

Integrated Cyber–Kinetic–Information Warfare

Insights from the Venezuela Crisis of 2026

Jitendra Nandan Bhatt and Abhishek Lal***

The Venezuela crisis of January 2026 provides a contemporary case for examining the conduct of hybrid warfare in which cyberspace operations, kinetic actions and information-domain effects were integrated to shape the operational environment. Publicly reported indicators, including radar degradation, communications disruption, localised power outages and concurrent kinetic activity, suggest the coordinated use of non-kinetic effects to create favourable conditions for military action. Assessed through the lens of modern cyber and joint operations doctrine, the case reflects a sequenced campaign in which cyberspace exploitation and selective disruption were used to degrade situational awareness, delay command response and compress adversary decision-making during a critical operational window. The role of Telegram further demonstrates how civilian digital platforms can become instruments of command, control, influence and public perception during crises. Leadership disruption and narrative fragmentation created information uncertainty, affecting both regime coherence and public confidence. For India, the case underscores the need to treat cyberspace and the information domain as permanently contested battlespaces, fully

* Brigadier Jitendra Nandan Bhatt, SM, VSM is the Commander of the Army Cyber Group, the apex cyber organisation of the Indian Army.

** Lt Col Abhishek Lal is a serving officer of the Indian Army, presently serving with the Army Cyber Group.

integrated into operational planning, deterrence, resilience and national security preparedness.

Keywords: *Cyberspace Exploitation (CE); Cyberspace Attack (CA); Cyber–Kinetic Integration; Digital Battlespace Shaping; Operational Environment Shaping; Cyber-Enabled Influence Operations*

INTRODUCTION

Contemporary warfare increasingly reflects the integration of cyberspace as a decisive enabling domain rather than a discrete or episodic arena of conflict.¹ Modern military campaigns routinely employ cyber capabilities to shape the operational environment, compress adversary decision cycles, and create conditions favourable for kinetic action while maintaining limited visibility and escalation control.² This convergence lies at the core of contemporary hybrid warfare, where military power is applied not only through conventional force, but also through cyber operations, electromagnetic effects, information activities, political signalling, and the calibrated disruption of state coherence.³ Within this construct, cyberspace exploitation (CE), cyberspace attack (CA), kinetic operations and information activities are sequenced and synchronised as elements of a coherent multi-domain operational design.⁴ The events surrounding Venezuela in early January 2026 provide a relevant case through which this model of integrated warfare can be examined.⁵ Public reporting and official statements indicate that non-kinetic effects occurred in close temporal alignment with air and rotary-wing activity during a time-sensitive operation.⁶ Observable indicators included disruption of radar coverage, limited activation of air-defence systems, degradation of communications, and widespread power outages during critical operational windows. While open-source reporting does not permit definitive technical attribution, the timing and coordination of these effects are consistent with the application of preparatory intelligence activity and carefully calibrated non-kinetic measures intended to shape the operational environment prior to and during kinetic action.⁷ Taken together, these indicators appear consistent with intelligence preparation of the operational environment encompassing critical infrastructure, surveillance and air-defence networks, command-and-control systems, telecommunications nodes, power distribution networks and key digital dependencies.⁸ In a digitally dependent state, these systems do not operate in isolation. Power distribution supports communications; communications support command continuity; command continuity supports air-defence response; and official communication channels shape

both military coordination and public confidence.⁹ Disruption of selected parts of this networked fabric for a limited period can therefore produce operational effects greater than the immediate technical disruption. It can degrade situational awareness, slow command response, fragment decision-making, and reduce the adversary's ability to generate organised resistance. At the strategic level, the Venezuela episode reflects defining characteristics of contemporary cyber-enabled warfare. Cyber operations increasingly appear designed to be precise, reversible and escalation-aware, generating operational advantage while preserving political and strategic flexibility.¹⁰ Their value lies not only in the damage they may cause, but in the conditions they create. A short-duration disruption of radar confidence, communications reliability, or command visibility may be sufficient to create a temporary window of advantage for kinetic action. In this sense, cyberspace does not replace conventional force. It prepares, protects, enables, and amplifies it. The sequencing of preparatory access, selective disruption and kinetic execution reflects a mature integration of cyberspace into joint operational planning rather than ad hoc or isolated cyber activity. This marks a movement from platform-centric warfare, where operational effectiveness is measured primarily through the employment of aircraft, ships, missiles, armoured formations, or other military platforms, towards condition-centric warfare, where the decisive objective is to shape the adversary's ability to perceive, decide, communicate and respond.¹¹ The central contest is increasingly over time, coherence and decision advantage. A force that can delay the adversary's understanding of events, even briefly, may gain disproportionate freedom of manoeuvre during the decisive phase. Concurrent contestation of the information domain further underscores this convergence.¹² The use, control and disruption of digital communication platforms during high-tempo operations highlight the linkage between cyber activity, command continuity, perception management and public confidence. Cyber effects in this context function not as stand-alone technical actions but as instruments that shape situational awareness, suppress adversary response, influence public perception, and enable freedom of manoeuvre across domains. The Venezuela case also demonstrates that information-domain effects may arise not only from deliberate propaganda or psychological messaging, but also from structural disruption. When leadership communications, digital platforms and official messaging channels are degraded or fragmented, the result may be narrative uncertainty, public confusion, and loss of confidence in state authority. Telegram, in this context, functioned not merely as a civilian messaging application, but as a regime communication platform, an influence

channel, and a contested information space.¹³ Leadership disruption and narrative fragmentation generated instability during critical phases of the operation, demonstrating how civilian digital platforms can acquire operational significance during crises by serving simultaneously as channels of command, mobilisation, surveillance, propaganda and public perception management. This article examines the Venezuela campaign as a case study in the operationalisation of cyberspace within a broader military framework. It situates CE and CA within an integrated operational environment, emphasising their role in shaping battlefield conditions, enabling manoeuvre, disrupting adversary coherence, and influencing the information domain rather than treating cyber activity as an isolated category of warfare. The argument is not that cyber operations independently determine military outcomes, but that their proper integration into joint operational design can create decisive windows of advantage by degrading the adversary's ability to sense, decide, command and communicate. For India, the case carries important implications. Regional adversaries increasingly employ cyber and information activities below conventional thresholds to influence decision-making, degrade readiness, disrupt public confidence, and constrain operational freedom. Future crises may not begin with artillery fire, air strikes, or overt mobilisation alone. They may be preceded by persistent cyber reconnaissance, infrastructure mapping, information probing, narrative shaping, and selective disruption of digital systems. Understanding how advanced militaries integrate cyberspace into joint campaigns, particularly through intelligence preparation and selective denial of sensing, communications and defensive systems, is essential for the development of resilient doctrine, credible deterrence and effective countermeasures in an increasingly contested digital battlespace.¹⁴ This analysis adopts a qualitative, effects-based approach grounded exclusively in open-source information, including publicly available reporting, official statements, policy documents and secondary analytical literature. The assessment emphasises temporal correlation, sequencing of effects and cross-domain convergence rather than technical attribution of specific cyber or electromagnetic mechanisms. Reported disruptions are treated as observable operational effects evaluated for their alignment, timing and cumulative impact on situational awareness, command continuity, decision-making and public perception. Open-source constraints preclude definitive attribution, and alternative explanations cannot be fully excluded. Accordingly, the Venezuela case is treated as illustrative rather than prescriptive, with implications framed at the doctrinal, operational and resilience levels¹⁵.

CYBER OPERATIONS MODEL IN THE VENEZUELA CAMPAIGN (CE → CA → KINETIC)

The Venezuela operation of 3 January 2026 offers a contemporary case through which the employment of cyberspace operations can be examined as an operational enabler within multi-domain warfare when assessed against publicly articulated United States Cyber Command (USCYBERCOM) doctrine and operational concepts.¹⁶ The campaign reflects the sequenced employment of CE and CA in support of kinetic objectives, wherein cyber effects appear to have functioned not as autonomous instruments of conflict, but as force multipliers shaping the conditions under which military action unfolded.¹⁷

Viewed through a military-operational lens, the significance of the Venezuela case lies not merely in the occurrence of cyber-related disruption, but in the apparent orchestration of effects across multiple domains. Contemporary operations increasingly seek advantage before overt contact by shaping the battlespace in advance of kinetic execution.¹⁸ In such campaigns, cyberspace functions as a preparatory layer through which access is established, dependencies are identified, vulnerabilities are assessed, and options for calibrated disruption are developed. The decisive value of cyber power therefore lies not only in technical penetration or disruption, but in its capacity to alter the conditions under which an adversary perceives, decides, coordinates and responds. The operational logic reflected in the Venezuela episode appears broadly consistent with the philosophy associated with USCYBERCOM, wherein cyberspace operations are integrated, mission-focused and synchronised with wider military objectives in support of time-sensitive and high-value actions while maintaining escalation control. Within this framework, cyber activity contributes to the shaping of operational conditions, compresses adversary reaction timelines, weakens command continuity and reduces confidence in sensing and communications systems during decisive moments. Such effects become particularly consequential when synchronised with kinetic manoeuvre and selective electromagnetic activity, enabling military objectives to be pursued under conditions of reduced adversary responsiveness.

The broader significance of this model lies in its departure from warfare centred principally on physical destruction. Increasingly, operational success derives not only from the destruction of enemy capability, but from the disruption of enemy coherence. A force unable to sense accurately, communicate reliably, coordinate effectively, or issue timely orders may

suffer operational paralysis despite retaining considerable physical assets. Temporary degradation of radar confidence, communications reliability, power stability, or command visibility during critical operational windows may therefore produce effects disproportionate to the scale of disruption itself.¹⁹ In contemporary conflict, limited and reversible disruption may be sufficient to secure disproportionate military advantage if applied at the decisive moment. In this sense, cyber power does not replace conventional force; it prepares, protects and amplifies it.²⁰ When synchronised with kinetic manoeuvre, information-domain activity and electromagnetic effects, cyber capabilities become instruments of operational art rather than stand-alone technical actions. Their value lies in creating temporary asymmetry, compressing adversary reaction timelines, fragmenting coordination, and securing freedom of manoeuvre during the decisive phase while avoiding uncontrolled escalation. The Venezuela operation is therefore best understood, not as an isolated cyber episode, nor as a purely kinetic action accompanied by incidental technical disruption, rather, it reflects an integrated campaign model in which cyberspace prepared the battlespace, selective disruption conditioned the operational environment, kinetic force exploited the resulting window of advantage and information effects shaped both command continuity and public perception. The sections that follow examine this sequence through the interconnected phases of operational preparation, selective disruption, kinetic execution and information-domain effects. While a single case study cannot establish doctrinal universality, the Venezuela episode provides a contemporary illustration of operational patterns increasingly visible in cyber-enabled conflict.

Integrated Sequencing and Operational Logic (CE → CA/EMS → Kinetic → Information Effects)

Modern high-tempo operations increasingly seek decision advantage before overt contact by synchronising non-kinetic and kinetic instruments into a unified effects chain.²¹ The operational design typically follows a deliberate sequence in which CE secures persistent access and intelligence dominance, CA, synchronised with electromagnetic spectrum manoeuvre (EMS or EW), imposes time-bound denial across sensing and communications, and precision kinetic action culminates inside a carefully engineered window of adversary disorientation.²² The Venezuela operation of 3 January 2026 reflects this pattern as an effects-led and systems-oriented approach aimed at degrading situational awareness, compressing reaction timelines, shielding manoeuvre, and achieving political-military objectives under escalation

control. In this model, the adversary is treated not as isolated units and installations, but as a connected operational fabric comprising power infrastructure, telecommunications, sensors, command chains and narrative authority. The campaign therefore targets the seams that sustain cohesion, responsiveness and legitimacy. Limited disruption of selected systems may generate effects disproportionate to the scale of disruption itself. Temporary degradation of communications can delay command execution; reduced confidence in sensing can weaken defensive responsiveness; and fragmentation of authoritative messaging may amplify uncertainty during periods of heightened operational tempo. The significance of such sequencing lies in its ability to generate temporary operational asymmetry. Cyberspace exploitation establishes access and intelligence advantage prior to overt action, while CA and electromagnetic effects convert that access into selective operational pressure during decisive phases. Kinetic manoeuvre then exploits the resulting window, while information-domain effects emerge simultaneously through degraded command continuity, fragmented communication and intensified narrative competition. The objective is not indiscriminate disruption, but calibrated effects sufficient to constrain coherent resistance while preserving escalation control and post-operation flexibility.

The Venezuela case therefore illustrates a broader transformation in contemporary warfare in which success increasingly derives from the synchronisation of effects across domains and the compression of adversary decision-making timelines at decisive moments. In such campaigns, military advantage rests not solely on superior capability, but on the ability to shape the conditions under which the adversary perceives, decides, coordinates and responds.

Operational Context and Timeline of Events

In the early hours of 3 January 2026, a sequence of operational effects unfolded across Venezuela that shaped the execution environment for subsequent kinetic action. Public reporting indicated localised degradation of radar coverage and reduced air-defence responsiveness during the initial phase of the operation, coinciding with the movement of air and rotary-wing assets. Within the same operational window, disruptions to telecommunications were reported, affecting both civilian and governmental communication channels in and around Caracas. These effects were followed by localised power outages impacting urban centres and elements of critical infrastructure during the period of highest operational tempo. Kinetic action and leadership targeting occurred within this window of degraded sensing, communications

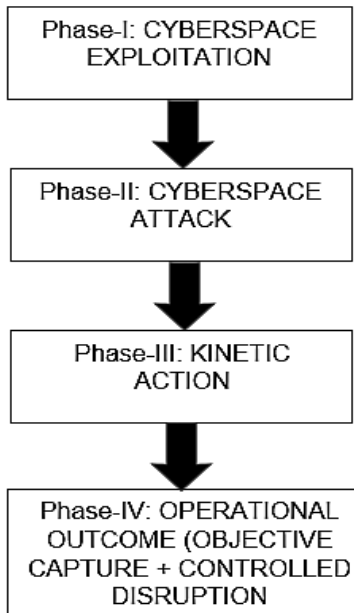
and coordination. In the immediate aftermath, restoration of services proceeded unevenly, while command continuity and information coherence remained fragmented.²³ The temporal alignment of these effects suggests deliberate shaping of the operational environment prior to and during kinetic execution, rather than isolated or sequential system failures.

Cyberspace Exploitation (CE) and Intelligence Preparation of the Operational Environment

Cyberspace exploitation constitutes the preparatory phase that enables operational choice without producing overt effects. In the context of the Venezuela operation, the observed pattern of synchronised disruption is consistent with prior intelligence preparation of the operational environment, in which critical digital dependencies and command relationships are mapped in advance of execution. Such preparation enables discrimination rather than indiscriminate disruption, allowing planners to identify which systems can be temporarily suppressed to generate operational advantage while limiting escalation risk and avoiding long-duration infrastructure damage.²⁴ At the operational level, cyberspace exploitation supports persistence and optionality. Rather than relying on a single access point or a single effect, exploitation activity seeks multiple pathways and redundant footholds that can be activated selectively and survive partial exposure. This approach reduces uncertainty at the moment of execution and enables precise timing of later effects. The value of exploitation lies in the ability to transition from access and observation to controlled effects without having to re-enter the environment under crisis conditions. A central output of exploitation is dependency mapping across infrastructure and command systems. Power distribution, telecommunications, radar interfaces and command-and-control networks function as an enabling layer for state response. Understanding how these systems interact, reroute and recover under stress informs decisions on the timing, scope and duration of subsequent non-kinetic and kinetic actions.

Cyberspace Attack (CA) and Electromagnetic Spectrum Effects

Cyberspace attack follows exploitation as the controlled application of disruption intended to amplify kinetic effectiveness during a defined operational window. Precision characterises this stage, with effects designed to be geographically limited, time-bound and reversible, denying the adversary the ability to observe, coordinate and respond during decisive phases without causing prolonged governance collapse or humanitarian fallout. In the Venezuela case, the reported concurrence of communications disruption and



localised power outages during the period of highest operational tempo is consistent with this logic of calibrated denial. When combined, even limited degradation of power and telecommunications can disproportionately affect command continuity, coordination and situational awareness. These effects do not require comprehensive infrastructure failure to be operationally significant. Temporary uncertainty and delayed response are often sufficient to compress decision-making timelines and constrain coherent defensive action. Cyber effects in such operations function alongside electromagnetic spectrum activity rather than in isolation. Degradation of radar coverage, sensing confidence, or communications reliability may result

from cyber action, electromagnetic interference, internal system fragility, or a combination thereof. The operational significance lies in the cumulative outcome rather than the specific mechanism, underscoring how cyber and EMS/EW measures can be synchronised to weaken sensing, coordination and recovery during the decisive operational window.²⁵

Integration with Kinetic Action and Information Effects

Kinetic action represents the culmination of the effects chain, executed after the adversary has been conditioned by non-kinetic shaping. Reduced sensing, disrupted communications, delayed decision cycles, and uncertainty regarding the operational picture combine to limit effective resistance during the execution window. In this construct, non-kinetic effects are not merely supporting measures, but enabling conditions that protect manoeuvre, reduce exposure and increase the probability of mission success. The operational advantage generated by this integration lies in time dominance.²⁶ By compressing the adversary's ability to react, the attacker completes kinetic objectives before coherent response can be organised. The Venezuela case indicates that cyber and electromagnetic effects were employed not to replace kinetic action, but to shape the battlespace in which it occurred. The same

effects also generated immediate information-domain consequences by degrading authoritative messaging, increasing uncertainty, and accelerating narrative competition during the highest-tempo phase. Once objectives were achieved, attenuation of non-kinetic effects preserved post-operation flexibility and limited escalation risk.

Operational Outcome and Immediate Effects

The integrated sequencing of cyberspace, electromagnetic, kinetic and information effects produced a compressed operational window in which adversary response was fragmented and delayed. During this period, degradation of sensing, disruption of communications, and uncertainty within command structures constrained coordinated defensive action and reduced the effectiveness of air-defence and internal security mechanisms. Kinetic objectives were executed within this window under conditions of limited situational awareness and restricted response capacity. In the immediate aftermath, restoration of critical services occurred unevenly, while command continuity and information coherence remained impaired. From an operational perspective, the outcome was not the permanent denial of infrastructure or governance, but the temporary suppression of adversary coherence sufficient to enable mission accomplishment while preserving escalation control and post-operation flexibility.²⁷

Strategic Observations from the Campaign

Sequencing as a Strategic Instrument of Power

The most consequential feature of the Venezuela campaign was not the employment of any individual capability, but the orchestration of effects across time. Sequencing emerged as a strategic instrument in its own right, enabling limited actions to generate disproportionate outcomes.²⁸ By arranging cyberspace exploitation, non-kinetic disruption and kinetic force into a coherent temporal logic, the operation shaped the conditions under which decisions were made, rather than merely contesting physical terrain. This approach reflects a shift from platform-centric warfare towards condition-centric warfare, in which advantage is achieved by determining when and how an adversary is able to perceive, decide and respond. For senior commanders, the implication is increasingly clear: operational success derives not solely from mass or persistence, but from mastery of sequence, synchronisation and timing.

Control of Time as the Central Objective of Contemporary Operations

The campaign demonstrates that modern conflict is increasingly decided through control of time rather than control of space. Temporary disruption of sensing, communications and coordination compressed adversary decision cycles during the decisive moment, creating a window in which kinetic objectives could be achieved with limited resistance. This form of time dominance does not seek permanent denial or destruction. Rather, it exploits transient asymmetry by acting faster than an adversary can comprehend unfolding events and organise a coherent response. Such an approach reflects a maturation in military thought, where the objective is not indefinite suppression of an adversary, but temporary disruption sufficient to secure operational advantage. This has important implications for force design, planning and command philosophy, privileging tempo, adaptability and synchronisation alongside endurance and mass.

Information Effects as a Consequence of Structural Dependency

A critical insight from the operation is that information-domain effects increasingly arise from structural dependency rather than deliberate messaging or manipulation.²⁹ Disruption of command continuity, degradation of communication pathways, and leadership uncertainty collectively weakened narrative coherence during the decisive phase.³⁰ These effects were not primarily psychological; they were systemic.³¹ In digitally dependent environments, the ability to communicate authoritatively and consistently becomes inseparable from the integrity of underlying networks. Once that integrity is disrupted, information instability follows as a natural operational consequence. For military planners, this reinforces that influence and perception can no longer be treated as separate lines of operation. They increasingly emerge from the performance of command systems under stress. The contest for narrative advantage therefore begins not only with messaging, but with the resilience of the systems through which authority communicates, and legitimacy is maintained.

Digital Dependence as a Strategic Centre of Gravity

The Venezuela case reinforces that digital infrastructure has become a strategic centre of gravity in contemporary conflict. Power systems, telecommunications, sensing networks and command architectures form a tightly coupled operational substrate upon which both military and civil authority depend. Disruption of this substrate, even temporarily, generates cascading effects extending well beyond the tactical level. This dependence

not only creates strategic leverage, but also strategic vulnerability. The decisive question for future conflicts is no longer whether digital systems will be targeted, but whether states possess sufficient resilience to absorb disruption without the loss of operational coherence. Resilience is therefore no longer a defensive afterthought; it is increasingly a determinant of deterrence credibility, operational endurance and strategic stability.

VENEZUELA'S TELEGRAM ECOSYSTEM AND THE INFORMATION-DOMAIN BATTLEFIELD

In the 18 months preceding January 2026, Venezuela developed a Telegram-based communications ecosystem that served simultaneously as a regime command-and-control medium and an influence platform embedded within civilian communications. The system combined centralised leadership direction with distributed participation by security forces, loyalist groups and civilians. This structure enabled governance coordination, internal security reporting, and propaganda dissemination at speed and scale. Telegram's architecture, comprising invite-only command groups, semi-autonomous influence channels, and civilian-integrated reporting nodes, created an operationally opaque communication environment in which state activity was embedded within routine civilian messaging. Given the limits of open-source reporting, the assessment of Telegram's internal operational use remains inferential and is based upon reported leadership statements, observed platform behaviour, and publicly reported information effects. The events of 3 January 2026 nevertheless exposed the fragility of this hybrid architecture. The kinetic removal of executive leadership produced immediate disruption within regime communications and triggered cascading effects across the information domain. Telegram rapidly became a contested digital battlespace marked by fractured command continuity, competing narratives, and loss of centralised information control.³²

Telegram as a Communication and Control Platform

The Venezuelan leadership's migration from WhatsApp to Telegram in mid-2024 represented a deliberate reconfiguration of national communication infrastructure. Publicly justified by President Nicolás Maduro as a response to external manipulation and internal destabilisation, the shift was intended to improve regime resilience and reduce exposure to foreign influence. Over time, Telegram evolved into a primary platform for regime communication, coordination, mobilisation and narrative control.

Invite-Only Command Networks

Closed Telegram groups were established as controlled channels for transmitting directives from executive authorities to loyalist security forces and affiliated units. These groups enabled rapid dissemination of orders while reducing exposure to platform moderation, public scrutiny and routine external collection.

Propaganda and Influence Channels

Semi-autonomous channels functioned as hubs for narrative dissemination, crowd-sourced reporting and social targeting. These channels allowed regime messaging to circulate widely while remaining embedded within civilian information flows. Their operational value lay in speed, reach and deniability, enabling official and semi-official narratives to spread without always appearing as direct state communication.

Operational Security Architecture

Telegram's encryption, governance model and group-management features enabled near real-time coordination while reducing external visibility. This created a "black box" communication environment that shielded operational activity from routine oversight and made the boundary between civilian communication, regime coordination and influence activity increasingly difficult to distinguish.

Civil–Military Integration

Civilians were incorporated into reporting and surveillance networks, providing local situational inputs to central nodes. This integration not only extended regime reach into communities but also increased dependence on leadership continuity and uninterrupted information flows. The same network that strengthened internal visibility in normal conditions became vulnerable under leadership disruption, as the loss of central direction could rapidly convert distributed participation into rumour, confusion and uncontrolled narrative spread.³³

Impact of Leadership Decapitation on Telegram Networks

The neutralisation of Venezuela's executive leadership generated immediate disruption across the Telegram ecosystem.³⁴ The loss of central coordination nodes fragmented command channels, resulting in delays, conflicting instructions, and temporary paralysis among regime-aligned actors. Digital command networks dependent upon vertical authority struggled to function

in the absence of clear leadership direction. At the same time, the absence of authoritative messaging created an information vacuum. Unverified claims regarding leadership status, governance continuity, and defections spread rapidly across both operational and civilian channels. Civilian participation amplified these effects as forwarding, commentary, and speculation accelerated the diffusion of contradictory narratives. Situational awareness degraded rapidly, complicating coordination, response and confidence in official direction.

Telegram, Information-Domain Exploitation and Digital Instability

The disruption of Telegram networks following leadership decapitation created exploitable conditions in the information domain without the need for direct cyber intrusion. With regime-controlled channels temporarily paralysed, competing narratives emerged and circulated with limited resistance. Telegram's high interconnectivity and message-forwarding architecture accelerated the diffusion of unverified information and operational rumours. As centralised messaging weakened, alternative narratives gained visibility. Civilian actors who had previously functioned as extensions of regime reporting and surveillance networks became inadvertent amplifiers of emergent information flows. Influence effects were therefore achieved indirectly, driven less by deliberate manipulation than by the structural dependence of the Telegram ecosystem on centralised leadership. In the absence of effective central control, prominent channels and administrators assumed quasi-authoritative roles, shaping localised information environments and partially substituting for formal state communication mechanisms. Narrative competition intensified, and coherence proved difficult to restore. The information environment was further complicated by the circulation of AI-generated avatars, deep-fake audio and video, and fabricated proof-of-life messages.³⁵ These artefacts exploited platform dynamics to prolong uncertainty, erode trust in authoritative sources, and complicate verification. The convergence of leadership disruption, platform dependence, and AI-enabled content generation therefore produced sustained instability within the digital information environment, demonstrating how modern information-domain effects can emerge from structural disruption as much as from deliberate influence operations.³⁶

STRATEGIC LESSONS

The January 2026 Venezuela crisis illustrates a deeper transformation in the character of conflict that extends beyond the integration of cyber, kinetic

and information operations. The campaign reveals how modern warfare increasingly targets coherence itself—the ability of a state or organisation to sense, decide, communicate and sustain authority under pressure. The following lessons move beyond platform- or domain-specific observations and instead highlight structural dynamics likely to shape future warfare, deterrence and strategic stability.

Warfare Has Shifted from the Destruction of Capability to the Disruption of Coherence

A central and under-appreciated lesson of the Venezuela case is that contemporary operations no longer require the systematic destruction of military capability to achieve decisive effect. Instead, temporary disruption of coherence across sensing, command, communications and narrative authority can be sufficient to enable operational success.³⁷ Cyber and electromagnetic effects did not seek to dismantle infrastructure permanently; kinetic action did not aim to annihilate forces wholesale. Rather, the campaign disrupted the adversary's ability to function as an integrated system at the decisive moment. This reflects a broader transition from attrition-centric warfare towards coherence-centric warfare, in which the objective is not merely to destroy capability, but to prevent the adversary from acting as a unified and self-consistent entity. For future doctrine, this suggests that victory conditions may increasingly depend upon the temporary disruption of an adversary's ability to understand events, coordinate response, and sustain effective decision-making during decisive periods, rather than solely upon physical destruction.³⁸

Time, Not Territory, Is Emerging as the Primary Object of Contest

The campaign demonstrates that the central currency of modern conflict is increasingly time rather than space. Control was exercised not by holding ground or destroying forces, but by compressing the adversary's decision horizon while preserving one's own. Cyber and non-kinetic effects were delayed, desynchronised, and responses were disrupted, creating a temporal asymmetry that rendered conventional defensive reactions increasingly ineffective.³⁹ This inversion carries significant implications. States capable of generating short-lived but decisive temporal advantage may achieve outcomes disproportionate to their material investment. Future conflicts may therefore be decided in minutes or hours of engineered disorientation rather than through prolonged engagements, placing increased emphasis on anticipatory planning, rapid execution and organisational adaptability.

Civilian Digital Platforms Have Become Latent Command Systems

The Venezuelan Telegram ecosystem reveals an important structural reality: civilian digital platforms increasingly function as latent command-and-control systems, even when not formally designed for such purposes. Governance coordination, internal security reporting, influence dissemination, and situational awareness became embedded within routine civilian communication flows. This fusion expands state reach but simultaneously erodes distinctions between civilian and military information spaces. The critical implication is that once civilian platforms assume command-like functions, they inherit command-like vulnerabilities. The disruption of leadership continuity or information integrity can propagate rapidly across the wider ecosystem. Future military planning must therefore treat major civilian platforms not merely as venues for influence, but as *de facto* operational infrastructure whose stability, redundancy and failure modes directly affect state resilience and operational effectiveness.

Precision Is Now a Strategic Attribute, Not a Tactical Preference

The Venezuela operation underscores that precision in cyber and non-kinetic effects is no longer merely a matter of reducing collateral damage; it has become a strategic attribute linked to escalation control, legitimacy and post-conflict manoeuvre space. Time-bound and reversible effects enabled operational objectives to be achieved without foreclosing political options or triggering uncontrollable retaliation. This suggests that restraint, when deliberately engineered, may itself become a source of strategic strength. States capable of calibrating disruption with high temporal and functional precision gain greater freedom of action across the escalation spectrum. Precision should therefore be understood not simply as tactical efficiency, but as a strategic capability enabling influence without entrapment and coercion without long-term commitment.

CYBER WARFARE AS A DOMAIN OF INTEGRATED AND SYNCHRONISED OPERATIONS: IMPLICATIONS FOR INDIA

Cyberspace as a Permanently Contested Battlespace

The principal implication of the Venezuela case for India is the confirmation that cyberspace is no longer episodic or situational, but continuously contested. Cyber operations shape readiness, perception and escalation dynamics long before the outbreak of kinetic hostilities. For India, this

necessitates a shift away from crisis-centric cyber postures towards persistent engagement.⁴⁰ Cyber forces must operate continuously in the competition space, integrating intelligence collection, defensive hardening, and adversary mapping as standing military functions. Failure to maintain sustained presence in cyberspace risks strategic surprise and erosion of decision advantage during the opening phases of conflict.⁴¹

Cyber Power as an Instrument of Operational Art

Cyber capabilities derive strategic value not from scale or disruption alone, but from their integration into operational design. The Venezuela case demonstrates that cyber effects are most effective when employed to condition the battlespace, compress adversary reaction time, and protect kinetic manoeuvre. For India, this implies that cyber operations must be planned and commanded as instruments of operational art rather than technical support functions.⁴² Cyber planners should therefore be embedded within joint operational headquarters, with clear authorities for sequencing cyber, electromagnetic, kinetic and information effects. However, without such integration, cyber power may remain a technically capable but strategically under-utilised instrument, unable to decisively shape the operational environment, tempo and outcome of military campaigns.

Force Structure and Human Capital as Decisive Constraints

The effectiveness of cyber warfare is constrained less by technology than by organisation, doctrine and human capital. Sustained cyber operations demand highly skilled operators with deep technical expertise, operational judgement and continuity of experience. Conventional personnel systems, designed around rotational command appointments and generalist career progression, remain poorly suited to this requirement. For India, cyber force development must therefore prioritise specialised career pathways, longer tenures, structured talent retention and continuous skill renewal. Without deliberate human-capital reform, cyber formations may exist as formal structures, but may lack the depth, specialisation, continuity and resilience required to sustain advantage across prolonged competition and conflict.

Resilience and Critical Infrastructure as Determinants of Deterrence

India's growing dependence upon networked command systems, digital logistics, satellite connectivity, and data-driven decision-making creates both operational advantage and strategic vulnerability. The Venezuela case

demonstrates how limited disruption within digital systems can cascade into delayed response and loss of coordination without extensive physical destruction. Protection of critical infrastructure—military and civilian—therefore becomes inseparable from national defence. For India, resilience must increasingly be treated as deterrence by denial.⁴³ Redundancy, rapid recovery and effective civil–military coordination reduce the strategic payoff of adversary cyber operations while preserving operational freedom under pressure.⁴⁴ States capable of functioning through disruption constrain adversary options, strengthen deterrence credibility, and contribute to escalation stability during crises.

CONCLUSION

The Venezuela crisis of January 2026 underscores the transformative character of contemporary hybrid warfare, in which cyberspace, kinetic operations and information-domain activities are integrated to generate rapid and decisive effects. The operation demonstrates that cyber capabilities—both exploitation and precision disruption—are most effective when deliberately sequenced to shape adversary situational awareness, condition the operational environment, and enable kinetic action at decisive moments. Civilian-integrated digital networks, exemplified by the Venezuelan Telegram ecosystem, simultaneously expand operational reach and create systemic vulnerability, highlighting the dual-use character of modern communication infrastructure in conflict. From a doctrinal perspective, the case reinforces the necessity of unified operational frameworks that deliberately integrate cyber, kinetic, electromagnetic and information-domain activities. Such frameworks must account for cross-domain sequencing, dependencies between centralised and distributed systems, escalation management, and the exploitation of civil–military digital integration without introducing structural fragility. Precision, reversibility and legal alignment of cyber effects emerge not merely as technical preferences, but as strategic attributes that preserve flexibility, legitimacy and operational freedom while amplifying force effectiveness across both physical and cognitive dimensions of conflict. More fundamentally, the Venezuela crisis illustrates that future conflicts will increasingly be contested not only across physical battlefields, but within digital and informational environments where coherence, timing and perception shape operational outcomes. Cyber-enabled operations are no longer peripheral or episodic activities; they increasingly function as instruments of operational art requiring integration at the highest levels of command and planning. As states become

more dependent upon networked command, sensing and communication systems, the ability to sustain coherence under disruption will increasingly define combat effectiveness.⁴⁵

For India, the enduring lesson is clear; preparedness for future conflict will depend not only upon military capability, but upon the ability to anticipate disruption, sustain operational resilience, and integrate cyber and information-domain operations as inseparable elements of modern manoeuvre. The Venezuela case therefore offers enduring lessons for defence planning, force development, and doctrinal adaptation in an era of persistent digital contestation.

ACKNOWLEDGEMENT

This article is based exclusively on open-source information, publicly available reports, policy documents and secondary analytical material. Any discussions or exchanges that may have informed the author's thinking were informal in nature and did not involve access to privileged, classified, or restricted information. No external funding, sponsorship, or financial support was received for this work. The views, assessments, and interpretations expressed are solely those of the author and do not reflect the official policies, positions, or assessments of any government, military organisation, or affiliated institution.

NOTES

1. 'Explosions Reported in Caracas as U.S. Operation Unfolds', *The Guardian*, 3 January 2026, available at <https://www.theguardian.com/world/2026/jan/03/explosions-reported-venezuela-caracas>.
2. Maren Leed, *Offensive Cyber Capabilities at the Operational Level*, Center for Strategic and International Studies (CSIS), Washington DC, 2025, available at <https://www.csis.org/analysis/offensive-cyber-capabilities-operational-level>.
3. *Hybrid warfare* refers to the coordinated use of conventional military force, cyber operations, information activities, electromagnetic effects, political pressure, economic tools, and other instruments of state power to achieve strategic objectives, often below the threshold of declared war.
4. *Cyberspace exploitation (CE)* refers to operations undertaken to gain access to adversary networks, collect intelligence, map digital dependencies and prepare future operational options. *Cyberspace attack (CA)* refers to operations intended to disrupt, deny, degrade, manipulate, or destroy information, networks, systems, or digitally dependent capabilities.

5. 'Joint Publication 3-12: Cyberspace Operations', Department of Defense, United States of America, 8 June 2018, available at <https://nsarchive.gwu.edu/document/16681-joint-chiefs-staff-joint-publication-3-12>.
6. Antiy Labs, 'Preliminary Analysis and Reflections on the Large-Scale Blackout in Venezuela', 2025, available at <https://mp.weixin.qq.com/s/VeauL3WQE5dQsQP0huBl7w>.
7. *Non-kinetic measures* are actions that produce military or strategic effects without the direct application of physical force. These may include cyber disruption, electronic warfare, electromagnetic interference, deception, information operations, or psychological effects.
8. *Operational environment* refers to the combination of physical, cyber, electromagnetic, informational, political, social, and infrastructural conditions that influence the planning and conduct of military operations.
9. 'Joint Publication 3-0: Joint Campaigns and Operations', Department of Defense, United States of America, 2022.
10. *Proceedings of the 24th European Conference on Cyber Warfare and Security*, European Conference on Cyber Warfare and Security, Vol. 24, No. 1, 25 June 2025.
11. *Platform-centric warfare* focuses primarily on the employment of military platforms such as aircraft, ships, missiles, tanks, or satellites. Condition-centric warfare focuses on shaping the conditions under which the adversary senses, decides, communicates, and responds.
12. 'Maduro Calls for Using Telegram Instead of WhatsApp', *Dearborn.org*, 2026, available at <https://dearborn.org/preview/maduro-calls-for-using-telegram-instead-of-whatsapp-59064>.
13. 'Summary of the 2023 Cyber Strategy of the Department of Defense', Department of Defense, United States of America, 2023, available at https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.pdf.
14. Rosa Brooks, *The New Geometry of Conflict: How Digital Systems Shape Modern War*, Lawfare/Brookings Institution, 2024.
15. *Cyberspace as an Operational Domain*, NATO CCDCOE Publications, Tallinn, Estonia.
16. Maren Leed, *Offensive Cyber Capabilities at the Operational Level*, n. 2.
17. 'Joint Publication 3-12: Cyberspace Operations', n. 5. *Force multiplier* refers to a capability that increases the effectiveness of other military instruments. In this context, cyber effects enhance kinetic effectiveness by degrading adversary sensing, command, coordination, communications and response capacity.
18. *Battlespace* refers to the environment, conditions and systems—physical, digital, informational and electromagnetic—within which military operations are conducted and combat power is applied.
19. 'Cyber Effects and Escalation Control in Great Power Competition', RAND Corporation, 2024.

20. M. Fischerkeller and R. J. Harknett, 'Persistent Engagement, Agreed Competition, and Cyberspace Interaction', *Journal of Cybersecurity*, Vol. 5, No. 1, 2019.
21. *Effects chain* refers to a deliberate operational sequence in which one action creates conditions for the next. In this context, the sequence may be understood as CE CA/EMS kinetic action information-domain effects.
22. *Electromagnetic Spectrum Manoeuvre (EMS)/Electronic Warfare (EW)* refers to military activity intended to use, protect, manipulate, or deny access to the electromagnetic spectrum in support of military objectives, affecting radar, communications, sensing, navigation and command systems.
23. *Information coherence* refers to the ability of political and military authorities to maintain clear, consistent and credible messaging during crisis. Loss of information coherence may generate uncertainty, competing narratives and reduced public confidence.
24. 'Cyber Effects and Escalation Control in Great Power Competition', RAND Cyber Research, 2024.
25. Maren Leed, *Offensive Cyber Capabilities at the Operational Level*, n. 2.
26. *Time dominance* refers to the ability to act and achieve objectives faster than an adversary can observe, understand, decide and respond effectively during a critical operational window.
27. F. G. Hoffman, 'Hybrid Warfare and Challenges', *Joint Force Quarterly*, No. 52, 2009.
28. *Sequencing as a strategic instrument* refers to the deliberate arrangement of military and non-military actions in time to shape adversary decision-making, create operational advantage, and enable effects disproportionate to the scale of individual actions.
29. *Structural dependency* refers to reliance on interconnected systems whose disruption can produce cascading effects across command, infrastructure, governance and public communication.
30. *Narrative coherence* refers to the ability of political or military authority to maintain a consistent, credible and widely accepted account of events during crisis. Its disruption may generate uncertainty, competing claims and erosion of public confidence.
31. D. Kilcullen, *The Dragons and the Snakes: How the Rest Learned to Fight the West*, Hurst & Company, London, U.K., 2020.
32. I. Ali, E. Banco, S. Holland and P. Stewart, 'Mock House, CIA Source and Special Forces: The U.S. Operation to Capture Maduro', *Reuters*, 4 January 2026, available at <https://www.reuters.com/business/aerospace-defense/mock-house-cia-source-special-forces-us-operation-capture-maduro-2026-01-03/>.
33. 'Was the U.S. Capture of Venezuela's President Legal?', *Reuters*, 5 January 2026.
34. *Leadership decapitation* refers to the removal or neutralisation of senior political or military leadership with the intent of disrupting command continuity, coordination and decision-making.

35. *Deep fake* refers to AI-generated or manipulated audio, video, or visual content designed to imitate real individuals, often complicating authentication and increasing the risk of misinformation during crises.
36. 'Legality of U.S. Capture of Venezuela's Maduro in focus at United Nations', *Reuters*, 4 January 2026, available at <https://www.reuters.com/world/americas/legality-us-capture-venezuelas-maduro-focus-united-nations-2026-01-04/>.
37. *Coherence-centric warfare* refers to an approach in which the objective is to disrupt the adversary's ability to function as a coordinated system by weakening sensing, communication, decision-making and authority rather than relying primarily on physical destruction.
38. *Temporal dysfunction* refers to a temporary disruption in an adversary's ability to understand events, coordinate response, and act coherently during a decisive operational period.
39. 'U.S. Flexes Air Power in Maduro Extraction Mission', *Reuters*, 7 January 2026, available at <https://www.reuters.com/business/aerospace-defense/us-flexes-air-power-maduro-extraction-mission-2026-01-07/>.
40. *Persistent engagement* refers to the continuous conduct of cyber activity in the competitive space to maintain awareness, shape adversary behaviour, and reduce the risk of strategic surprise before open conflict.
41. Australian Strategic Policy Institute, 'Cyber isn't the Whole Story in Venezuela — But It's a Key Takeaway,' *The Strategist*, 29 January 2026.
42. Telegram Privacy Policy.
43. *Deterrence by denial* refers to reducing an adversary's expected gains by strengthening resilience, redundancy and defensive capacity, thereby making disruptive action less effective or worthwhile.
44. Louise Marie Hurel, 'Layered Ambiguity: U.S. Cyber Capabilities in the Raid to Extract Maduro from Venezuela', Royal United Services Institute (RUSI), 14 January 2026, available at <https://www.rusi.org/explore-our-research/publications/commentary/layered-ambiguity-us-cyber-capabilities-raid-extract-maduro-venezuela>.
45. 'The Wider Implications of U.S. Action in Venezuela: RUSI Experts React', Royal United Services Institute (RUSI), 7 January 2026, available at <https://www.rusi.org/explore-our-research/publications/commentary/wider-implications-us-action-venezuela-rusi-experts-react>.