warfare (EW) and cyber effects. By the end, it was evident that Operation Absolute Resolve confirmed

a longstanding Western ambition: non-kinetic dominance rather than kinetic attrition (Centre for the Changing Character of War, 2026).

However, understanding what OAR demonstrated—and what it did not—is essential to avoid overconfidence in non-kinetic centrality, especially regarding more prepared and resilient A2/AD architectures. This tension generates a central research puzzle: while OAR is widely cited as evidence that cyber and electronic warfare can bypass modern A2/AD systems, it remains unclear whether the operation revealed a broadly transferable model or merely exposed unique adversary vulnerabilities. It is this grey area that leads to the central question of this paper: to what extent did Operation Absolute Resolve's integration of multi-domain non-kinetic fires demonstrate a scalable framework for bypassing sophisticated regional A2/AD environments, or does its success rely on adversary-specific conditions?

Operation Absolute Resolve: What Actually Happened?

It is evident that Operation Absolute Resolve illustrates an emerging evolution in contemporary Western military operations, yet its success still raises questions. The operation was conceived as a limited, high-tempo exercise, aimed at achieving rapid access and political objectives while avoiding escalation (Feickert, 2025; Baker, 2026). Central to the U.S. approach was the employment of a fifth-generation aircraft, particularly the F-35, in a broader operational design that employed these platforms as distributed electronic warfare and sensor nodes. Meanwhile, U.S Cyber Command reportedly conducted operations against Venezuelan command-and-control radar networks to degrade situational awareness before initial contact (Hadley, 2026; Johnson, 2026; Parrikar, 2026).

Building on this design, despite the presence of imported Russian-origin air defence systems such as the S-300VM and Buk-M2, known for upper-tier-level denial of airspace to advanced aircraft and missiles, the operation did not involve a prolonged kinetic suppression of enemy air defences. This marked a clear departure from traditional SEAD models (Panella, 2026; Cordesman, 2015) that emphasised the physical destruction of radar and missile systems. One of the most notable being

NATO's 1999 Kosovo operation, whose success was achieved through sustained kinetic pressure against a resilient air defence network. Instead, the operation in Venezuela reflected an evolution towards cyber and electronic warfare as access-enabling tools shaping the information environment, rather than acting as supporting effects (Hadley, 2026; Sandboxx, 2022). Operation Absolute Resolve is in stark contrast with the NATO operation, since it relied on short-duration non-kinetic power as a paralysing method for the defence system, exhausting it over time (Parrikar, 2026; Roudani, 2026). Therefore, it is evident that OAR did not demonstrate a hard replacement for kinetic power, but rather the increasing centrality of non-kinetic fires as force multipliers. During OAR, cyber and electronic warfare shaped the battlespace, thereafter, enabling kinetic forces to operate with greater precision (Baker, 2026). The operation's success was rooted in the integration of both methods, not simply from the sufficiency of non-kinetic means alone.

Venezuela's Shortcomings and the Security Illusion

Despite sudden actions, much of the operation's success also lies in the failure of the Venezuelan air defence. The country's shortcomings can be largely attributed to its weak A2/AD architecture, including fragmented command-and-control, limited sensor fusion, and poor interoperability between surveillance and missile systems (Roudani, 2026; Panella, 2026). These weaknesses are amplified by chronic training deficits and limited operational readiness, which constrained the ability of Venezuelan operators to employ complex systems effectively (Panella, 2026; Sandboxx, 2022). Furthermore, these shortcomings were compounded by long-standing maintenance and sustainment issues, exacerbated by sanctions and restricted access to spare parts, in turn degrading system reliability during the crisis (Sandboxx, 2022; Roudani, 2026). This lack of an integrated, resilient, and networked defence architecture left Venezuela particularly vulnerable to cyber disruption and electronic attack, targeting centralised nodes (Cordesman, 2015; Roudani, 2026). After understanding the dangers of extrapolated systemic vulnerability, attributing OAR's success to simple weaknesses in Russian-origin air defence technology risks generating misleading conclusions (Sandboxx, 2022; Pelayo et al., 2026; Cordesman, 2015).

The overall outcome in Venezuela has been interpreted as a demonstration that multi-domain non-kinetic fires offer a blueprint for bypassing other A2/AD environments (Baker, 2026). One of the paradoxical consequences of OAR is that it worked too well, thereafter encouraging over-optimistic interpretations that non-kinetic modes of warfare are independently decisive. However, such interpretations may risk mistaking enabling effects for substitute ones and open the door to a strategic security illusion: that the Venezuelan case reflects systematic vulnerability rather than context-specific weaknesses in integration, maintenance, and operational doctrine (Panella, 2026).

Scalability of OAR's Framework: The Case of Iran

It is important to establish that success in a permissive context does not promise success elsewhere. Applying a most-different system design logic allows for evaluation of scalability across four dimensions: A2/AD integration, command and control, doctrinal anticipation, and ability to sustain access. Venezuela represented a fragmented and weakly integrated A2/AD environment; meanwhile, Iran exemplifies a layered, redundant, and mature architecture. In this case, Iran poses a more sophisticated A2/AD environment for such comparative analysis (Gunzinger, 2011; Cordesman, 2020), serving as a hard test of whether the OAR environment can scale against other systems. Comparing the two dissimilar cases will allow for an assessment of whether the non-kinetic OAR model is more universally applicable.

Operation Absolute Resolve demonstrated how tightly integrated cyber and electronic warfare (EW) effects can create windows of operational access in a degraded or poorly networked A2/AD environment (Roudani, 2026; Panella, 2026). However, assessing the true strength and significance of Operation Absolute Resolve requires examining whether its underlying logic can scale against more resilient and integrated A2/AD architectures. Unlike Venezuela, Iran's A2/AD strategy is built around a multi-layered and geographically dispersed defence posture (Cordesman, 2020). The architecture combines a mix of medium and long-range strike systems, layered air defences, and asymmetric tools tailored to its geographic chokepoints, such as the Strait of Hormuz, a natural constraint that complicates

adversary access and magnifies defensive depth (Gunzinger, 2019; Cordesman, 2020).

Dimensions of the framework's scalability concern not merely the achievement of initial access, but the ability to sustain operational freedom over time. OAR demonstrated the capacity to generate short-lived windows of advantage through synchronised cyber and electronic effects (Hadley, 2026). However, access is more about a continuously contested condition. The operational challenge, therefore, becomes more about maintaining cumulative degradation across the phases of a campaign, especially against resilient adversaries. Unlike Venezuela, where imported systems were never fully integrated into a resilient, networked defence architecture, Tehran's network includes indigenously developed surface-to-air missile systems such as the Khordad-15, an Iranian-designed SAM capable of detecting and intercepting aerial threats at extended ranges (Army Recognition, 2025). Complementing this is the Bavar-373 long-range air defence system, also domestically produced and meant to rival legacy foreign systems such as the Russian S-300VM (Cordesman, 2020). The emphasis on domestic production not only solidifies resilient self-sufficiency but also shapes the systems' doctrinal integration, with mobility and reduced dependence on centralised nodes. This implies that transient cyber and electronic disruptions alone are unlikely to cause decisive damage, even if initial access were to be achieved (Noguerol, 2026; El-Komy, 2025).

In sharp contrast to Venezuela, Iranian doctrine further assumes that future conflict environments will include contestation in the cyber and electromagnetic domains. This means planners embed redundancy and decentralisation into their command-and-control agreements to sustain operations even when some nodes are disrupted (Boltuc, 2025). This design is in stark contrast with Venezuela, in which fragmented command links limited sensor fusion and contributed to operational degradation under EW pressure (Cordesman, 2015; Roudani, 2026). The limits of purely non-kinetic effects suddenly become clear in this context: while EW and cyber operations often rely on transient advantages tied to intelligence, timing, and exploitable vulnerabilities, as seen in Venezuela, Tehran's architecture aims to

mitigate single points of failure through dispersion, redundancy, and alternative pathways (Cordesman, 2020). Such a hardened architecture dealing with a temporary disruption of particular nodes is unlikely to collapse (Cordesman, 2020), showing a lack of OAR framework scalability to sophisticated A2/AD environments overall. Moreover, compared to Venezuela, cyber effects that depend on exploiting software, links, or logistic chains face a high bar in Iran, which has both practices operating with degraded connectivity and has invested in indigenous systems and 'air-gapped' modes of operation for critical nodes (Government of Canada, 2025). This means that even sophisticated electronic attack techniques can be blunted by passive sensing, emission-control doctrine, mobility, or even procedural workarounds such as pre-delegated decision authority (Boltuc, 2025). In practical terms, this shifts the operational problem from temporarily disrupting access to sustaining pressure across multiple layers of the defensive system, requiring a combination of non-kinetic and kinetic actions to impose cumulative effects rather than relying on single-domain disruption (Hall, 2025). Evidently, the approach demonstrated in Operation Absolute Resolve does not scale cleanly to a context like Iran's without substantial augmentation.

Against this backdrop, OAR's non-kinetic playbook, while useful as part of a comprehensive approach, is unlikely to serve as a standalone blueprint against deeply integrated A2/AD environments (Cordesman, 2020; Hall, 2025). Effectively challenging such similar postures would require persistent, multi-phased operations and sustained attrition to overwhelm layered defences and redundant command mechanisms (Hall, 2025). Of course, such an approach would then raise costs and escalation risks, compared to the rapid conditions that favoured OAR. Therefore, the model applied in Venezuela functions best as a force multiplier integrated into a broader joint campaign; however, it cannot be a universal blueprint for the logistical and organisational hard-kill measures necessary to defeat high-level, resistance-oriented A2/AD networks (Hall, 2025; Boltuc, 2025).

Conclusion

Operation Absolute Resolve demonstrated that tightly integrated cyber and electronic warfare used for access-enabling can create short-term windows of operational access without reliance on kinetic suppression; however, its success was demonstrated to be heavily conditional (Sandboxx, 2022; Pelayo et al., 2026; Cordesman, 2020). In this sense, OAR only offers a limited proof of concept for how multi-domain non-kinetic effects can complicate adversary decision-making (Panella, 2026). Furthermore, the operation's success was inseparable from Venezuela's inner structural weaknesses, which are not generally found within all other A2/AD environments, therefore showing that OAR's effects are not independently decisive or universally scalable (Sandboxx, 2022; Roudani, 2026). When further assessed against a more resilient adversary such as Iran, the limits of OAR's model become even more apparent. Iran's dispersed and redundant architecture, combined with its doctrinal anticipation of cyber and electromagnetic contestation, reduces the likelihood that transient non-kinetic disruption alone could generate relevant independent outcomes (Noguerol, 2026; El-Komy, 2025; Cordesman, 2020; Boltuc, 2025).

Consequently, Operation Absolute Resolve may not demonstrate a universally scalable blueprint for bypassing sophisticated A2/AD systems (Cordesman, 2020; Hall, 2025) and instead illustrate the conditional utility of non-kinetic fires as a force multiplier within a broader joint campaign. Ultimately, OAR underscores that future access operations will often hinge not on technical dominance, but on the integration of non-kinetic and kinetic effects, with sustained multi-domain pressure upon resilient adversaries.

References

Army Recognition. (2025). *15th Khordad-3 air defense system*. Army Recognition. https://www.armyrecognition.com/military-products/army/air-defense-systems/air-defense-vehicles/15th-khordad-15

Baker, S. (2026). *Venezuela's Russian air defenses didn't shoot down U.S. aircraft*. Business Insider. https://www.businessinsider.com/venezuelas-russian-air-defenses-didnt-shoot-down-us-aircraft-2026-1

Boltuc, S. (2025). *Iran missile deterrence strategy*. SpecialEurasia. https://www.specialeurasia.com/2025/04/12/iran-missile-deterrence-strategy/

Centre for the Changing Character of War. (2026). *Home*. University of Oxford. https://www.ccw.ox.ac.uk/

Feickert, A. (2025). Congressional Research Service. (2025). *IF11409*. U.S. Congress. https://www.congress.gov/crs-product/IF11409

Cordesman, A. H. (2015). *Iran air and sea missile threat*. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150219_Cordesman_IranAirSeaMissileThreat_Web.pdf

Cordesman, A. H. (2020). *Iran Gulf net assessment*: Third phase reduced. Center for Strategic and International Studies. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/200326_Iran_Gulf_Net_Assesment.Third_Phase.Reduced.GH6%281%29.pdf

El-Komy, F. (2025). *Sanctions, Iran, and manufacturing*. Habtoor Research. https://www.habtoorresearch.com/programmes/sanctions-iran-manufacturing/

Government of Canada, Cyber Security Agency. (2025). *National cyber threat assessment 2025–2026*. https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

Gunzinger, M. (2011). *Sustaining America's strategic advantage in the Middle East*. Center for Strategic and Budgetary Assessments. https://www.files.ethz.ch/isn/154637/CSBA_SWA_FNL-WEB.pdf

Gunzinger, M. (2019). *Strategic threat: Iranian hybrid warfare in the Gulf*. Center for Strategic and International Studies. https://www.csis.org/analysis/strategic-threat-iranian-hybrid-warfare-gulf

Hadley, G. (2026). *Venezuela: Nonkinetic effects at the forefront. Air & Space Forces Magazine*. https://www.airandspaceforces.com/venezuela-nonkinetic-effects-forefront/

Hall, S. (2025). *Synchronizing non-lethal and non-kinetic effects for operational control*. Small Wars Journal. https://smallwarsjournal.com/2025/11/07/synchronizing-non-lethal-and-non-kinetic-effects-for-operational-control/

Johnson, R. (2026). *The U.S. Navy's EA-18G Growler made Venezuela pay*. National Security Journal. https://nationalsecurityjournal.org/the-u-s-navys-ea-18g-growler-made-venezuela-pay/

Kajal, K. (2026). *U.S. Growlers blinded Venezuela's air defenses*. Interesting Engineering. https://interestingengineering.com/military/us-growlers-blinded-venezuelas-air-defenses

Long, J. (2026). *Beyond lethality: The primacy of influence in cognitive warfare*. Irregular Warfare Initiative.

https://irregularwarfare.org/sof-in-competition/beyond-lethality-the-primacy-of-influence-in-cognitive-warfare/

Noguerol, L. (2026). *Geopolitics, power, and cyber conflict*: *Venezuela and Iran as case studies in cyber-enabled statecraft*. MIA Strategic Intel. https://miastrategicintel.com/geopolitics-power-and-cyber-conflict-venezuela-and-iran-as-case-studies-in-cyber-enabled-statecraft/

Panella, C. (2026). *U.S. wins against Russian, Chinese air defenses: Risk of wrong lessons*. Business Insider. https://www.businessinsider.com/us-wins-against-russian-chinese-air-defenses-risk-wrong-lessons-2026-1

Parrikar, M. (2026). *Operation Absolute Resolve and the future of warfare: Military lessons for India*. Eurasia Review. https://www.eurasiareview.com/14012026-operation-absolute-resolve-and-the-future-of-warfare-military-lessons-for-india-analysis/

Pelayo, J., Fortenrose, K., Sennett, E. (2026). *The Venezuela–Iran connection and what Maduro's capture means for Tehran, explained*. Atlantic Council. https://www.atlanticcouncil.org/blogs/menasource/the-venezuela-iran-connection-and-what-maduros-capture-means-for-tehran-explained/

Roudani, C. (2026). *Why Venezuela's air defenses never fired*. Geopolitical Monitor. https://www.geopoliticalmonitor.com/why-venezuelas-air-defenses-never-fired/

Sandboxx. (2022). *The S-400 myth: Why Russia's air defense prowess is exaggerated*. Sandboxx. https://www.sandboxx.us/news/the-s-400-myth-why-russias-air-defense-prowess-is-exaggerated/