



CENTRAL INTELLIGENCE AGENCY

CIA NOTE

(U) Summary of Select Intelligence Reporting from 2004-2020 on Venezuela's Electronic Voting Manipulation Capabilities

29 June 2026



[REDACTED]

[REDACTED]



CENTRAL INTELLIGENCE AGENCY

CIA NOTE

29 June 2026

(U) Summary of Select Intelligence Reporting from 2004-2020 on Venezuela's Electronic Voting Manipulation Capabilities

(U) Summary

Intelligence Community reporting from 2004-2020 documented persistent concerns about Venezuelan government manipulation of electronic voting systems and the potential national security implications for US election infrastructure. The intelligence established that Venezuelan government officials developed sustained interest and likely some capability in manipulating electronic voting systems, including Smartmatic technology, to influence electoral outcomes in Venezuela. The 2006 Intelligence Community assessment that Smartmatic's ties to Venezuela posed a national security threat was based on solid intelligence regarding Venezuelan government intent to influence US politics and evidence of Venezuelan manipulation of their own electoral systems. This assessment led to US government action forcing Smartmatic to divest its US operations in 2007. reporting indicated that electronic voting systems contained vulnerabilities that could theoretically be exploited by sophisticated actors with insider access. However, while the intelligence validated significant concerns about foreign-linked voting technology vendors, it did not definitively confirm that large-scale electronic fraud was successfully executed in specific Venezuelan elections, with CIA's baseline assessments maintaining that other factors better explained electoral outcomes. The reporting on advanced techniques like provided concerning insight into alleged Venezuelan government capabilities and intent, but came from limited sourcing.

(U) **Scope Note:** This summary focuses on what Intelligence Community reporting established regarding Venezuela's intent and capabilities to manipulate voting machines, both domestically and potentially in other countries. It is not a comprehensive re-assessment of all available intelligence on this topic, but rather a summary of key findings from select intelligence documents spanning 2004 to 2020.

(U) Venezuela Government Interest in Election Manipulation

Intelligence sources between 2004 and 2020 reported that Venezuelan President Hugo Chavez and his successor Nicolas Maduro demonstrated sustained interest in manipulating electoral outcomes through electronic voting systems. In April 2004, intelligence reporting indicated Chavez stated his objective was to prevent the reelection of a sitting US president, suggesting intent to influence US domestic politics.¹ This finding was part of the basis for the Intelligence Community's 2006

¹ This product reflects a CIA perspective and was not coordinated within the intelligence Community. It was produced under the auspices of Deputy Director of CIA for Analysis.

CIA NOTE

assessment that Smartmatic's acquisition of US voting systems company Sequoia posed a "moderate threat" to US national security.²

██████████ Prior to Venezuela's 2012 presidential election, ██████████ reported that Chavez's intelligence services, including the General Directorate of Military Counterintelligence (DGCIM) and the Bolivarian Intelligence Service (SEBIN), worked with the National Electoral Council (CNE) and Smartmatic to develop plans to manipulate election results using preprogrammed voting machines. ██████████ reported that these plans called for deploying altered machines to approximately 300 voting centers in traditionally pro-Chavez areas to ensure victory by approximately 1.5 million votes.³ Following the election, which Chavez won by approximately 1.6 million votes, sources reported that Chavez congratulated his team for successfully implementing the manipulation plan.⁴

██████████ In September 2020, ██████████ reported that Venezuela ██████████ had developed detailed technical plans to manipulate the December 2020 National Assembly elections using what were ██████████. According to this reporting, the technique involved creating a second set of virtual machines that would replicate legitimate voting machine results, then substitute manipulated data while making votes appear to originate from legitimate machines. ██████████
██████████
██████████

(U) Technical Capabilities and Vulnerabilities

██████████ CIA analysts assessed in 2006 that certain capabilities ██████████ regarding electronic voting manipulation were technically possible and operationally feasible.⁵⁷ Specifically, ██████████ that voting machines

in Venezuela had unspecified artificial intelligence components installed, were designed to alter vote tallies, could detect when they were being audited, and could provide printed receipts without registering, recording or transmitting those votes.⁸ While CIA analysts judged these capabilities were theoretically achievable, this assessment focused on technical feasibility rather than confirmation that such features were actually implemented.

██████████ A 2013 CIA alternative analysis, produced using the "Devil's Advocacy" methodology, outlined a plausible scenario for how large-scale electronic manipulation could have occurred in Venezuela's 2012 election without detection. This analysis noted that Venezuela's electronic voting system was vulnerable to insider access, the centralized nature of the CNE's control over voting technology, and gaps in opposition monitoring capabilities. The report assessed that if such manipulation occurred, "elections in Venezuela and other countries that are clients of the technology provider could be in doubt."⁹ However, CIA's baseline assessment maintained that no large-scale electronic fraud occurred in 2012, based on pre-election polling data, absence of irregular voting patterns, and the opposition's concession.¹⁰

██████████ Intelligence reporting consistently indicated that individuals with ties to Venezuelan intelligence services had access to election technology and voting systems. In 2012, sources reported that Chavez assigned an army communications specialist to the CNE to provide real-time access to election results.¹¹ Reporting from 2012 also indicated that the CNE Information Technology Director, described as a confidant of the head of military intelligence with expertise in voting technology, was responsible for designing protocols for auditing voting software.¹² These relationships provided potential pathways for manipulation of electronic voting systems.

CIA NOTE

(U) [REDACTED] Technique

[REDACTED] The September 2020 intelligence reporting on [REDACTED] plans provided the most detailed description of a specific technical approach to election manipulation,

[REDACTED] technique was allegedly designed to:¹³

- [REDACTED] Replicate digital hash files sent to the central vote counting database;
- [REDACTED] Mimic real voting machines that favored the ruling party;
- [REDACTED] Overwrite hash files of voting machines that favored the opposition; and
- [REDACTED] Make altered votes appear to originate from legitimate voting machines.¹⁴

[REDACTED] this technique would, in theory, allow the Venezuelan government to monitor and adjust results in real-time during and after the election. The reporting indicated that virtual machine technology would be employed to accomplish this manipulation while evading detection through standard audit procedures.¹⁵

(U) IC Assessments and Concerns

[REDACTED] The 2006 National Security Threat Assessment produced by the National Intelligence Council evaluated Smartmatic's acquisition of Sequoia Voting Systems as a "moderate overall threat to US national security interests." This assessment was based on several factors:

- [REDACTED] Intelligence indicating Chavez's intent to influence US domestic politics and public opinion;
- [REDACTED] Reporting that the Venezuelan government manipulated Venezuelan national elections with Smartmatic's direct involvement;
- [REDACTED] [REDACTED] intelligence that Smartmatic directors held credentials from Venezuelan intelligence services
- [REDACTED] Open source reporting of corrupt relationships between Smartmatic and Venezuelan government officials; and
- [REDACTED] Smartmatic's and Sequoia's reported contracts in approximately 400 US counties at the time.¹⁶

[REDACTED] The assessment concluded that Smartmatic's susceptibility to Venezuelan government manipulation makes the acquisition a potential instrument for Venezuelan officials seeking to undermine confidence in, or manipulate the electoral process in, the United States.¹⁷ This finding led to pressure from the Committee on Foreign Investment in the United States (CFIUS) that resulted in Smartmatic divesting its ownership of Sequoia in 2007.

[REDACTED] In March 2018, Smartmatic ceased operations in Venezuela after publicly accusing the Maduro regime of inflating voter turnout by over one million votes in the August 2017 National Constituent Assembly election—figures that diverged from data recorded by Smartmatic's voting machines. This represented a break between Smartmatic and the Venezuelan government after years of the company providing electoral technology to Venezuela.¹⁸

CIA NOTE

(U) Limitations and Analytic Caveats

██████████ The intelligence reporting contains important limitations that must be considered when assessing what it establishes:

██████████ First, the 2006 Intelligence Community assessment concluded that neither Smartmatic nor the Venezuelan Government had the capability—that is, the level of control or access required—to manipulate the outcome of an election outside of Venezuela in a predictable fashion. The Venezuelan Government's ability to manipulate the results of voting in Venezuela rested in part on its ability to control every stage of the electronic voting process, from initial acquisition of the machines to pre- and post-voting machine security, to programming, to storage of paper voting receipts, to control of the audit process. Neither the Venezuelan Government nor Smartmatic would have such a complete spectrum of access during an electoral process outside Venezuela.¹⁹

██████████ Second, CIA's baseline assessment regarding Venezuela's 2012 election maintained that large-scale electronic fraud did not occur, despite ██████████ reporting of manipulation plans. This assessment was supported by pre-election polling showing Chavez ahead by approximately 10 percentage points, a 24% increase in government spending before the election, the opposition's concession of defeat, and CIA quantitative analysis showing no irregular voting patterns indicative of systematic manipulation.²⁰

██████████ Third, the 2013 Devil's Advocacy Report that outlined a plausible fraud scenario was explicitly an alternative analysis exercise rather than a definitive finding. The report acknowledged "conflicting ██████████ reporting" and "limited insight into key elements of the electronic voting system."²¹

██████████ Fourth, the September 2020 reporting on ██████████

██████████ and judged the regime did not need to resort to gross fraud to win the December 2020 National Assembly elections, given that virtually the entire opposition boycotted and the regime had already co-opted opposition party leadership.²²

CIA NOTE

[illegible][illegible]