[redacted]

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]

[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

[redacted] 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. [redacted] 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 [redacted] 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

[redacted] 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

[redacted] 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.

[redacted]

[redacted]

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.[6][7] 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.

(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]

[redacted]

(U) Limitations and Analytic Caveats

[redacted] The intelligence reporting contains important limitations that must be considered when assessing what it establishes.

[redacted] 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]

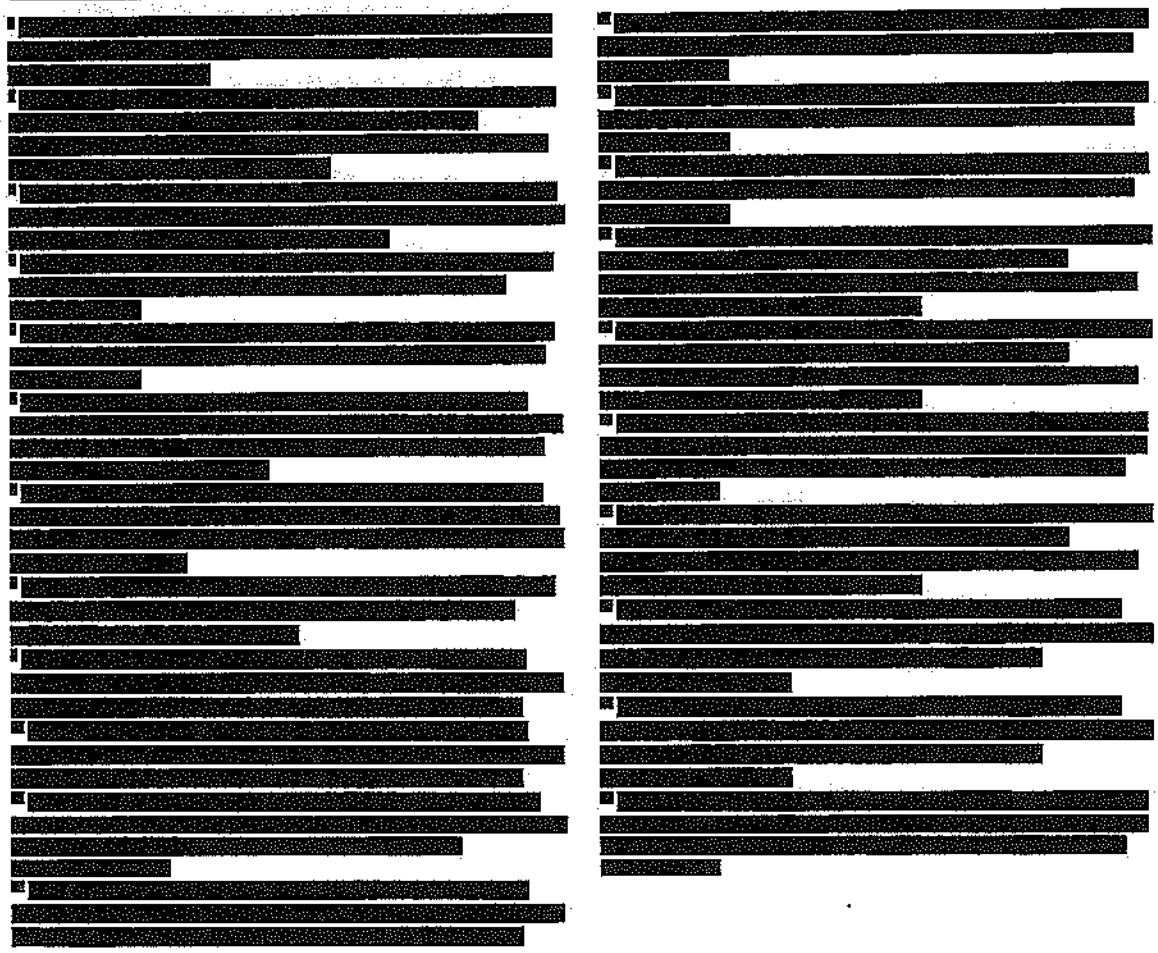
[redacted] Second, CIA's baseline assessment regarding Venezuela's 2012 election maintained that large-scale electronic fraud did not occur, despite [redacted] reporting of manipulation plans. This assessment was supported by pre-election polling showing Chavez ahead by approximately 10 percentage points, 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]

[redacted] 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 [redacted] reporting" and "limited insight into key elements of the electronic voting system."[21]

[redacted] Fourth, the September 2020 reporting on [redacted] 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]

[redacted]

CIA NOTE



[redacted]

[redacted]

Published online on 01 July 2020

[redacted] China: Cyber Activities Probably Prelude to Election Espionage

[redacted] ***China is probing the presidential campaign for opportunities to tailor collection and gather insight on policy positions on US-Chinese issues.*** US policy on China is a longstanding high collection priority for Beijing, and Chinese cyber actors have conducted such activity in every US presidential election campaign since at least 2008, according to [redacted] open-source reporting.

[redacted] *Chinese cyber actors are targeting US presidential campaign information, probably to gather intelligence that enables future operations.*

- [redacted] Since [redacted] 2018, Chinese cyber actors known in the private sector as APT31—[redacted]—have targeted the personal e-mail accounts of senior US leadership, including officials in the Executive Office of the President and high-ranking officials in multiple Executive Branch organizations, Congress, and the federal judiciary, [redacted]
- [redacted] Since 2017, a separate [redacted] has worked with the [redacted] to enable more stealthy operations by identifying the e-mail addresses of high-level US officials, then requesting that [redacted] obtain or crack the passwords for targeted accounts, [redacted]

[redacted] ***As the 2020 election approaches, the IC has detected Chinese state-sponsored cyber actors targeting the former Vice President's presidential campaign, probably to gather intelligence that could enable future operations, the first instance this election cycle that we have seen them directly targeting a US presidential campaign*** China has also conducted cyber espionage against other US election-related entities, [redacted] The IC assesses that China does not currently intend to covertly interfere to try to sway the outcome of the election, although this activity could enable such operations, if Beijing made a decision to do so.

- [redacted] As of 20 May, APT31 actors had sent spear-phishing e-mails containing tracking links to the G-mail accounts of staffers associated with a presidential campaign, [redacted] On 4 June, Google announced that APT31 was targeting the campaign.
- [redacted] Google and the FBI both briefed campaign officials on the Chinese cyber operations shortly after discovering the activity. Google officials have publicly stated that the spear-phishing attempts were unsuccessful; [redacted]
- [redacted] During the past year, Chinese cyber actors have collected US election-related information from US voter databases, a polling data company, political and nonprofit organizations, fundraisers, and advisory organizations for political campaigns, [redacted]

[redacted] ***APT31's method of sending tracking links suggests that the Chinese operators are mapping out the target network for follow-on approaches, possibly including tasking campaign staffers' e-mail accounts in the Chinese military's signals intelligence system for collection.*** Tracking links collect metadata such as

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]

[redacted]

Internet activity and system information that the operators can use to exploit the accounts and identify other targets of interest.

- [redacted] Knowledge of a campaign official's operating system and software would allow cyber actors to determine whether they could quickly exploit known vulnerabilities or if they needed to develop malware to gain undetected access to the victim's machine.
- [redacted] If a target opened a spear-phishing e-mail with a tracking link—even without clicking on any links—it would confirm an active account for the cyber actors, potentially narrowing the target set for future [redacted] operations.

(U) *For additional information:*

[redacted]

(U) *Produced jointly under the auspices of the Chief of Analysis,* [redacted] *the Federal Bureau of Investigation, and the National Security Agency.*

[redacted]

[redacted]OCUMENT DETAILS

CONTENTS

Produced By: CIA **Product Type:** World Intelligence Review **Document Number:** WIRe2020-05063

Publication Date: 01 Jul 2020

Contact: [redacted] (secure), [redacted] (open)

ELECTION REPORT

EXECUTIVE SUMMARY

From around 2019 to 2024, the Cybersecurity and Infrastructure Security Agency (CISA) conducted a set of technical and operational activities to evaluate the security of certain U.S. election systems. These activities, all carried out upon the request of system owners and operators, included direct examination of election-related software; penetration testing of state, local, tribal, and territorial (SLTT) networks; and incident response operations for intrusions into elections systems. Through these activities, CISA developed a strong understanding of the vulnerabilities that, at the time of testing, affected select election-related software products and network environments evaluated by CISA. In every software product or election-related network in which CISA identified a vulnerability, CISA notified the owner or operator of the vulnerable product or network and encouraged them to mitigate the vulnerability.

CISA's findings highlight the reality that election-related software, like all complex software, contains vulnerabilities that require timely remediation. While past partnerships with election vendors enabled early identification of security weaknesses prior to product release, structural constraints in the certification ecosystem significantly limit vendors' abilities to patch systems quickly. For example, some government election systems certification regimes require that no patches be applied for months before an election. These limitations, combined with inconsistent vulnerability disclosure practices, result in election systems being deployed with known and unpatched security issues.

Beyond software quality, CISA's assessments repeatedly show that the IT networks operated by SLTT election offices lack cybersecurity hygiene. Many election vendor threat models assume strong network segmentation and isolation of election systems. However, in practice, election infrastructure is often accessible from general enterprise networks, creating opportunities for lateral movement by adversaries who compromise email systems, user workstations, or other information technology (IT) assets. Weak identity management, limited logging, and insufficient segmentation exacerbate the risk that a cyber threat actor could access or disrupt mission critical election IT components.

Overall, the security of U.S. elections is shaped by the interaction of three major factors: (1) software vulnerability management constrained by outdated certification regimes; (2) inconsistent transparency from election system vendors on vulnerabilities and patch status; and (3) the cybersecurity immaturity of many SLTT networks responsible for hosting election systems. Addressing these challenges requires coordinated action across technical, policy, and regulatory domains. This report provides detailed analysis and proposes targeted recommendations to strengthen election infrastructure security and enhance public trust in the resilience of the nation's elections infrastructure.

Introduction

From around 2019 to 2024, CISA evaluated the security posture of election entities through multiple, mutually reinforcing technical activities. These included, upon the request of relevant entities, direct source code and binary analysis of election software, protocol and interface assessments, penetration testing and red team operations against SLTT networks, and response operations for cybersecurity incidents affecting those same partners. Together, these activities provided CISA with a multilayered view of vulnerabilities across the software supply chain, deployment environments, operational workflows, and adversary targeting trends. In every case that CISA identified a vulnerability in a software product or election-related network, CISA notified the owner or operator of the vulnerable product or network and encouraged them to mitigate the vulnerability.

CISA correlated vulnerability data; adversary tactics, techniques, and procedures (TTPs); threat intelligence; configuration weaknesses; logging gaps; and systemic architectural issues across numerous assessments of SLTT entities. The agency's analysis helped identify security regressions (in which modifications to software result in the re-emergence of previously resolved issues), recurring ineffective or harmful attempts at solutions, and conditions that enabled adversaries to exfiltrate sensitive data, modify election artifacts, or degrade system availability.

The intent of this report is to draw from CISA's assessments in the 2019-2025 timeframe to present an assessment of the security of U.S. election systems—covering not just voting and registration specific software components, but also the broader enterprise environments in which they operate, to include things like email accounts and other office IT assets. The document concludes with recommendations designed to help policymakers and technical leaders meaningfully reduce systemic risk and strengthen public confidence.

Election Software Security

Direct Software Examination (Static and Dynamic Analysis)

From 2019 through 2024, CISA partnered with Idaho National Laboratory (INL) on the Critical Product Evaluation program to conduct direct technical assessments of election software, in many cases prior to the public release of such software. These assessments occurred only upon the request of the relevant software vendor and included:

- Automated and manual static source code review;
- Binary fuzzing of parsers, media handling components, and data import modules;
- Cryptographic implementation analysis (e.g., misuse of PRNGs, poor key handling);
- Interface security testing, including authentication, authorization, and API boundary validation;
- Supply chain dependency reviews, including third-party libraries, OS packages, and firmware where applicable; and
- Dynamic analysis in hardened and adversarial runtime environments.

While vendors generally viewed the program as valuable, the model created disincentives for transparent, industry standard vulnerability disclosure. Vendors benefited from private remediation prior to market release, but the downstream ecosystem—SLTT administrators, risk managers, and external researchers—did not receive clear vulnerability histories or patch transparency. The program was therefore retired in 2024 based on stakeholder feedback, and final reporting concluded in 2025.

CISA's analysis of the Critical Product Evaluation reports confirms that election software, like any complex system, contains a spectrum of vulnerabilities, including input validation bugs, insecure deserialization, insufficient logging, race conditions leading to unpredictable results, insecure crypto primitives, and privilege escalation paths. Many vulnerabilities were remediated quickly by vendors before release. However, CISA did not independently validate whether production builds deployed in SLTT environments incorporated all fixes.

Constraints on Security Updates

SLTT election officials face difficulties in applying security updates to election software in a timely manner. Most SLTT officials have minimal IT budgets and cybersecurity staff. In addition to resource constraints, some election systems are only deployed for limited periods of time in the immediate period surrounding an election. Others are deployed for longer periods but are "locked down" to prevent any changes during the months or weeks leading up to election day. In some cases, these lockdown periods are mandated by state law. Those state laws may also require that SLTT entities only deploy election software that has been certified by the Election Assistance Commission (EAC), which may also delay the application of security updates if an update postdates EAC certification. These jurisdictional differences present a fragmented certification ecosystem to election software vendors.

The following technical risks predictably arise from this complex environment:

- Vendors often cannot ship security fixes outside narrow certification cycles without jeopardizing eligibility for upcoming elections.
- Third-party components embedded in election systems (operating systems [OS], device drivers, middleware, cryptographic libraries) cannot be patched at normal modern software cadence.
- Legacy OS baselines and unsupported runtime components accumulate unpatched vulnerabilities.
- The absence of secure auto-update mechanisms prevents rapid response to zero-day threats.

In practice, these constraints produce environments where known, documented vulnerabilities persist for months or years on production election systems, increasing exposure to opportunistic and targeted threats. The election vendors' reluctance to publicly disclose vulnerabilities in certified products further limits SLTT operators' ability to make informed risk decisions, perform compensating control analysis, or adjust architectural segmentation.

National policymakers should encourage harmonization of rules applicable to patch management and certification of election systems. Such harmonization would allow SLTT election officials greater flexibility in installing security updates in a timely manner and would present a less fragmented environment for election system vendors.

Election Systems in SLTT Operating Environments

SLTT Network Security Posture

Election software is deployed into SLTT managed networks that frequently lack the defensive maturity assumed in vendor threat models. Across numerous penetration tests and red team engagements, CISA observed recurring structural weaknesses in SLTT-managed networks:

- Flat or minimally segmented networks, allowing lateral movement from standard enterprise zones (email servers, line-of-business applications) into election related environments.
- Weak identity and access management, including poor enforcement of multi-factor authentication, shared credentials, and inadequate service account hygiene.
- Lack of endpoint hardening, including outdated OS versions, insufficient event logging, and unmonitored administrative interfaces.
- Legacy remote access and file transfer pathways that remain reachable from segments that should be isolated.
- Insufficient monitoring of network traffic, preventing detection of adversary activity.[1]

In multiple cases, CISA assessors gained full network control within hours or days, demonstrating that many SLTT partners remain soft targets incapable of stopping even moderately skilled adversaries.

Most states have moved away from paperless electronic voting machines, because these systems don't provide a physical record or give voters a way to ensure their selections were recorded accurately. The replacement paper-voting systems also contain vulnerable components; in 2020, ImageCast X Ballot Marking Devices printed voters' completed ballots on paper but encoded their selections in a barcode that voters had no way to verify. A researcher showed that hackers could change the votes encoded in the barcode, without even having physical access to the machines.[2] The Office of the Director of National Intelligence (ODNI) additionally commissioned a forensic examination of Dominion Voting Systems devices used in Puerto Rico's 2024 election.[3] While CISA did review the report, the agency did not have access to those devices and was unable to perform an examination.

---

1 Cybersecurity and Infrastructure Security Agency (CISA). *Cyber Risk Summary: Election Infrastructure (EI) Subsector, October 2022–September 2023*. Published February 2024.

2 J. Alex Halderman, *Security Analysis of Georgia's ImageCast X Ballot Marking Devices: Expert Report Submitted on Behalf of Plaintiffs Donna Curling, et al., Curling v. Raffensperger, Civil Action No. 1:17-CV-2989-AT, U.S. District Court for the Northern District of Georgia, Atlanta Division*, with assistance from Drew Springall, July 1, 2021.

3 Dominion Voting Systems Democracy Suite Preliminary Vulnerability Assessment, Mojave Research for the ODNI, September 25, 2025.

Segmentation Failures Against Vendor Threat Models

Election vendor threat models typically assume that there is strong network segmentation between election systems—such as voter registration databases, electronic pollbooks, election management systems/tabulation systems, and central scanning infrastructure—from general enterprise IT environments. However, CISA assessments from 2019-2024 repeatedly showed:

- Election systems were reachable from enterprise hosts due to shared authentication domains, legacy VLAN configurations, or "temporary" exceptions that become permanent;
- Inadequate firewall rule hygiene, with over-broad allow rules and insufficient egress controls;
- Election infrastructure that is co-located on general purpose virtualization clusters that also host public facing workloads; and
- Overreliance on "airgap" assumptions that do not reflect actual connectivity (e.g., vendor support tunnels, unmonitored remote management tools, or indirect network paths).

These misalignments between theoretical and actual deployment models create exploitable pathways for adversaries capable of moving from commodity phishing based initial access to high value election assets.

The Importance of Transparency

American citizens have a right to know when the infrastructure that runs elections has been compromised, and what happened as part of the incident. By openly acknowledging incidents and describing mitigation steps, vendors and localities can show that they are proactively defending critical infrastructure rather than obscuring vulnerabilities. This transparency encourages continuous improvement, drives investment in stronger defenses, and reinforces that protecting elections is a collective national priority.

Clear and consistent disclosure strengthens accountability across the institutions responsible for safeguarding election systems. Even the perception of secrecy around cybersecurity incidents can erode trust faster than the incidents themselves. Communicating early, often, and honestly—while still protecting sensitive operational details—helps ensure that Americans maintain faith in the integrity of their elections and the resilience of the systems that support them.

Mitigation Measures

CISA recommends that SLTT election officials take the following mitigation measures:

1. Harmonize relevant patch management and certification rules for voting systems and associated IT infrastructure to allow cybersecurity changes to be made in real-time, without impacting certification.
2. Adhere to CISA's Best Practices for Securing Election Systems, at https://www.cisa.gov/news-events/news/best-practices-securing-election-systems.
3. Use human-readable paper ballots.

4. Conduct post-election manual audits of paper ballots to confirm that voting systems function as intended and to identify errors prior to certification of results.
5. Encourage election software providers to:
    a. Assign Common Vulnerabilities and Exposure (CVE) numbers for vulnerabilities in their software;
    b. Provide notice to customers if elections software source code is leaked or stolen;
    c. Report cybersecurity incidents to relevant authorities; and
    d. Include a software bill of materials (SBOM) with all products.
6. Ensure clear, consistent, and transparent documentation of all security incidents and remediation processes.

Conclusion

CISA's findings highlight that U.S. election systems are subject to the same security concerns as most other software systems: they are subject to outdated and fragmented certification regimes, insufficient vulnerability transparency, and persistent cybersecurity gaps in SLTT operating environments. These issues are not attributable to any single entity but are the result of complex interdependencies between vendors, certifiers, policymakers, and resource constrained SLTT partners.

Strengthening election-system security requires coordinated action across the entire ecosystem. SLTT election offices need sustained investment in network modernization, segmentation, identity management, and monitoring capabilities. CISA's recommended mitigation measures—including paper-based voting records, rigorous post-election manual audits, SBOM adoption, and improved incident tracking—provide a path toward measurable, near-term improvements.

From: [redacted]
To: [redacted]
Cc: [redacted]
Subject: Everyone"s favorite topic
Date: Thursday, December 23, 2021 12:52:29 PM

Classification: [redacted]

Classified By: [redacted]
Derived From: [redacted]
Declassify On: [redacted]
==========

[redacted]

Take a minute and read through this report. It cites some of the same intel and logic used in 2020 to say that these same units were NOT engaged in election influence but were instead only issue-focused, to now argue that China IS influencing the [redacted] election. The regional influence, focus on issues, etc. They literally cite as support for their argument some of the same reporting used in the mainline assessment in our minority report.

For example, they cite [redacted] activity as being "the Chinese military" even though in 2020 the IC said we didn't know who it was. *This report describes the same unit that* [redacted] *and I said were influencing the US 2020 election and now characterizes it as an election-influence unit and attributes it to the Chinese Government*. That's a weird coincidence, and one we should highlight for oversight. FBI and [redacted]

We should consider how this looks and on what logical, non-partisan basis the IC makes calls one way or the other. Why is this unit engaged in election influence in the [redacted] and [redacted] "to promote China's interests" but when they do it here it's "issue influence" but somehow not election-related? *It's the same personnel doing the same kind of activity.*

[redacted]
National Intelligence Officer - Cyber
ODNI/National Intelligence Council

Secure: [redacted]
Email: [redacted]
Unclass: [redacted]
Unclass email: [redacted]

==========
Classification: [redacted]

To: [redacted]
Cc: [redacted]
Subject: FW: ICA Comments

Classification: [redacted]

[redacted]

==========

Hi [redacted]– Forwarding these comments from FBI for your awareness. They had previously told me that Director Wray signed off on the ICA text, and the only changes since then have been downgrades of [redacted] reporting and the DNI's minor initial edits. Most of this we've been over numerous times already. So it's not clear to me if they're backtracking or just commenting for the record.

[redacted]
Director, Election Threat Analysis
National Intelligence Council/DNI Election Threat Executive
[redacted]

From: FLORIS, NIKKI L. (CD) (FBI) [redacted]
Sent: Wednesday, December 30, 2020 1:42 PM
To: [redacted]
Cc: UGORETZ TONYA FBI USA GOV [redacted]
Subject: ICA Comments --[redacted]

Classification: [redacted]

[redacted]

==========

Hi [redacted]

Couple of thoughts on the updated ICA draft, all of which center on the minority view and some of which you have previously heard from the FBI team. Generally speaking, while we are fine with the inclusion of the minority view textbox, we firmly believe the analysis in said text box must comport to the same analytic standards as the rest of the ICA. This is an absolute red line for the FBI. Additionally, we do not support the inclusion of the minority view in the KJs; without proper context and source descriptions, the minority view is given parody to the ICA assessments. Below are some more specific points:

In the first para, the NIO notes that China's leaders also "intended" some of Beijing's efforts to indirectly affect US candidates, etc. The IC has repeatedly stated, based on a body of intelligence, there is no evidence of said intention, though we note there was an awareness of this potential effect. To state this as bluntly as the NIO does, without evidence to support this claim, is extremely misleading.

In the second para, the NIO notes he gives move weight to several clandestine and liaison reports, without any sort of source description whatsoever. By minimizing the source descriptions, clandestine reporting from US or liaison sources of dubious credibility, poorly identified sourcing chains, and minimal track records of reporting is given the same weight as signals intelligence of identified senior Chinese diplomatic and intelligence figures, as well as clandestine reporting of decision making in Beijing from sources with established records of reporting that is generally reliable.

In the last tic, the NIO assesses China "may" also have encouraged protests. There is no evidence of this in the reporting, and the citations associated with this tic certainly do not support this assessment. This is highly misleading and a misrepresentation of the underlying reports.

The final para in the dissent argues that we have collection gaps on the entities that would probably execute influence operations. This point appears to acknowledge that IC collection demonstrated that China's leaders practiced restraint and did not intend to influence the outcome of the election and instead focuses on where collection gaps might miss evidence of the execution of influence ops. This shift in focus by the NIO is inconsistent with earlier portions of the dissent argumentation and argues that US collection did not find what China has actually done. As we've said before, citing the absence of evidence is an absolute red line for us.

Thanks again for all the work on this [redacted]. . . we will continue to stand by for any additional drafts, etc. On a more positive note, the Iran section edits are much improved and we greatly appreciate you working with us on this! I am out of the office tomorrow, but Cynthia is in should you need to reach anyone on the team. We will be back in full force Monday.

Have a wonderful New Year,
Nikki

DAD Nikki L. Floris
Counterintelligence Division
Open: [redacted]
NSTS: [redacted]
FBIHQ Rm [redacted]

==========
Classification: [redacted]

[redacted]

NATIONAL INTELLIGENCE COUNCIL

ASSESSMENT

19 August 2020 NICA 2020-06885D

[redacted] Foreign Threats to 2020 US Federal Elections

(U) Key Takeaways

[redacted] ***Scope Note: This is a downgraded version of a paper originally published on 19 August, 2020, and includes information current as of that date. This paper updates NICM 2020-32,*** [redacted] ***and NICM 2020-033,*** [redacted] ***which also addresses China's broader influence efforts. This paper does not make assessments about the impact of these efforts on the US. It also does not discuss efforts that the IC cannot attribute to foreign actors.***

(U) Ahead of the 2020 US elections, foreign states will continue to use covert and overt influence measures in their attempts to sway US voters' preferences and perspectives, shift US policies, increase discord in the United States, and undermine the American people's confidence in our democratic processes.

- [redacted] Foreign states or other actors may seek to compromise our election infrastructure for a range of possible purposes, such as interfering with the voting process, stealing sensitive data, or calling into question the validity of the election results. We judge that Russia, China, Iran, as well as many nonstate actors, have the capability to conduct such activities, although it would be difficult for them to manipulate voting processes at scale and without detection.

[redacted] We are primarily concerned about ongoing and potential influence activity by Russia, China, and Iran.

- [redacted] We assess that Russia is using a range of measures primarily to denigrate former Vice President Biden and what it sees as an anti-Russia establishment. For example, it is directing or encouraging proxies to spread claims about Vice President Biden. Some Kremlin-linked actors are also seeking to boost President Trump's candidacy on social media. More broadly, Moscow's efforts seek to amplify social discord in the US and undermine Washington's global standing.

- [redacted] We assess that China prefers that President Trump be defeated; in the past few months it has stepped up public rhetoric criticizing his Administration, which it recognizes may affect the election. Although [redacted] Beijing did not intend to try to affect the election, [redacted] online [redacted] influence, and collecting

(U) This assessment was prepared under the auspices of the National Intelligence Officer (NIO) for Cyber. It was drafted by the National Intelligence Council [redacted] *Questions may be directed to the NIO* [redacted]

Classified By: [redacted] | Derived From: [redacted] | Declassify On: [redacted]

[redacted]

derogatory information about US public officials

-

We also are monitoring for signs that other countries or nonstate actors such as criminal groups are acting on their preferences for the election and attempting to covertly influence public opinion, disrupt election operations, or jeopardize election data with tactics such as the use of ransomware.

(U) **Election Terminology**

(U) **Election influence** includes overt and covert influence activities of foreign governments or actors serving as agents of, or on behalf of, foreign governments intended to directly or indirectly affect a US election—including activities targeting candidates, political parties, voters or their preferences, or political processes. **Election interference** is a subset of election influence involving the technical aspects of the election, including activities targeting voter registration, casting and counting of ballots, and the reporting of results.

(U) **Russia**

-

- President Putin and senior Russian officials are overseeing efforts by proxies— —to spread claims about former Vice President Biden as well as Ukrainian politicians and alleged Ukrainian influence in the 2016 US election. These claims include that when the former Vice President was in office, he engaged in criminal activity in his dealings with Ukraine and individuals tied to Ukrainian energy firm Burisma. Derkach, Kilimnik, and other proxy actors

affiliated with the Russian Government are advancing such narratives with US officials and other prominent persons as well as online, including through personal interactions and audio and documentary film releases via US and Ukrainian media outlets.

- These figures are conspiring to intensify their efforts as the election approaches to orchestrate a high-profile corruption scandal implicating former Vice President Biden and the Democratic Party at the peak of the 2020 US presidential campaign. Their aim is to defeat the former Vice President and ensure the President's victory. Some of these proxy actors anticipate that Ukraine-themed narratives about Democratic corruption will play a decisive role in the election and that US persons are key to propagating these narratives.

Since our assessment in May, Russia continues to use state media, social media, and other online media platforms to denigrate the former Vice President, the Democratic Party, and the US political "establishment," and to promote divisions in the country. This content has largely been favorable to the President, but on occasion it criticizes his administration for policies that run counter to Russian interests.

- Russian actors have circulated narratives about voter fraud resulting from mail-in balloting and called some US primary voting processes "rigged" by the Democratic Party.

- Some Russian actors have shifted their focus from social media to on-line news sites. Since last year, the Lakhta Internet Research (LIR) troll farm, Russia's Foreign Intelligence Service (SVR), and the Main Directorate of the General Staff of the Russian Federation (GRU) have employed cadres of US and other foreign authors to create anti-American and US-focused political content on English-language news platforms, including "United World International," These groups leverage their US contacts to seed their narratives more broadly into Western media,

We continue to assess that Russia's understanding of US electoral dynamics and its assessment of who is likely to win will guide its calculus as the election approaches. Ongoing cyber operations could inform or fuel further influence efforts. For example, as of June 2020, reconnoitered multiple state and local government websites; we do not know the purpose of this effort. In July, a commercial cybersecurity company believed may have targeted a US political organization, probably unsuccessfully, though we cannot independently attribute the activity. Russia for years has targeted and collected information about current and former US Government officials, which it could leak to the public at any time.

(U) China

We assess that China prefers that the President—whom Beijing sees as unpredictable and tough on China—does not win reelection. Although Beijing did not intend to try to affect the election, online influence, and collecting derogatory information about US public officials

China uses mostly enticements and occasionally coercion to extract more pro-China positions and to punish those whom Beijing views as opposed to China's interests. It also employs disinformation and critical statements attacking the US Government's handling of the COVID-19 pandemic and other issues, such as the closure of the Houston Consulate, Hong Kong, the legal status of the South China Sea, and China's efforts to dominate the 5G market. a pro-China network of online accounts posted video content critical of President Trump before it was deactivated by social media platforms; We assess Beijing probably calculates that a concerted effort to influence the Presidential election would backfiring and offer uncertain benefit, but also recognizes critical statements might affect the race.

- a newspaper owned by the Chinese claimed that economic measures Beijing could take against supporters of legislation and lawsuits seeking compensation from China over the COVID-19 pandemic may impact US state and congressional races. This is the first time we have observed Beijing issue a public warning that suggests it is willing to impose economic costs that could affect US elections.

we judge that China will evaluate the implications of various electoral outcomes on its interests. If Beijing were to assess that the increasingly downward trajectory in US-China relations threatened China's rise and could not be dealt with using existing tools, it might attempt to more directly thwart the President's reelection, including by leaking information or through online influence network.

[redacted]

- [redacted] Beijing has expanded its cyber collection of data related to the 2020 US elections by carrying out opportunistic intrusions against US private-sector entities in efforts to collect information on US political candidates, campaigns, donors, and voter data. [redacted]

[redacted] Threats to Election Infrastructure

[redacted] We assess that hostile actors could exploit Internet-connected election infrastructure—such as voter registration databases, pollbooks, and state or local election officials' websites—because of its ease of access and comparative lack of security. These systems are designed for accessibility, commonly through web portals, making them vulnerable to a range of malicious cyber activities. A committed adversary could potentially use access to these systems to disrupt or sow doubts about our democratic election processes.

[redacted] We assess that hostile actors could also manipulate systems that count or tabulate votes—such as voting machines—on a localized basis, but it probably would be difficult to coordinate a campaign to alter voting results on a wide scale. Post-election audits and paper trails also most likely would uncover such efforts in the nearly all US states. Similarly, foreign actors would have difficulty coordinating a large scale campaign to manipulate mail-in voting, and robust postal tracking probably would detect any large-scale effort.

[redacted] Cyber operations targeting the reporting of electronic tabulation results could delay reporting but probably would not affect the integrity of certified results. Denial of service attacks would also delay public access to results.

(U) Iran

[redacted] ***Iran is conducting an influence campaign to undermine the current President and US democratic institutions, and to divide the country in advance of the 2020 elections.*** Tehran sees the current administration as promoting regime change in Iran, [redacted] a view that increases the Iranian leadership's interest in trying to prevent the President's reelection. Iran's efforts probably will focus on online covert influence, such as spreading disinformation on social media and recirculating anti-US content. [redacted]

- [redacted] Supreme Leader Khamenei probably has authorized the influence campaign. These efforts focus largely on creating or amplifying social media content that criticizes the President and recirculating existing news reports, memes, and hashtags focused on US civil unrest, domestic protests for racial justice, mail-in voting, and the administration's handling of the COVID-19 pandemic.

- [redacted]

[redacted]

- Over the past two years, social media companies have removed thousands of Iranian-origin inauthentic accounts—some with links to the Iranian Government—that have shared information critical of both the current President and other presidential candidates and that even impersonated a candidate in 2018. Tehran also uses these accounts to attempt to influence US audiences by promoting messages aligned with Iranian policies. Tehran's links to some of these efforts.

Iran could attempt to manipulate or attack election infrastructure—as it has in elections in the Middle East and South Asia—but we do not have any information indicating that it intends to do so in the United States. It could also seek to collect and publicly release damaging information.

- In January, Iranian-contract cyber actors tried to compromise a server associated with a US business involved in election infrastructure, FBI worked with the company to remediate the problem.

- In June, Google announced that Iranian-linked cyber actors had unsuccessfully attempted to spearphish email accounts associated with campaign staffers working for the US President. Iran pursues such efforts in part to acquire derogatory information it could release publicly, as well as to inform its broader aims of weakening the US and damaging its standing abroad.

(U) Other Foreign Actors

A range of other foreign actors have expressed preferences for the outcome of the election. We have reporting on a few that have either considered or taken steps to attempt to covertly influence US voters, presidential candidates, or US politics surrounding the election. For example:

- Senior **Turkish** officials, including President Erdogan, believe that segments of the US Government have an entrenched, anti-Turkey viewpoint, and as a result have sought to covertly influence US politicians' and political candidates' thinking on

Turkey. Ankara's efforts have, over the past year, included covert funding of US municipal election campaigns, unregistered lobbying efforts, and messaging on social media by state-owned outlets.

- **Criminal or other nonstate groups** also have the capability to compromise US election infrastructure. Gaining access to election-related systems could allow them to disrupt the voting process, steal sensitive data, or undermine confidence in the election results, but we do not know whether any of them have specific plans to do so. Some incidents have already occurred; in April, unidentified actors used ransomware to compromise the computers of a Virginia county administrator and vote registrar,

Other foreign actors have preferences for the outcome of the US presidential election, and in the runup to November 2020 they may express their views in statements to the press, in diplomatic channels, or privately. Most probably will make only oblique or tempered public comments to avoid the appearance of trying to shape the outcome of the election. For example:

- **German** Chancellor Merkel almost certainly would prefer that President Trump not win reelection because of personality conflicts between the two leaders and her perception that the current administration's policies have complicated Germany's, the EU's, and NATO's geopolitical positions, In public remarks in July, she implicitly criticized the President's response to the COVID-19 pandemic, and in June she cited the 2020 election as a "risk factor" for the EU during a private video call with other European leaders.

- **In mid-2019, Saudi** Crown Prince Muhammad Bin Salman expressed concern that Riyadh would lose US support for its priorities if the President were to lose the election in 2020, the President was the most Saudi-friendly of any US President,

[redacted]

NIC [redacted] NATIONAL INTELLIGENCE COUNCIL

[redacted] Efforts by Selected Countries To Manipulate US Political Landscape

[redacted] This graphic describes efforts by selected countries to attempt to manipulate aspects of the US political landscape over at least the past four years. It is not intended as a comparison of the scope, scale, or level of effort of each country's influence activity. For example, the scope and scale of China's current influence activity at the state and local far outpaces Russia's and Turkey's, and Russia has leaked intelligence-acquired information more often than Iran.

[redacted]

✖ Not observed, not aimed primarily at United States, or only symbolic ○ Preliminary or preparatory steps, with or without specific intent ✔ Observed

EFFORTS		RUSSIA	CHINA	IRAN
Public opinion *(overt)*	*Releasing press statements, state-run media content*	✔	✔	✔
Public opinion *(covert)*	*Covertly messaging on social media*	✔	✔	✔
National leaders/policy	*Covertly influencing Executive Branch or Congressional leaders' thinking or policies*	✔	✔	✔
State or local leaders/policy	*Covertly influencing state or local government leaders' thinking or policies*	✔	✔	✖
Leaking intelligence-acquired information	*Publicizing information gathered through intelligence operations to damage a US political figure or organization*	✔	○	✔
Election processes	*Targeting, accessing, or manipulating election processes or election-related systems*	✔	○	○
Legal processes	*Influencing US law enforcement investigations, prosecutions, or other aspects of the US legal process*	✔	○	✖
Economic leverage	*Offering economic inducements to secure policy concessions*	✖	✔	✖
Punitive measures	*Retaliating for US decisions or actions*	✔	✔	✖

[redacted]

NIC • 2007-00866

[redacted]

[redacted]

NATIONAL INTELLIGENCE COUNCIL

MEMORANDUM

ALTERNATIVE ANALYSIS

16 October 2020

NICM 2020-09381

[redacted] Making the Case That China Has Taken Some Steps to Influence the Presidential Election

[redacted] ***Scope Note:*** *This memorandum was prepared by the National Intelligence Officer (NIO) for Cyber and the Director, Election Threat Analysis (D/ETA). It offers an alternative perspective to the IC's assessment that China has not attempted to influence the outcome of the 2020 Presidential election. It was provided to the IC for comment before publication but is not an IC-coordinated memorandum.*

[redacted] **The NIO for Cyber and the Director for Election Threat Analysis (D/ETA) assess that Beijing has taken at least some low-level, exploratory steps to undermine the President's reelection chances by denigrating him and shaping voter perceptions. Their assessment differs from the IC's judgment that Beijing has considered but not deployed influence efforts to affect the Presidential election.**

- [redacted] **The NIO and D/ETA assess that Beijing's efforts probably have included overt messaging, nascent online covert influence capabilities, diplomatic measures, and the use of economic leverage.**
- [redacted] **They assess that these efforts probably have not included the use of Beijing's most aggressive options for influencing or interfering in the election, [redacted] because Beijing wants to minimize the risk of blowback and hopes to stabilize the relationship after the election.**
- [redacted] **The NIO and D/ETA have low-to-medium confidence in these assessments because [redacted] much of the available reporting would be consistent with either the mainline or alternative view.**

(U) IC Mainline Judgments

[redacted] The IC, including the NIO for East Asia and other NIC officers, assesses Beijing has not deployed influence efforts intended to change the outcome of the US Presidential election. [redacted] that Chinese leaders desire stability in the US-China relationship and believe they have a range of tools that can achieve their goals regardless of who wins the election. The IC also assesses [redacted] that the election of either candidate will present opportunities and challenges for China probably informs their risk calculus against influencing the election. The IC assesses that Beijing prefers to respond to US actions with restraint to show resolve and preserve the ability to repair relations after the election.

- [redacted]

(U) *This memorandum was prepared by the National Intelligence Officer (NIO) for Cyber and the Director, Election Threat Analysis. Questions may be directed to the NIO* [redacted]

Classified By: [redacted] | Derived From: [redacted] | Declassify On: [redacted]

[redacted]

- In 2019, assessed that "hostile forces" could fabricate claims that Beijing was interfering in the election to demonize China and that no matter who won the election Washington's hardline policies against Beijing were unlikely to change, Chinese noted that Beijing should avoid giving Washington any pretext to "scapegoat" China and to claim that it was interfering in the election, In 2020 also assessed, despite the President's attempts to blame China to divert attention from the pandemic and his electoral prospects, that managing tensions without causing irreparable damage to bilateral relations over the next six months remained in China's interest,

- Chinese leaders may have decided that there is little point to taking the risk of an influence effort because they believe their preferred outcome is probable. As early as this year, Chinese assessed that the pandemic and economic downturn had diminished the President's reelection prospects and since then Beijing has been planning for either electoral outcome and conducting outreach to both candidates and their campaigns,

The IC has seen no indication that Beijing is engaged in an effort to influence the outcome of the presidential election, nor has it observed activity that it assesses is likely the result of such an effort by Beijing. While we have seen Beijing develop other options that could be used to influence the election, we have not seen these capabilities deployed.

- claimed that China had not interfered with the US election and recommended that China speak and act circumspectly when faced with US assertions about Chinese and Russian interference,

- in 2019– to prevent the US President's reelection by suppressing his base,

(U) An Alternative Perspective: Indicators of Influence Efforts

The NIO and D/ETA agree with the large majority of the IC's judgments about China's calculus and approach to the election. They assess, however, that the IC's judgment that no element of the Chinese Government has taken any steps to influence the Presidential election at least through the summer. They also have less confidence than the rest of the IC that China's preparations for influence efforts were not carried out given contradictory reporting

[redacted]

[redacted] The NIO and D/ETA assess [redacted] over the summer [redacted] private sector and open source reporting on influence activities already underway suggest that the Chinese Government has been engaging in at least some level of influence targeting US voters and candidates with the knowledge that their activities could have an effect on the election outcome.

- [redacted] Beijing began taking unspecified steps around [redacted] 2020 to damage the US President's reelection campaign in response to US pressure on China's [redacted] technology sector, [redacted] planning discussions among [redacted] officials to respond to US pressure were taking place at increased frequency, and that senior leaders expected China's semiconductor industry would continue to be damaged if the US President were reelected. Unspecified Chinese Government officials [redacted] that [redacted] Chinese [redacted] expected relief from sanctions if as a result of their efforts, US resolve weakened or a candidate from a named US political party were elected instead of the President being reelected.

- [redacted] 2020, the [redacted] recommended that China collect derogatory "black materials" on the US President, [redacted] and [redacted] official which the [redacted] recommended China "sensationalize" at the appropriate time, [redacted]

[redacted]

- (U//[redacted]) **IC Terminology: Election influence** includes overt and covert influence activities of foreign governments or actors serving as agents of, or on behalf of, foreign governments intended to affect directly or indirectly a US election—including candidates, political parties, voters or their preferences, or political processes. **Election interference** is a subset of election influence targeted at the technical aspects of the election, including voter registration, casting and counting of ballots, and reporting of results.

- [redacted] The NIO and D/ETA assess that China [redacted] intend to at least indirectly affect US candidates, voters' preferences, and political processes, thus meeting the definition of election influence

[redacted]

- [redacted] the Chinese Government had tasked its missions in the US to use Chinese groups and organizations to incite protests in the US to damage the President's public standing and undermine his reelection chances, [redacted]

[redacted]

- The Chinese had assessed that racial conflict would be a large factor in the election, government-affiliated[21] Chinese technology company employees were assisting with a campaign, to covertly incite violence and protests against the US Government.[22][23]

- Chinese were experimenting with the creation of deepfakes intended to denigrate President Trump in response to directives made by to improve Beijing's ability to manipulate public opinion.[24]

During the same period, a pro-China influence network on US social media platforms posted messages supporting Beijing's views that included some English-language content denigrating the President and his Administration's policies. The activities of these networks are consistent with what we would expect to see from intelligence services or similar actors taking steps to build nascent online influence capabilities;[26] the NIO and D/ETA assess that their level of sophistication

- Although we cannot directly tie this network to the Chinese Government, the NIO and D/ETA assess that elements of the government were, at a minimum, aware of and condoned the campaign, and may have directed or conducted it. We base this assessment on the alignment of the content with Beijing's overt messaging themes, its striking similarity to the themes and tactics of previous Chinese influence campaigns that seek to blend their influence operations into broader public discourse, the duration and frequency of the activity spanning several months, the rapidity with which the network created videos in response to world events, and the network's consistent ability to operate outside China's Great Firewall.

- a US social media platform took down a separate cluster of unattributed pro-China accounts that defended a range of Chinese interests, but which also included accounts posing as Americans and posting some US election-focused content. The unidentified actors running these accounts created four groups—one favoring the President, two favoring his opponents, and one that primarily denigrated the President.[28] The accounts have since been shut down, but others could easily take their place and would be difficult to detect;

- The IC assesses that since 2018, China has been researching methods and developing new tools for using online covert influence operations to sway the perspectives of American audiences. Chinese planned a report on the potential impact their covert influence operations could have on the presidential election,

These are developments that the IC has identified as increasing the likelihood that Beijing would seek to influence the election outcome.[c]

China's Possible View of an Influence Campaign

The NIO and D/ETA assess that China may intend much of its broader messaging on issues in US-Chinese relations to also undermine the President's reelection prospects. China probably views as low-risk broad campaigns that emphasize specific issues in the US-China relationship and use a mixture of public statements, diplomatic engagement, private messaging, targeting of campaign donors, and online covert efforts to influence US officials, firms, and the public to oppose the President.[d] Beijing has authorized the conduct of increasingly aggressive overt and covert influence campaigns aimed at criticizing policies of the Administration while trying to avoid blame for interfering in a U.S. Presidential election.

- China, starting in March, launched overt and covert influence efforts to shape the global public narrative regarding Beijing's response to COVID-19 and denigrate the Administration's pandemic response, including by spreading disinformation about the pandemic's origins and publicizing English-language cartoons denigrating the President's handling of the crisis, judging from open source The NIO for Cyber and D/ETA assess that Chinese leaders believe these activities could impact the election.[45]

- In May, a newspaper owned by the Chinese Communist Party claimed that economic measures Beijing could take against supporters of legislation and lawsuits seeking compensation from China over the COVID-19 pandemic may affect US state and congressional races.[46] This was the first time the IC had observed Beijing issue a public warning that suggests it is willing to impose economic costs that could affect US elections, although in 2019 advised to gain leverage over US policy by directing unspecified resources to political swing states

- To help resolve a border dispute with India in Beijing's favor, Chinese planned to disseminate on US social media platforms content" discrediting the President,

[d] The NIO and D/ETA note that in NICM 2019-113 the IC warned that, because China probably would use the same tactics to influence the election as it already uses to influence US policy, we might not detect such a pivot.

- [redacted] Beijing over at least the past year has stepped up its efforts to influence the views and policies of candidates for US political office, [redacted] by targeting their key advisors and financial donors, [redacted] Chinese diplomats acknowledge the sensitivity of targeting donors and have sought to hide such activity from US authorities.[54]

[redacted] Tempering the assessments of the NIO and D/ETA is the fact there is no reporting to suggest that China has engaged in some of the more aggressive measures available to it to influence the US election outcome, such as funneling large donations or trying to compromise voting infrastructure[e] or interfere with mail-in ballots. There are also indications that some elements of state power, such as trade, are being used ambiguously. For example, despite trade disputes, China continues to buy agricultural products as part of the Phase One trade deal which Beijing probably assesses will help the President's reelection bid as well as help stabilize the bilateral relationship. The apparent lack of a whole-of-government campaign to favor one side [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

NIC NATIONAL INTELLIGENCE COUNCIL

[redacted] Comparing Judgments on Chinese Election Influence

[redacted] The NIO for Cyber and the Director for Election Threat Analysis assess that Beijing has taken at least some low-level, exploratory steps to try to undermine the President's reelection chances by denigrating him and shaping voter perceptions ahead of the election. Their assessment differs from the IC's consensus judgments primarily in confidence levels and on whether Beijing has deployed influence efforts to try to affect the outcome of the Presidential election.

[redacted]

✓ Yes ✗ No

China has...	IC JUDGMENT	MINORITY ASSESSMENT
...Broad influence efforts in the United States (diplomatic, business, media)	✓	✓
...Probable preference for Trump's defeat	✓ [redacted]	✓
...Considered an influence effort aimed at the Presidential election	✓	✓
...Prepared options for influence effort in Presidential election	✓	✓
...Concerns about risk versus gain in any influence effort, particularly blowback if discovered	✓ [redacted]	✓ [redacted]
...Prepared for victory by either Trump or Biden	✓	✓ [redacted]
...Avoided a whole-of-government influence effort and any interference with US election systems	✓ [redacted]	✓ [redacted]
...Intends public and diplomatic actions to undercut Trump in election	✗ [redacted]	✓ [redacted]
...Undertaken a few covert influence efforts to undermine Trump's reelection	✗	✓

[redacted]

NIC • 2010-00891

[redacted]

[redacted]

NATIONAL INTELLIGENCE COUNCIL

MEMORANDUM

15 January 2020 NICM 2020-003

[redacted] Vulnerabilities in US 2020 Election Infrastructure

(U) Key Takeaway

[redacted] ***Scope Note:*** *This memo assesses the potential impact of cyber operations against US election infrastructure for the 2020 presidential election, including the voting process and integrity of results. It does not assess adversary intentions or views of US vulnerabilities.*

[redacted] We assess that at least Russia, China, Iran, and North Korea have the capability to access and potentially manipulate data in US election-related computer systems, but we do not know whether they have specific plans to interfere with the functioning of these systems.

- [redacted] We assess that centralized election-related data repositories, such as voter registration databases, pollbooks, and official election websites, are most vulnerable to exploitation, and adversaries could use access to these systems to disrupt election processes.
- [redacted] Systems that tabulate, transmit, or display election results are vulnerable to localized exploitation but would be difficult to manipulate on a wide enough scale to alter the election outcome.
- [redacted] Adversary claims of manipulation would be difficult to disprove and could undermine public confidence in election results.

[redacted] **We judge that US adversaries, including at a minimum Russia, China, Iran, and North Korea, as well as nonstate groups, have the capability to compromise US election infrastructure for the 2020 presidential election.** Adversaries gaining access to US election-related systems could disrupt the voting process, steal sensitive data, or undermine confidence in the election results, but we do not know whether any of them have specific plans to manipulate election-related systems.

- [redacted] Russia almost certainly reconnoitered all US state election networks during the 2016 election cycle, accessed election-related infrastructure in at least two states, and exfiltrated voter data from at least one state. Russia, China, Iran, and North Korea are all capable of conducting similar operations during the 2020 election cycle, judging from their known cyber capabilities and past operations.
- [redacted] The availability of sophisticated computer network intrusion or attack tools on the dark web gives additional countries and nonstate actors the potential capability to interfere in the election. We judge that cyber criminals and hacktivists could also target election infrastructure for financial or political reasons, based on past incidents possibly or definitely attributed to such groups.

(U) *This memorandum was prepared under the auspices of the National Intelligence Officer (NIO) for Cyber.* [redacted]

[redacted]

Classified By: [redacted] | Derived From: [redacted] | Declassify On: [redacted]

[redacted]

(U) Definitions of Cyber Terms

(U/[redacted]) **Attack.** A cyber actor attempts to degrade, destroy, disrupt, manipulate, or otherwise hinder the operation of a system or network. Manipulation or deletion of data solely to hide an intrusion is not considered an attack.

(U/[redacted]) **Compromise.** A cyber actor gains unauthorized access to collect data or execute demands or installs malware linked to a malicious Internet protocol address.

(U/[redacted]) **Exploit.** A malicious actor collects data, deploys additional malware, or establishes persistent access on a compromised system. Cyber actors may compromise more accounts and systems than they exploit, in part because of the availability of tools that automate the process of compromising vulnerable systems.

(U/[redacted]) **Scan.** A cyber actor sends a system specific network traffic and observes its responses to identify security vulnerabilities. Internet scanning is very common but may have only a modest success rate, meaning cyber actors scan far more systems than they actually affect.

[redacted] Centralized Data Repositories Most Vulnerable

[redacted] **We assess that adversaries could most easily exploit centralized election-related data repositories because of their ease of access and comparative lack of security.** These systems, which are used to collect, update, and store voter information, are designed for regular access, commonly through web portals, which makes them vulnerable to a range of malicious cyber activities. A committed adversary could exploit access to these systems to disrupt election processes across the country.

- [redacted] **Voter Registration Databases.** States house their voter registration databases predominantly on Internet-connected systems that are designed for easy access because maintaining up-to-date voter registration records is a nearly continuous process. Adversaries could alter data to potentially prevent individual voters or groups of voters from voting, causing delays on election day or forcing voters to use provisional ballots. Adversaries could also use the registration data—which in some cases is also available publicly or for purchase—to tailor other interference or influence efforts.

- [redacted] **Pollbooks.** Registration databases transfer voter registration information to e-pollbook devices or paper pollbooks used to check in voters at the precinct level. Some pollbooks are tied to Internet-connected databases that adversaries probably would be able to easily exploit to manipulate data, with effects similar to those from manipulation of registration databases.

- [redacted] **State and Local Election Officials' Websites.** These sites provide public information about voting locations or, in some states, are used to report voting results. Attacks on or compromises of these sites could deter individuals from voting or cast doubt on election results.

[redacted] Vote-Administering Systems Vulnerable to Localized Exploitation

[redacted] **We assess that systems designed to tabulate votes, transmit vote amounts, or display election results probably are vulnerable to localized exploitation but would be difficult to manipulate at scale.** For example, hackers have repeatedly demonstrated that some voting machines are easy to compromise.

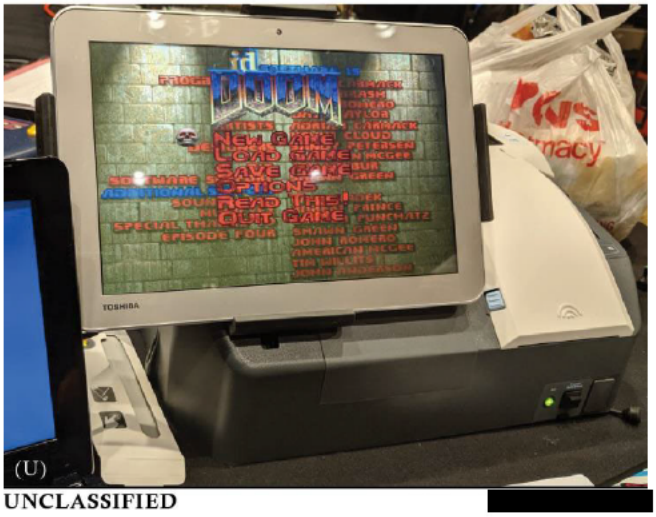
- [redacted] Direct recording electronic machines, which record and process votes digitally and store tabulation data in removable memory, are particularly vulnerable to cyber operations, especially machines with no paper backup. Such

machines, however, are used far less than other, more secure types of voting machines.

- [redacted] Adversaries who obtained physical access to voting machines could alter how they function, manipulate the data in them, or install malware, according to US state and academic investigations. At the 2019 DefCon cyber security conference, hackers demonstrated the ability to compromise more than 100 voting machines, all of which had been certified for use in at least one US voting jurisdiction.

(U) Pollbook Hacking Example

(U) A pollbook was modified at the 2019 Defcon Voting Machine Hacking Village to run the popular videogame Doom, according to press reporting.



(U)

UNCLASSIFIED [redacted]

- [redacted] Thirty-one states and the District of Columbia allow eligible voters to submit absentee ballots via Internet or fax, making these votes susceptible to disruption or manipulation. Four states allow voters to return absentee ballots via a web-based portal, seven allow some voters to return ballots via fax only, and one allows mobile voting secured with blockchain technology. Absentee votes, however, are small in number and typically closely monitored for anomalies.

[redacted] **We assess that vote tabulation systems would be difficult to manipulate on a wide enough scale to compromise election results.** The systems in each voting location are not connected to the Internet or to each other, and many methods for exploiting them rely on physical proximity. Although an adversary could manipulate voting results across multiple jurisdictions and enough states to influence a presidential election, we judge that conducting such a campaign would be difficult and that postelection audits and paper trails very likely would uncover such an effort.

- (U) A growing number of jurisdictions are using voter-verified paper backups and postelection

[redacted] Ballot and Voting Machine Preparation Vulnerabilities

(U//[redacted]) Ballot and voting machine preparation is vulnerable to cyber, supply chain, or insider threats. We judge, however, that security and mitigation measures used in these processes, and the distribution of voting machine storage facilities countrywide, would make it difficult for an adversary to coordinate a campaign to manipulate voting results across an entire state or multiple states.

- [redacted] **Ballot Preparation.** Creating paper or electronic ballots to upload to voting machines is usually outsourced to third-party vendors. Some use Internet-connected computer systems and lack password and encryption policies, which could allow malicious actors to corrupt ballot files. Logic and accuracy tests to ensure the machines function properly before election day, however, probably would detect such activity.

- [redacted] **Voting Machine Preparation.** Voting machines configured at a central location are vulnerable to insider threats. Malware introduced into the voting machines during this phase might affect multiple jurisdictions but also would be detectable during the preelection testing.

audits (now required in 38 states), which can alert election officials to manipulation or errors.

[redacted] **We assess that cyber operations targeting the electronic tabulation of results could delay results reporting from affected jurisdictions, potentially creating public uncertainty but probably not affecting the integrity of certified results.** Tabulated results are stored independently of copies displayed on results websites, although investigations of malicious activity could delay results and introduce public uncertainty about the validity of vote counts. Denial of service (DOS) attacks or manipulation of copies of the results in transit would delay public access to the results or make them difficult to access, creating the appearance of modified results.

- [redacted] The Blue Ribbon Commission on the vulnerabilities of Pennsylvania's election infrastructure found the transmission of preliminary results to public-facing websites is vulnerable to "man-in-the-middle" attacks, in which the attacker manipulates data mid-transmission. Such attacks would not alter separately stored certified copies of tabulation results, which are processed offline, but even short delays in reporting the results could introduce doubts about the security of the election or the validity of the results.

- [redacted]

- [redacted] In May 2019, unidentified cyber actors rendered a US county election website unavailable on the night of a mayoral primary; the incident did not affect the tabulation results, which were stored on a separate system not connected to the Internet.

[redacted] False Manipulation Narratives Could Undermine Public Confidence

[redacted] We assess that adversaries could also make false claims about their ability to manipulate US election infrastructure as part of a broader effort to undermine confidence in US democratic processes. Much of the voting public probably knows little about the process of administering US elections, which could allow false narratives to gain traction. Government efforts to investigate and publicly invalidate such claims could take weeks or months, providing time for concerns about election security to spread. Disproving claims would also be impossible if adversaries evaded US intelligence collection.

- [redacted] Adversaries could make wholly fabricated claims, such as announcing that they have compromised all US voting machines, a claim that would be difficult and time-consuming—or impossible—for the US Government to disprove.

- [redacted] Adversaries could also link an exaggerated claim—for example, about their ability to affect the election outcome—to actual operations, such as DOS attacks against election-related websites or intrusions into voter registration databases. Linking the two could introduce public doubts about the validity of the election, even if the actual cyber operations were unrelated to the casting, tabulating, and reporting of votes.

- [redacted] A widely publicized compromise of election infrastructure probably would undercut public confidence in the election, even if the compromise was not used to manipulate election-related data or systems.

[redacted] Mitigating Threats to Infrastructure

[redacted] We assess that enhancing the physical security and cyber protections of election systems and messaging the US public and adversaries could mitigate some of the vulnerabilities of the complex US election process. Potential measures include the following:

- [redacted] **Physical Security and Cyber Hygiene.** These terms refer to adopting best practices for the physical and cyber protection of election facilities and equipment. Basic security measures—replacing obsolete equipment, strengthening password policy and audit processes, and implementing network segmentation—might prevent less sophisticated adversaries from disrupting election processes but probably would be insufficient to deter the most advanced and determined nation-state actors.

- [redacted] **Third-Party Vendor Verification.** Establishing and refining screening procedures for vendors who manufacture or transship election infrastructure could reveal shared vulnerabilities or insider threats.

- [redacted] **Public Messaging and Education.** Public messaging would be vital to providing accurate and timely information about the effects and limited scope of low-impact cyber operations. Partnerships with state and local election officials, cyber security firms, and the media could help minimize commercial disruptions, as well as counter cyber-enabled information operations. Timely public messaging before the election would help to educate the public about adversary goals and make US officials the trusted source for information about the integrity of the election process, recovery efforts, and investigations into attempted cyber attacks.

- [redacted] **Messaging to Adversaries.** Privately messaging adversaries to emphasize that attempts to manipulate US election infrastructure are unacceptable and would have serious consequences could deter them from taking such steps.