http://dx.doi.org/10.18623/rvd.v23.5479

CYBER PRESSURE, THE PDVSA INCIDENT, AND THE CAPTURE OF NICOLÁS MADURO: AN OPEN-SOURCE ASSESSMENT

A PRESSÃO CIBERNÉTICA, O INCIDENTE DA PDVSA E A CAPTURA DE NICOLÁS MADURO: UMA ANÁLISE BASEADA EM FONTES DE DOMÍNIO PÚBLICO

Article received on: 11/19/2025
Article accepted on: 2/19/2026

João Marcos Barbosa Oliveira*
*Escola de Aperfeiçoamento de Oficiais (ESAO), Bento Gonçalves, Rio Grande do Sul, Brazil
barbosaoliveira.joao@eb.mil.br

Ismael Deus Marques**
**Fundação Getúlio Vargas (FGV), Brasília, Distrito Federal, Brazil
ismaeldmarques@gmail.com

Jovair Pazzini de Melo Souza*
*Escola de Aperfeiçoamento de Oficiais (ESAO), Bento Gonçalves, Rio Grande do Sul, Brazil
pazzini.jovair@eb.mil.br

Eduardo Stefani***
***Universidade Nove de Julho (UNINOVE), São Paulo, São Paulo, Brazil
eduardo_stefani@outlook.com

The authors declare that there is no conflict of interest

Abstract
The capture of Venezuelan President Nicolás Maduro in January 2026 was preceded by a series of non-kinetic events that reshaped the operational environment in Venezuela. Among these, a cyber incident affecting Petróleos de Venezuela S.A. (PDVSA) in December 2025 stands out as a relevant case of cyber pressure applied against critical infrastructure in the theater of operations. This article analyzes the PDVSA cyber incident using open-source information to assess its characteristics, documented impacts, and strategic relevance as contextual cyber pressure preceding a limited regime intervention. Rather than asserting direct causality between the PDVSA incident and the subsequent capture operation, the article situates the incident within broader discussions on cyber-enabled coercion, infrastructure vulnerability, and ambiguity in attribution. The study contributes an empirically grounded case analysis to the emerging literature on cyber operations as shaping mechanisms in contemporary conflict.

Keywords: Cyber Pressure. PDVSA. Operation Resolute. Venezuela.

Resumo
A captura do presidente venezuelano Nicolás Maduro, em janeiro de 2026, foi precedida por uma série de eventos não cinéticos que reconfiguraram o ambiente operacional na Venezuela. Dentre estes, um incidente cibernético que afetou a Petróleos de Venezuela S.A. (PDVSA) em dezembro de 2025 destaca-se como um caso relevante de pressão cibernética aplicada contra infraestruturas críticas no teatro de operações. Este artigo analisa o incidente cibernético na PDVSA utilizando informações de fontes abertas para avaliar suas características, impactos documentados e relevância estratégica como uma pressão cibernética contextual que precedeu uma intervenção limitada no regime. Em vez de afirmar uma causalidade direta entre o incidente na PDVSA e a subsequente operação de captura, o artigo situa o evento em discussões mais amplas sobre coerção viabilizada pelo espaço cibernético, vulnerabilidade de infraestruturas e ambiguidade de atribuição. O estudo contribui com uma análise de caso empiricamente fundamentada para a literatura sobre operações cibernéticas como operações de moldagem em conflitos contemporâneos.

Palavras-chave: *Pressão Cibernética. PDVSA. Operação Resolute. Venezuela.*

1 INTRODUCTION

Cyber operations increasingly shape the strategic environment in which military and political actions unfold. Rather than operating solely as decisive instruments, cyber activities often function as mechanisms of pressure, disruption, and uncertainty that condition decision-making and operational tempo [1]. In late 2025, Venezuela experienced a cyber incident affecting the state-owned oil company Petróleos de Venezuela S.A. (PDVSA), the backbone of the country's economy and a critical source of regime revenue [2].

This incident occurred weeks before the January 2026 U.S.-led Operation Absolute Resolve that resulted in the capture of President Nicolás Maduro. Public reporting indicates that the capture operation relied heavily on non-kinetic effects, including cyber and space-enabled capabilities, to limit regime response and coordination [3]. While the cyber incident at PDVSA was not officially linked to the capture operation, its timing and impact deserve analytical attention as part of the broader cyber environment in the Venezuelan theater.

This article addresses the following research question: how can the December 2025 PDVSA cyber incident be analytically understood as cyber pressure within the operational context preceding the January 2026 capture of Nicolás Maduro? The study does not seek to establish attribution or direct operational linkage. Instead, it aims to document the incident, assess its observable effects, and discuss its relevance within contemporary theories of cyber-enabled coercion and shaping operations.

2 CYBER OPERATIONS, PRESSURE, AND CRITICAL INFRASTRUCTURE

Cyber operations against critical infrastructure have been widely discussed as tools of coercion, signaling, and strategic pressure rather than solely as instruments of immediate battlefield advantage [4]. Energy infrastructure, in particular, occupies a central role due to its economic, political, and societal importance [5]. Disruption of administrative, logistical, or financial systems can impose costs, generate uncertainty, and force adversaries into reactive postures without crossing traditional thresholds of armed conflict [6].

The literature emphasizes that such operations are often characterized by ambiguity. Attribution is frequently contested, technical details remain undisclosed, and effects may be indistinguishable from systemic fragility or mismanagement [7]. This ambiguity can itself serve strategic purposes by impacting response options and limiting escalation pathways [8].

3 METHODOLOGY

This study employs a qualitative case-study methodology based on open-source intelligence (OSINT). Sources include international news agencies, investigative journalism, policy analysis from think tanks, and official statements released between December 2025 and January 2026. The analysis follows a process-tracing approach, reconstructing a timeline of reported events and identifying consistent patterns across independent sources [9].

Evidence is evaluated based on source credibility, corroboration across outlets, and transparency regarding uncertainty. No classified material or technical forensic data was used. Consequently, conclusions are limited to observable effects and reported impacts rather than definitive attribution or technical characterization.

In addition to media reporting and policy analysis, the OSINT methodology employed in this study recognizes the value of structured, passively collected datasets that do not rely on vulnerability exploitation. Beyond the Crystal Vault repository, initiatives such as the *Venezuela Digital Observatory* systematically collect and monitor publicly accessible governmental domain data (e.g., .gob.ve and .mil.ve), including WHOIS records, name server configurations, and domain availability over time [10]. These datasets enable longitudinal assessment of state digital presence and infrastructure evolution, complementing narrative OSINT sources and reinforcing the analytical robustness of passive open-source collection techniques.

4 THE PDVSA CYBER INCIDENT (DECEMBER 2025)

In mid-December 2025, PDVSA publicly acknowledged that it had suffered a cyber incident, which Venezuelan authorities described as an external attack [2]. While

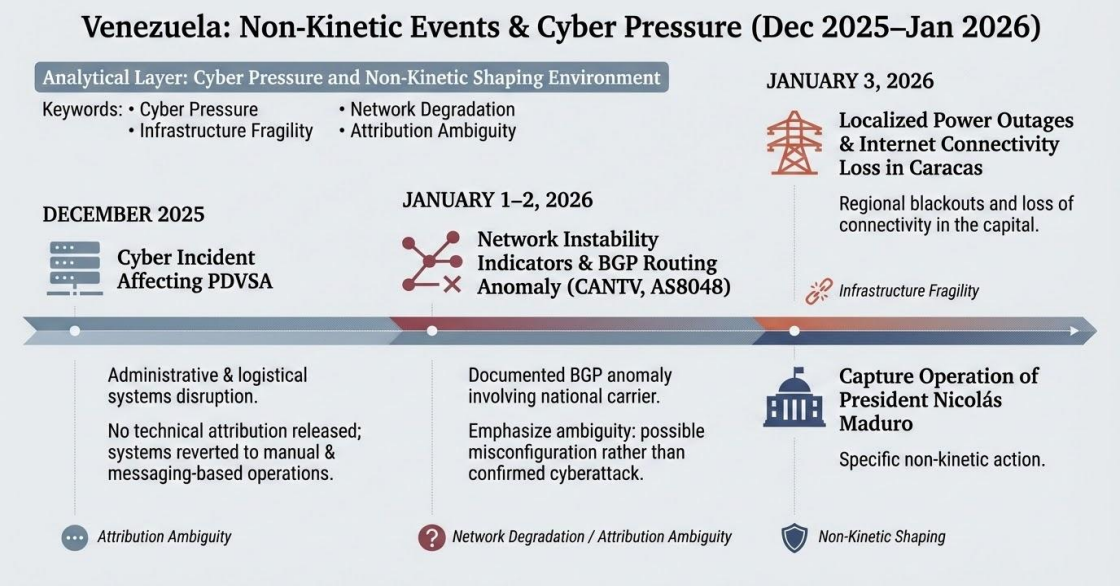
official statements claimed that oil production and exports were not significantly affected, reporting by independent sources indicated widespread disruption to administrative and logistical systems [11].

According to multiple accounts, PDVSA temporarily lost access to centralized information systems used for cargo scheduling, billing, and internal coordination. As a result, personnel reportedly reverted to manual record-keeping, phone calls, and messaging applications such as WhatsApp to sustain operations [11]. Some oil shipments were delayed, and coordination with foreign partners became more cumbersome, even as physical production continued [10].

Notably, no technical details regarding malware, intrusion vectors, or indicators of compromise were publicly released. Attribution claims made by Venezuelan officials were not supported by independent forensic evidence in the public domain [12]. The incident therefore exemplifies a cyber event that is operationally documented but technically opaque.

Figure 1

Timeline of Non-Kinetic Events in Venezuela Between December 2025 and January 2026



In addition to journalistic reporting, open-source intelligence initiatives have highlighted the extent of publicly exposed governmental information in Venezuela. Beyond Crystal Vault, the digital footprint of Venezuelan state entities can be

characterized through open-source geographic and structural datasets. Public repositories such as *venezuela-json* compile standardized geospatial data on Venezuelan municipalities, states, and administrative divisions, enabling spatial contextualization of governmental infrastructure without privileged access [13]. When combined with domain-level OSINT and API-derived metadata, such geospatial datasets allow for external profiling of connectivity patterns, administrative distribution, and potential points of systemic fragility at scale. The "Crystal Vault" OSINT repository aggregated approximately 9.3 GB of data from publicly accessible governmental APIs and WordPress endpoints, including thousands of media files containing EXIF metadata and hundreds of GPS coordinates linked to state institutions. This dataset illustrates how sensitive geospatial and organizational information can be passively collected without exploiting internal systems, reinforcing assessments of structural exposure and informational vulnerability within the Venezuelan state apparatus [14].

Although no evidence demonstrates that the PDVSA incident directly enabled the January 2026 capture operation, its strategic relevance lies in its contribution to a climate of vulnerability and uncertainty. PDVSA represents the financial lifeline of the Venezuelan regime; disruption to its administrative systems carries symbolic and practical weight [5].

From a strategic perspective, such an incident can be understood as cyber pressure rather than cyber attack in the narrow sense. By degrading bureaucratic efficiency and highlighting systemic fragility, the incident may have increased regime stress and reduced resilience in the face of subsequent non-kinetic and kinetic actions [6]. Importantly, the ambiguity surrounding the incident limited clear avenues for retaliation or escalation.

5 OPERATION RESOLUTION REVOLVE

Independent network measurement platforms provide additional contextual evidence regarding the digital environment surrounding the January 2026 operation. During the period coinciding with the capture of Nicolás Maduro, NetBlocks reported a measurable loss of internet connectivity in parts of Caracas, correlating with localized power outages during the operation. As a network monitoring organization that relies on real-time measurements rather than self-reported data, NetBlocks offers an independent

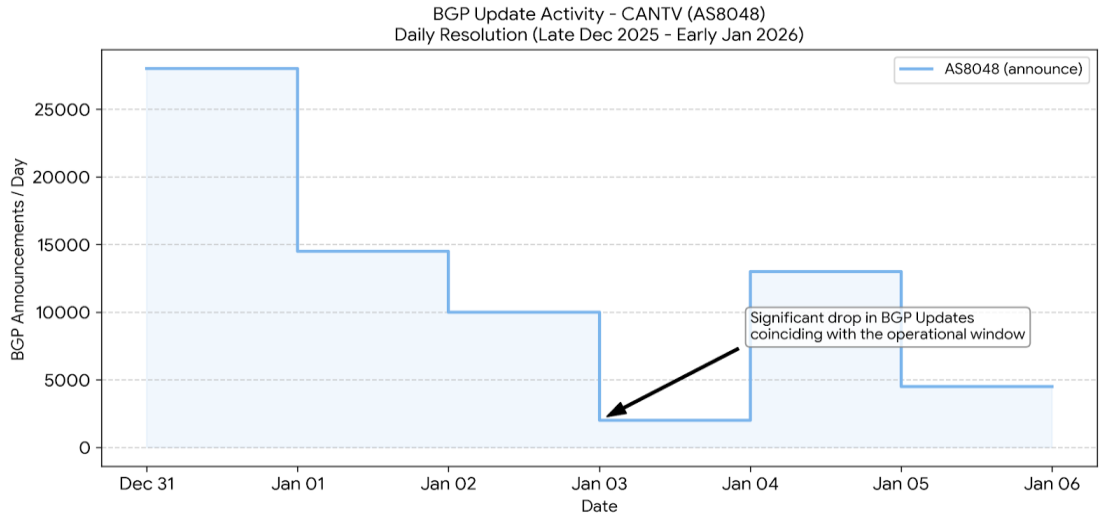
indicator of systemic disruption affecting communications infrastructure [15]. While such connectivity loss does not, in itself, demonstrate the presence of a cyberattack, it confirms that the operational environment experienced degradation consistent with non-kinetic disruption.

Complementary analysis from infrastructure and routing specialists further underscores the ambiguity inherent in interpreting these signals. Cloudflare documented a Border Gateway Protocol (BGP) anomaly involving Venezuela's primary telecommunications provider, CANTV (AS8048), on 2 January 2026, immediately preceding the capture operation. The analysis suggested that the event was more consistent with routing misconfiguration or policy failure than with a deliberate cyber intrusion [16]. Subsequent technical reporting echoed this interpretation, cautioning against premature attribution of the anomaly to offensive cyber activity [17].

Beyond isolated, short-duration anomalies such as route leaks, longitudinal network data reveals a broader pattern of infrastructure degradation during the operational window. Figure 2 illustrates the daily volume of Border Gateway Protocol (BGP) announcements for Venezuela's primary telecommunications provider, CANTV (AS8048), as aggregated by the RIPE Network Coordination Centre (RIPE NCC) [18]. A stark decline in routing activity is observable in early January 2026: daily announcements plummeted from approximately 28,000 in late December to fewer than 2,000 by 3 January. This macroscopic collapse in BGP update activity temporally aligns with both the localized power outages reported by NetBlocks and the execution of the capture operation, providing quantitative open-source evidence of severe, systemic network instability precisely when regime coordination capabilities were most critical.

Figure 2

Daily BGP Update Activity for CANTV (AS8048) Between Late December 2025 and Early January 2026



Note. Data derived from RIPE NCC (RIPEstat) [18].

Notably, a review of public and auditable datasets from major academic and operational network-monitoring platforms, including the Internet Outage Detection and Analysis project (IODA), RIPE Atlas, and BGPStream, did not yield evidence explicitly attributing network disruptions during the capture of Maduro to a cyberattack. No official reports or event bulletins from these platforms documented anomalous traffic patterns, active probing failures, or routing incidents that could be conclusively associated with offensive cyber operations during the relevant time window [19]. The absence of such records does not preclude the possibility of cyber activity, but it reinforces the methodological necessity of restraint in attribution. In highly contested and opaque environments, the lack of corroboration from independent measurement infrastructures constitutes a meaningful analytical finding in itself, underscoring the limits of OSINT-based inference and the persistent ambiguity that surrounds cyber-enabled pressure in conflict environments. The PDVSA case illustrates several broader dynamics relevant to cyberwarfare scholarship. First, it underscores the gap between operational effects and technical transparency in cyber incidents affecting critical infrastructure. Second, it highlights how cyber events can function as shaping mechanisms within a broader campaign without serving as decisive actions themselves [8].

Finally, the case demonstrates the analytical challenges posed by reliance on OSINT in environments characterized by censorship, political polarization, and limited disclosure. In parallel, policy-oriented analyses have argued normatively for the deliberate use of sustained cyber pressure as a coercive instrument against the Venezuelan regime, framing cyber operations as an alternative to conventional military force [20]. While such contributions are valuable for strategic debate, they differ fundamentally from the present study's empirically grounded approach, which emphasizes observable effects, evidentiary limits, and attribution ambiguity rather than prescriptive advocacy. In this context, socio-political and juridical OSINT repositories also play an important complementary role. Projects such as *La Memoria de Venezuela* aggregate publicly available data on sanctioned individuals, legal proceedings, and international enforcement actions associated with Venezuelan political actors, drawing on sources including OFAC listings, judicial filings, and human rights documentation [21]. While not constituting technical cyber evidence, such datasets contextualize cyber incidents within broader patterns of institutional vulnerability, coercive pressure, and geopolitical constraint, enriching interpretation of cyber-related events beyond purely technical dimensions. These constraints necessitate cautious claims and emphasize the value of case-based documentation over definitive attribution.

6 CONCLUSION

The January 2026 capture of Nicolás Maduro unfolded within a complex non-kinetic environment marked by cyber incidents, infrastructure fragility, and measurable disruption to communications and power systems. In that context, the December 2025 cyber incident affecting Petróleos de Venezuela S.A. (PDVSA) is best understood as a salient instance of cyber pressure directed at a core pillar of regime stability. Publicly available evidence does not substantiate claims of direct operational linkage or confident technical attribution between the PDVSA incident and the capture operation; nonetheless, the incident remains analytically significant due to its timing, target selection, and observable operational effects.

Taken together, the PDVSA disruption and contemporaneous indicators of network degradation and routing instability, documented by sources such as NetBlocks

and Cloudflare, illustrate the layered ambiguity that characterizes cyber-enabled pressure in contested environments. The case shows how interference with administrative and logistical systems can generate strategic friction without producing decisive, attributable outcomes, aligning more closely with theories of cyber-enabled coercion and shaping than with models of cyber warfare centered on immediate battlefield effects. Methodologically, the study also underscores both the value and limits of OSINT: triangulating journalism, structured OSINT datasets, network measurement platforms, and socio-juridical repositories enables an empirically grounded reconstruction while leaving intent and authorship necessarily uncertain.

Ultimately, the Venezuelan case study serves as a critical precedent for future multi-domain operations. As military doctrines evolve to account for the convergence of physical and cyber theaters, the ability to project power through continuous cyber pressure will likely become a defining characteristic of warfare. For policymakers and defense planners, particularly in regions with highly exposed critical infrastructure, the lessons preceding Operation Absolute Resolve highlight the urgent need to integrate robust OSINT capabilities into national security frameworks. Furthermore, it underscores the necessity of developing resilience strategies that acknowledge attribution ambiguity not merely as a fog to be cleared, but as a permanent, weaponized feature of conflict.

REFERENCES

[1] Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux.

[2] Reuters. (2025, December 15). *Venezuela's PDVSA says operations unaffected by cyber attack, blames U.S*. https://www.reuters.com/world/americas/ venezuelas-pdvsa-says-operations-unaffected-by-cyber-attack-blames-us-2025-12-15/

[3] DiMolfetta, D. (2026, January 28). *US developed 'non-kinetic' cell ahead of Venezuela mission to push cyber operations*. Nextgov/FCW. https://www.nextgov.com/cybersecurity/2026/01/us-developed-non-kinetic-cell-ahead-venezuela-mission-push-cyber-operations/411029/

[4] Lindsay, J. R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies, 22*(3), 365–404.

[5] Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71.

[6] Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies, 24*(2), 316–348.

[7] Schmitt, M. N. (Ed.). (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge University Press.

[8] Moore, D. (2022). *Offensive cyber operations: Understanding intangible warfare*. Oxford University Press.

[9] Bennett, A., & Checkel, J. T. (2015). *Process Tracing and the Social Sciences*. Cambridge University Press.

[10] Ggangix. (2024). *Venezuela Digital Observatory*. GitHub repository. https://github.com/ggangix/venezuela-digital-observatory

[11] Bloomberg. (2026, January 15). *Venezuelan oil industry runs on WhatsApp after cyber attack*. https://www.bloomberg.com/news/articles/2026-01-15/ venezuelan-oil-industry-is-running-on-whatsapp-after-cyberattack

[12] The Record. (2025). Venezuela state oil company blames cyberattack on U.S., offers no evidence. https://therecord.media/venezuela-state-oil-company- blames-cyberattack-on-us

[13] Jobsamuel. (2023). *venezuela-json: Geospatial data of Venezuelan administrative divisions*. GitHub repository. https://github.com/jobsamuel/venezuela-json

[14] Ringmast4r. (2025). *Crystal Vault: Venezuela OSINT Dashboard*. https://ringmast4r.github.io/crystal-vault/

[15] NetBlocks (2026). Confirmed internet connectivity disruptions in parts of Caracas during power outages. NetBlocks. https://x.com/netblocks/status/ 2007434366545174662

[16] Cloudflare (2026). A closer look at a BGP anomaly in Venezuela. Cloudflare Blog. https://blog.cloudflare.com/bgp-route-leak-venezuela/

[17] The Register. (2026). Venezuela BGP routing incident likely misconfiguration, not cyberattack.

[18] RIPE NCC. (2026). RIPEstat: BGP Update Activity for AS8048. Réseaux IP Européens Network Coordination Centre. https://stat.ripe.net/

[19] CAIDA. (2024). *Internet Outage Detection and Analysis (IODA): Methodology and Platform Overview*. Center for Applied Internet Data Analysis. https://www.caida.org/projects/ioda/

[20] Healey, J. (2026). *The case for cyber pressure against Venezuela*. Lawfare. https://www.lawfaremedia.org/article/the-case-for-cyber-pressure-against-venezuela

[21] Takove. (2023). *La Memoria de Venezuela*. GitHub repository. https://github.com/takove/la-memoria-de-venezuela

Authors' Contribution

All authors contributed equally to the development of this article.

Data availability

All datasets relevant to this study's findings are fully available within the article.

How to cite this article (APA)

Oliveira, J. M. B., Marques, I. D., Souza, J. P. de M., & Stefani, E. (2026). CYBER PRESSURE, THE PDVSA INCIDENT, AND THE CAPTURE OF NICOLÁS MADURO: AN OPEN-SOURCE ASSESSMENT. Veredas Do Direito, 23(5), e235479. https://doi.org/10.18623/rvd.v23.5479