MANOHAR PARRIKAR
idsa
MANOHAR PARRIKAR INSTITUTE FOR DEFENCE STUDIES AND ANALYSES
मनोहर पर्रिकर रक्षा अध्ययन एवं विश्लेषण संस्थान

MP-IDSA
Issue Brief

Operation Absolute Resolve and the Future of Warfare: Military Lessons for India

A B Shivane

January 13, 2026

Summary

Operation Absolute Resolve underscores the urgency for India to accelerate theaterisation, build a genuinely integrated C5ISR architecture and kill chain, achieve cyber and electromagnetic spectrum dominance, raise the Special Operations Command, develop cognitive warfare capabilities, strengthen civil–military fusion, and elevate multi-domain warfare integration to a new level. The caution remains that these lessons, as relevant, can be applied while staying anchored in India's own strategic culture, threat perception and operational environment.

Introduction

The events of 3 January 2026 in Venezuela will eventually be studied by professional military institutions worldwide. For India, they demand attention not as distant drama but as a live demonstration of how powerful states conduct decisive military operations. The United States carried out a short, violent, electronically-dominated suppression campaign and a precision Special Forces decapitation strike, capturing President Nicolás Maduro inside the capital city before Venezuela's defence network could meaningfully respond. A layered air defence system built around Russian, Chinese and Iranian platforms collapsed within less than an hour when confronted with a well-prepared, modern power projection.[1]

For Indian defence planners, this operation reveals what modern seizure of initiative looks like, how technologies shape tempo, why intelligence now outweighs brute firepower, and how doctrine transforms hardware into usable capability. More importantly, it reveals vulnerabilities of systems that many nations consider protective shields and the strategic language of electronic warfare, cyber disruption and integrated suppression of enemy air defences.[2]

Years of Preparation behind Minutes of Action

Absolute Resolve was not improvised. It was engineered over the years. Power grids had already been infiltrated. Communication networks were already mapped. Surveillance systems were quietly compromised. Dormant malware likely sat silently for months or years. When the operation began, cyber warriors did not 'attack'. They activated what was already there. The blackout was not accidental. It was a targeted Supervisory Control and Data Acquisition (SCADA) attack, reportedly aimed at Venezuela's Guri Dam network, designed not only to shut off power but also to create systemic shock and communications collapse.

When power failed, air defence networks shifted to backup systems, creating time-lag blind spots, precisely when US helicopters crossed the coastline. Cyber warfare did not blind radars. It lied to them. Advanced 'Suter-type' intrusions rendered radar and air defence networks unreliable, showing operators clear skies while over 150 aircraft entered protected airspace.[3] Command and control were cleanly severed. Key telecommunications nodes were reportedly targeted with denial-of-service attacks,

[1] Josh Luberisse, **"Operation Absolute Resolve: Anatomy of a Modern Decapitation Strike"**, *RealClearDefense*, 5 January 2026.

[2] Rendy Andriyanto, **"Inside the Capture of Venezuela's President - Operation Absolute Resolve"**, *Gotrade News*, 5 January 2026.

[3] Josh Luberisse, **"Operation Absolute Resolve: Anatomy of a Modern Decapitation Strike"**, no. 1.

leaving military leaders unable to issue firing orders. In a political system where initiative is punished, the absence of orders ensured paralysis.

Even the surveillance infrastructure was turned against its own master. Modern state surveillance, often powered by foreign technology ecosystems, has become a vulnerability. Reports indicate compromise of the Venezuelan smart surveillance backbone, allowing adversaries to literally 'see' through the state's own cameras. Thus, the real battle did not begin on 3 January. It started years earlier, when systems were infiltrated, networks compromised, and trust was silently destroyed. By the time boots moved, the nation was already neurologically disconnected.

Conduct of Operations: Precision, Ruthlessness and Total Synchronisation

This operation stands out not only for what happened, but also for the complete absence of a response. There were no missiles fired, no Air Defence engagements, no organised resistance. These were not by luck but by design—denial, domination, deception and deceit. Some of the features which stood out are highlighted below.

Intelligence Depth as the Foundation

All eight dimensions of intelligence—Open Source (OSINT), Human (HUMINT), Signals (SIGINT), Measurement and Signature (MASINT), Technical (TECHINT), Geospatial (GEOINT), Imagery (IMINT), and Cognitive (COGINT)—were fused not over weeks but months and years. This resulted in both physical and psychological paralysis of the adversary and ensured victory at the lowest cost and in the shortest time through a surgical, intelligence-driven operation.

Political Clarity and Command Certainty

There was no dilution of purpose. No confused objectives. No excessive consultation cycles. The chain from political decision to operational execution was crisp, short and empowered. This clarity of will translated into military impulse and tempo.

Jointness at Its Purest

This was actual joint warfare. Cyber warriors, airmen, space analysts, naval platforms, intelligence agencies and Special Forces operated not as separate services but as a single, fused organism. Carrier groups, regional bases, strategic bombers, fifth-generation fighters, tankers, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance (C5ISR) platforms, and rotary-wing aviation were integrated into a single theatre design.

Mastery over Surprise

Surprise today is not created by secrecy alone. The denial of enemy cognition makes it. Venezuela did not fail to respond; it was simply slow. It failed because it was simultaneously blinded, muted, deceived and isolated.

Tempo Dominance

Once initiated, the operation unfolded like a choreographed sequence. Strikes shaped the battlespace. Cyber kept the enemy comatose. Special Forces moved decisively. Extraction was seamless. Exposure time was minimal. Shock was permanent.[4] For the military mind, this was not aggression alone. It was military science executed with maturity and absolute confidence.

Multi-Domain Warfare

Operation Absolute Resolve is perhaps the most explicit demonstration of actual multi-domain warfare in action. The battlefield was not land, sea or air. It was everywhere simultaneously.

Cyber as the First Strike Arm

Cyber warfare did three things exceptionally: it turned off the city, causing blackouts, fear and disorder; it lied to radars, creating a false picture of safety; and it cut command chains, isolating leadership and freezing response. This was not a disruption. This was strategic paralysis. Venezuela's air defence systems were physically intact, stocked and operational—yet they were in a coma. That is the power of cyber-enabled warfare.

Domination of the Electromagnetic Spectrum

Electronic warfare complemented cyber domination. The electromagnetic spectrum became a weapon; blinding, deceiving, masking, securing and protecting simultaneously. The enemy was deaf, blind and directionless. Total paralysis achieved.

Air and Space Supremacy

More than 150 aircraft,[5] ranging from stealth fighters to electronic warfare (EW) platforms, operated through "defended" skies with zero loss. This was only possible because the sky had already been conquered digitally. Airpower did not fight through air defence. It flew through nothingness.

[4] Ibid.

[5] Ibid.

Special Operations Precision as the Visible Outcome

Delta Force was merely the visible blade of a sword powered by invisible machinery. Their speed and confidence were products of cyber dominance, C5ISR superiority, training, intelligence-based operations, joint operations, multiple rehearsals and contingencies, and political backing.

Information Warfare as a Battlefield Weapon

When information warfare targets the cognitive domain, the adversary realises its own systems cannot be trusted, and fear replaces confidence. This fear is a weapon, and it was used decisively.

Lessons for India

The heart of Operation Absolute Resolve was intelligence. American agencies reportedly built a continuous presence inside Venezuela months in advance. Human sources mapped routines, vulnerabilities and psychological habits. Persistent airborne surveillance platforms, supported by maritime assets and forward-positioned operational hubs, complemented the human layer with imagery, signals intelligence and pattern recognition.[6] This created what every modern military seeks, but few achieve: continuous awareness, precision certainty and the confidence to act at will.

For India, this reinforces a truth our own operations have consistently highlighted. Whether it was Balakot, surgical strikes across the Line of Control, or Operation Sindoor, success grows from patient intelligence architecture. However, Operation Absolute Resolve pushes this requirement to a significantly higher level. It illustrates the fusion of human intelligence with persistent high-altitude, stealth-based intelligence, surveillance and reconnaissance, and maritime-enabled command networks. India must therefore prioritise a sustained forward intelligence presence across all eight dimensions, long-endurance, stealth, surveillance, deeper integration between civilian and military intelligence, and a dedicated national-level pattern-of-life analytics.

In future crises involving high-value targets, adversary command centres or critical military infrastructure, intelligence preparation may last months or years, but the final execution window may shrink to minutes. The one-to-many ratio between preparation time and kinetic execution demonstrated in Venezuela represents the operational standard of future power actions.[7]

[6] Ibid.

[7] Ibid.

Electronic Warfare as the First Weapon

Perhaps the most striking element of the Venezuelan episode was the quiet violence that preceded the kinetic strikes. As American aircraft and special operations helicopters moved, Venezuela's air defence systems went blind, deaf and confused. Radars built to detect stealth aircraft, imported with the promise of survivability, were electronically paralysed. Command networks lost connectivity. Grid-linked systems were rendered powerless as cyber operations reportedly disrupted electricity distribution. Systems that appear powerful in static photographs are reduced to expensive pieces of silent metal.

For India, it has three lessons.

- First, air defence systems alone do not secure skies. Without hardened, resilient, redundant and intelligent networks, even sophisticated surface-to-air missiles become irrelevant.
- Second, electronic warfare is not an accessory. It is not a supplemental arm. It is now as central as air power or ground manoeuvre.
- Third, India must assume that in any future conflict involving technologically advanced adversaries, our own systems will face intense jamming, spoofing, cyber disruption, deceptive electromagnetic signatures and potentially coordinated power infrastructure manipulation.[8]

India has made significant strides in electronic warfare through DRDO programmes, dedicated electronic-warfare suites on aircraft, and specialised ground platforms. But the lesson here is scale and integration. Electronic warfare must move beyond platform-specific equipment to become a national combat discipline. It requires doctrine, trained cadres, permanent peacetime rehearsal cycles, civilian power grid resilience, and assured, satellite-independent communications. The Venezuelan case demonstrates that once your sensors are blinded, your decision cycle collapses. When the decision cycle collapses, everything else follows.[9] Above all, it highlights the importance of an indigenous defence ecosystem.

Suppression of Enemy Air Defence as a System, Not a Strike

While headlines may focus on Special Forces capturing Maduro, militarily, the decisive achievement was the suppression of enemy air defences. Venezuela's defence environment consisted of layered Russian surface-to-air missile systems such as S-300VM and Buk M2E, Chinese radar complexes such as JY-27A and JYL-1, Iranian-

[8] Ibid.

[9] Lt Gen A.B. Shivane (Retd), **"Venezuela and the Return of Power Politics"**, *Cross Section Conversations*, 4 January 2026.

supplied drones and scramblers, and multiple lower-tier platforms.[10] In concept, such a layered shield creates deterrence. In practice, when confronted by coordinated electronic and kinetic suppression, the shield crumbled.

American forces reportedly combined EA-18 G Growler electronic warfare aircraft, cyber operations, stealth platforms and anti-radiation missiles to systematically dislocate radar, paralyse communications, and then destroy emitters once they were activated. The outcome reveals something important for India. The age of static confidence in imported air defence systems is over. Survivability no longer depends solely on hardware. Survivability derives from mobility, deception, independent power supply resilience, diversified command links, disciplined emission control, and the ability to fight within an electronic storm.

For India, which operates layered air defences including modern long-range missile systems, the message is not alarmist. Instead, it is a call for realism. Systems must be continually trained to fight under conditions of total electromagnetic hostility. Dummy emitters, mobile deception networks, hardened underground command sites, and rapid dispersal doctrines are essential. India should also accelerate investment in its own Suppression of Enemy Air Defence capability. Future conflicts in our region will almost certainly demand the neutralisation of hostile missile shields. That requires indigenous anti-radiation weapons, offensive electronic-warfare aircraft, cyber integration with kinetic strikes, and doctrinal clarity on how to dismantle layered defences under time pressure.

Tempo, Integration and the Compression of Decision Time

One of the most remarkable aspects of the operation was tempo. More than 150 aircraft reportedly operated from multiple locations. Electronic warfare, cyber action, Special Forces insertion, air defence suppression and command targeting unfolded almost simultaneously. Within roughly half an hour of initial suppression, the ground capture was effectively secured. Within hours, the extraction was complete. For the defending state, this meant that detection, decision, coordination and response all had to occur inside an almost impossibly compressed timeframe. Their systems were not merely outmatched technologically; they were outpaced both cognitively and by the kill web.

For India, this highlights the importance of decision architecture. In any major crisis or limited war contingency, our political and military leadership must expect extremely compressed timelines. This requires pre-authorised frameworks, rehearsed joint-force responses, rapid political-military decision synchronisation, and a mission-command culture within services. India lacks a strategic war-gaming

[10] Josh Luberisse, **"Operation Absolute Resolve: Anatomy of a Modern Decapitation Strike"**, no. 1.

and scenario-building model in the absence of a National Security Strategy. India has made significant improvements in jointness, particularly with theatre command debates and integrated planning. However, Absolute Resolve shows that even the best equipment fails if the state cannot think, decide and act at the required speed. Further, it highlights India's strategic weakness: the absence of a national strategic security construct.

India must cultivate an institutional culture that prepares commanders to operate in degraded communications, partial-information environments, and high-speed operational contexts. War gaming, Red Team practice, and decision cycle training for political leadership are as crucial as missiles and aircraft. To create a whole-of-government approach, the national security strategy must be expedited. The United States succeeded not only because its machines worked, but because its organisations understood tempo as a weapon.[11]

The Meaning of Special Forces in Modern Strategy

Special Forces aviation and assault teams executed the final physical phase of the Venezuelan operation. This reinforces another vital lesson. Special Forces today are not isolated raiders. They are the sharpest end of an enormous intelligence, cyber, electronic and airpower ecosystem. Their success depends on the nation's ability to integrate all tools of modern military power into a concentrated, time-bound, high-precision strike.

India possesses competent Special Forces. What they require is precisely what the United States demonstrated. Long-range air mobility is protected by credible electronic warfare cover. National capacity to destroy or neutralise hostile air defence networks rapidly. Real-time intelligence fusion. Maritime support platforms that can sustain operations beyond immediate borders—deep doctrinal confidence among political leadership to employ them when required.[12]

Relevance to India's Strategic Environment

India lives in a far more contested strategic geography than Venezuela. Across our continental borders lie two adversaries with sophisticated air defence networks, advanced cyber capabilities, electronic warfare capabilities and strong surveillance architectures. At sea, India faces an expanding Chinese maritime footprint, supported by strategic access to Indian Ocean logistics. Internally and regionally, high-value targets and challenges posed by irregular warfare will persist.

[11] Rendy Andriyanto, **"Inside the Capture of Venezuela's President - Operation Absolute Resolve"**, no. 2.

[12] Josh Luberisse, **"Operation Absolute Resolve: Anatomy of a Modern Decapitation Strike"**, no. 1.

Therefore, the Venezuelan episode speaks to India across three broad levels.

First, deterrence is no longer simply about visible weapons. Deterrence now rests on whether a nation can protect its nervous system. Power grids, military communication networks, satellite resilience, electromagnetic spectrum dominance and robust ISR decide survival.[13] Thus, deterrence is all about denial and domination.

Second, India must internalise that future decisive actions will rely on rapid, integrated operations rather than sequential ones. Intelligence, cyber shaping, electronic paralysis, information warfare and kinetic strike will occur as a single orchestrated event. This demands joint theatre thinking.[14]

Third, India should draw both confidence and caution. Confidence, because many elements demonstrated by the United States are already under serious development within the Indian system. Caution: complacency about imported air defence systems or traditional security concepts will prove costly.[15]

Table 1. Strategic, Operational and Tactical Recommendations

Dimension	What Absolute Resolve showed	What India should emulate	What India should avoid
Strategic	Willingness to use decisive force for a single, clear objective.	Rapid politico-military decision loops and clear strategic objectives for limited, high-end operations.	Normalising extra-regional regime change raids that undermine India's credibility in the Global South.
Operational	150 aircraft, cyber-enabled SEAD, multi-base launch in a tight window.	Theatre-level joint planning, extensive-package training, and integrated cyber-space-electronic warfare-air campaigns.	Over-reliance on global basing and unique US-style enablers that India cannot replicate worldwide.

[13] Lt Gen A.B. Shivane (Retd), **"The Venezuela Precedent: Why Unilateral US Intervention Signals a Harsher Global Order for New Delhi"**, *ET Government*, 5 January 2026.

[14] Josh Luberisse, **"Operation Absolute Resolve: Anatomy of a Modern Decapitation Strike"**, no. 1.

[15] Ivaylo Valchev, **"Lessons from the Venezuela Takeover: When Laws Are Irrelevant Without Enforcing Mechanism"**, *The Strategic Perspective*, 6 January 2026.

Dimension	What Absolute Resolve showed	What India should emulate	What India should avoid
Tactical	Full-scale mock-ups, SOF–aviation–C5ISR fusion, 10-minute capture.	Realistic rehearsal facilities, Special Forces Command, precision breaching and extraction capability.	Treating such raids as routine tools instead of rare, high-risk options.

Used as a mirror, Operation Absolute Resolve pushes India to accelerate Theatreisation, build a genuinely integrated C5ISR architecture, and elevate SF Command and air power integration to a new level, while remaining anchored in India's strategic culture and neighbourhood-centric objectives.

Conclusion

Operation Absolute Resolve demonstrated what a mature 21st-century military ecosystem looks like when activated. It showed that air defence networks built on reputed systems can collapse quickly if they are not supported by resilient power, robust networks and disciplined doctrine. It revealed that future wars will begin in the electromagnetic spectrum long before missiles fly. It has been shown that intelligence preparation now exceeds all other priorities. It confirmed that tempo, integration and cognitive speed convert capability into decisive effect.

For India, the most profound lesson is that the battlefield now begins in cables, satellites, power grids, fibre optics, routers, servers and minds. Army formations, fighter aircraft and naval fleets will always matter. Still, they will operate only if the nation's digital nervous system survives and all assets in the multi-domain battlespace are networked. India needs to invest deeply in electronic warfare as a central combat capability. Strengthen cyber and grid resilience. Build long-endurance, stealth ISR and maritime-enabled intelligence support. Prepare theatre-level suppression of enemy air defences. Institutionalise a rapid decision culture. A dispassionate SWOT analysis of future warfare capabilities is required, with a time-sensitive action plan to ensure readiness. Future wars will not be defined by what is in the inventory; they will be determined by how one denies and dominates in a cyber- and electronic-warfare-saturated multi-domain operational environment.

About the Author

Lt. Gen. A.B. Shivane, PVSM, AVSM, VSM (Retd.) is a former Strike Corps Commander and Director General of Mechanised Forces.

Manohar Parrikar Institute for Defence Studies and Analyses is a non-partisan, autonomous body dedicated to objective research and policy relevant studies on all aspects of defence and security. Its mission is to promote national and international security through the generation and dissemination of knowledge on defence and security-related issues.

Manohar Parrikar Institute for Defence Studies and Analyses
1, Development Enclave, Rao Tula Ram Marg
New Delhi 110 010 India
T +91-11-2671 7983 F +91-11-2615 4191
www.idsa.in
Twitter @IDSAIndia
www.facebook.com/ManoharParrikarInstituteforDefenceStudiesAnalyses