OSET INSTITUTE

Position Paper | December 2020

Analysis of Recent Navid Keshavarz-Nia Affidavit

A Fact Check

1. Context

This is an analysis, requested by several, of the technical veracity of Navid Keshavarz-Nia's November 25th 2020 Michigan federal lawsuit affidavit (Civil Case No. 20-13134).[1] While the lawsuit seeking to overturn the state's election results failed in a ruling[2] on December 7th, the case could be appealed and therefore, the substance of the affidavit will likely remain at issue—at least in the court of public opinion. Therefore, this analysis remains meaningful, relevant, and timely.

In sum and substance, the affiant asserts his "belief" that adversaries conducted a successful cyber operation on at least one election office's Microsoft® Windows® personal computer system running the Election Management Software (EMS) component of a Dominion Voting System's product, and used the resulting access to the EMS's data to modify that data, and furthermore, to do so in a way that created a false election result. While plenty of media has given attention to this lawsuit and its associated affidavits, we focus our analysis on the technical issues of the Keshavarz-Nia affidavit, due to the affiant's reference to comments from OSET Institute leadership in said affidavit.

Generally, the affiant's claim is barely credible in terms of possibility; possibility is *not* fact; that is, that a cyber attack *actually* occurred, or that it succeeded in falsifying election results.[3] Recently, fifty-nine computer scientists and engineers and cybersecurity experts wrote an open letter on these matters that our leadership fully endorsed. An important point was made in that letter:

> *"Anyone asserting that a U.S. election was 'rigged' is making an extraordinary claim, one that must be supported by persuasive and verifiable evidence. Merely citing the existence of technical flaws does not establish that an attack occurred; much less that it altered an election outcome. It is simply speculation."*[4]

---

1 https://www.courtlistener.com/recap/gov.uscourts.mied.350905/gov.uscourts.mied.350905.1.19.pdf

2 https://www.courtlistener.com/recap/gov.uscourts.mied.350905/gov.uscourts.mied.350905.62.0_3.pdf

3 There are many well-known security vulnerabilities of the Microsoft Windows operating system as well as of features of voting system products that were *not* designed for defense against national state adversaries.

4 See: https://www.nytimes.com/2020/11/16/business/election-security-letter-trump.html

If such an "election result falsification" occurred in the manner alleged, the incident would not only be a major national security incident, but also an attack on the integrity of U.S. elections writ large.

Determining the truth or falsehood of the claimed cyber-attack would be a complex undertaking. However, much simpler methods are available to determine whether the publicly stated election results are true results from counting paper ballots. The ballots themselves can be consulted to determine the true election results, either by a risk-limiting audit with manual inspection of a statistically sound sample of the ballots, or by way of a manual inspection of all of the ballots.

If such an inspection concluded that the publicly stated election results are the true result from the ballots, then the issue of the alleged cyber-attack becomes moot, with respect to the integrity of the recent election's results: whether or not a cyber attack occurred, the election results would be known to be true.

In that case, the alleged cyber-attack would remain a very important allegation to investigate, as a matter of national security, of the cyber security of our election critical infrastructure, and of international policy where a true cyber-attack—regardless of the lack of practical consequences—must be understood for appropriate counter measures to be undertaken.

If the publicly stated result is found to be the true result, then investigation of the cyber-attack allegations can be undertaken through normal channels, with no further connection to the integrity of the elections' results.

If the publicly stated result does *not* match the actual ballots, then investigation is required *both* on the cyber-security front and into the detailed records of the elections' operations, where erroneous results could have been created from any of several causes from human error, to insider abuse, to nation state adversaries' cyber operations.

The main purpose of routinely performing post-election audits is to insist on evidence-based elections. In the absence of evidence of malfeasance, we must avoid giving credence to unproven theories that could undermine confidence in U.S. elections, to the benefit of our adversaries who use disinformation techniques to attack our national unity and sovereignty.

2. Executive Summary

The affiant offers only opinion to support his beliefs. Several of the points simply restate public knowledge about voting system technology security vulnerabilities that, by their existence alone, do *not* indicate the occurrence of a successful cyber operation that a) compromised election management systems (EMS) and b) also created a false election result. The litany of eleven statements in point #15 incorporates a variety of claims of

misbehavior, none of which appear to involve a cyber operation against a Dominion Voting Systems EMS ("Democracy Suite" or other).

The affiant is mistaken on a number of matters of fact (notably on the Philadelphia incident that did *not* involve Dominion products or services at all) that are restated as essential points of his conclusions. Despite his assertions of credentials and education in point #2, affiant also appears to lack basic understanding of:

- Cryptography;
- Standard IT practices in data backup, archive, and recovery;
- Internet Protocol (IP) network traffic recording (logging);
- Public information about the Dominion Voting Systems EMS product;
- Absentee ballot validation processes and anonymity of counted ballots; and
- Legal requirements on the election officials' duties in locally administering elections that combined local, state, and Federal contests.

In addition to the basic claim of belief in a cyber operation, affiant also makes broad and unsubstantiated claims of malfeasance by election officials (point #15, item "k"), as well as unspecific election fraud crimes in addition to the cyber-crimes of the believed cyber-operation on the Dominion Voting Systems (hereinafter "DVS") EMS, both claimed to have occurred in every "battleground" state, without specifying the states in which the election fraud occurred.

3. Point-by-Point Analysis

Points 1—3. These are personal assertions about credentials and experience.

The only, perhaps threshold issue here is that the affiant's claimed credential from the correspondence university, CalSouthern University: a "Ph.D. in Management of Engineering and Technology" is a degree not offered by CalSouthern University.

Point 4. Reference to pre-existing unsubstantiated theories of "Hammer and Scorecard" that have been repudiated by DHS CISA and debunked by several fact checking sites.

This is an irrelevant point regardless of its mendacity. Whether or not "Hammer and Scorecard" exists, there are *other* publicly attested methods to attack the Windows operating system on which that DVS EMS operates. Indeed, the affiant refers to numerous of publicly attested "reference attacks" starting in point #10 and later. There is ample record of attackable vulnerabilities—although *not* the use of them in any actual cyber operation against election systems—regardless of the existence of so-called Hammer and Scorecard tools. The affiant's use of unsubstantiated theories, unnecessary to support his beliefs, undermines the affiant's credibility.

Point 5. Personal Assertions/Claims

Point 6. Affiant references a "covert backdoor" that is in fact an overt feature for remote-access software support, described on page 33 of "2.02 Democracy Suite System Overview, Version: 5:.11-CO::7" published for public access on the web site of the Colorado Secretary of State.

It is well known that abuse of remote-access capability can result in unauthorized access to the Windows OS and hence *any* application software (including, but not limited to, DVS EMS). "Discovery" of this documented feature is unnecessary to support a claim of the *possibility*—although not an *actual* cyber-operation—of remote access as a vector for cyber attack. Affiant's claim to have "discovered" remote access, and mischaracterizing it in a way that is not required and unnecessary to support his beliefs, undermines the affiant's credibility.

Point 6. Affiant references as a backdoor for "illicit activities" a DVS EMS feature that is publicly documented in the document he references.

Using a public document to support a claim of a cover backdoor, when the capability being described is really a product feature, undermines the affiant's credibility.

The product feature in question is described on pages 42 and 43 of "2.02 Democracy Suite System Overview, Version: 5:.11-CO::7" and is for the addition of votes—a required product feature for the data entry of votes that are counted manually, and required to be added in order to complete the vote totals.

The manual count of ballots (typically a very small portion of total ballots) is permitted in several states, and indeed required in at least one, New Hampshire, where manual count is prescribed for the ballots of military/overseas voters ("UOCAVA voters") using the Federal Write-In Absentee Ballot. The affiant's claimed "*shifting … deleting … adding votes*" is required for manual data entry of votes, including editing the data entry of those (shifting, deleting) in the case of operator data entry error. In fact, it would be a poor product feature to allow the addition of manually collected votes by an operator, but *not* allow the operator to undo or correct erroneous data entry.

The claim that such data entry "*can take place through the Internet*" is predictable, considering that DVS EMS runs on an ordinary Windows PC that could be connected to the Internet and accessed via remote-access capability. Although such remote access is theoretically possible, it is also against standard election security practices, and in some states (including California) election law forbids the connection of voting system components to a network. To point out a technical possibility—but not present any specific actual abuse of remote-access—without the knowledge of typical election security practices, again undermines the affiant's credibility.

Credibility is further undermined by the entirely counterfactual claim that Internet activity can occur "*without a trace*" when in fact network monitoring tools routinely record Internet Protocol data. A technology professional, with the credentials and experience claimed in personal statements #1, #2, #3, and #5 would absolutely be aware of and understand this basic fact of IP networking, which indicates that affiant either lacks those claimed capabilities, or is ignorant of basic networking knowledge, or is mendaciously omitting basic facts as they negate the scenario the affiant is attempting to portray.

Point 7. Affiant makes allegations about Scytl SOE and data transfers.

The Scytl SOE product is *not* a voting system product, but an unofficial elections results reporting product that consumes vote-tally data from any voting system product (including but not limited to DVS) and publishes the data in human consumable form, for public online reporting of *unofficial* election results.

There is nothing remarkable about the transfer of DVS data to an election result reporting system, nor about the reporting system duplicating the results data in a disaster recovery center. The affiant's belief that 2020 data was transferred to Frankfurt, is irrelevant to fact that unofficial election results reporting data backup is routine. Affiant's unawareness of election results reporting practices, and standard data backup practices, undermines his credibility and highlights unawareness of election operations and IT operations, despite the capabilities made in the personal statement points #1, #2, #3, and #5.

Point 8. This is a recitation of older and debunked conspiracy theories, coupled with the addition of "intelligence reports indicate…" that is otherwise unsubstantiated.

The affiant's reference to supposed intelligence data that would be classified if it existed, suggests either that the claim is false or that affiant is disclosing classified information, again undermining his credibility. In addition, DVS has stated it has no ties to any foreign government.

Point 9. This is an inaccurate recitation of the evolving history of the corporate structure of Dominion, coupled with a belief that the corporate structure was created to impede "investigators" without stating the topic of investigation or the organization performing the investigation.

In fact, Dominion disclosed its then *current* corporate structure (which does *not* include Smartmatic) in 2017 in response to inquiries by the Senator Wyden in a series of written question-and-answer that started on 31 October 2017.[5] The affiant's reliance on an

[5] https://www.wyden.senate.gov/news/press-releases/wyden-questions-voting-machine-manufacturers-on-security-measures

undisclosed source (i.e., "Reports show…"), and ignorance of public statements, further undermine the affiant's credibility.

Point 10. This is another statement of public fact about a certain type of voting system vulnerability that does *not* indicate the actual use of the vulnerability in a cyber attack.

Point 11. This is another statement of public fact about a certain voting system vulnerability that does *not* indicate the actual use of the vulnerability in a cyber attack.

Notably, affiant seems unaware that the systems tested at DEFCON 2019 did *not* include the DVS EMS—which is the system that affiant believes was the target of a successful cyber operation. We observe that the DEFCON test results on non-EMS systems is both irrelevant to a recitation of DVS EMS vulnerability, and unnecessary, since the EMS runs on an ordinary Windows PC with well known vulnerabilities.

Point 12. This is about the Philadelphia USB memory hardware theft and misuses OSET Institute leadership comments in an Associated Press interview.

Leaving aside affiant's speculation about the contents of the stolen equipment, affiant's belief (i.e., that contents facilitated EMS remote access) displays complete ignorance of a) how EMS remote access is performed via industry standard remote-access authentication; and b) the fact that possession of cryptographic keys from USB devices is not required, as affiant should know from reading the DVS documentation the he references. Affiant's credibility is further undermined by these facts:

- The Philadelphia incident took place in October 2020, *not* 2019.
- The Philadelphia incident did *not* involve Dominion Voting Systems; it involved ES&S.
- According to ES&S, the USB devices use multiple levels of encryption and are "married" to single voting machines during programming. ES&S further stated that they immediately cut the devices off from the vendor's network upon learning of the theft.
- Affiant's claims (to have analyzed the "contents" of various voting systems' cryptographic keys) indicate a basic lack of understanding of cryptography: cryptographic keys do not have "contents," but are simply randomly generated numbers. (This assertion alone disqualifies the credibility of the affiant writ-large.)

In addition, examination of the OSET Institute's Edward Perez's full remarks[6] indicates that affiant misconstrued those remarks as being connected in any way to EMS remote access.

[6] https://apnews.com/article/voting-machines-voting-custodio-elections-philadelphia-f8a6453dc9e211ef20e9412d003511b1

Point 13. This is another statement of public fact about voting system vulnerability that does *not* indicate the actual use of the vulnerability in a cyber attack.

Congressional members expressing concern over DEFCON testers' finding, is both not remarkable, and in no way suggests that an *actual* cyber operation occurred.

Point 14. Affiants' claim to have an expert opinion about voting system technology is not supported by a claim about "the combination of DVS, Scytl/SOE Software/eClarity and Smartmatic."

In fact, these systems are *not* used in combination at all in the United States. In the U.S., Smartmatic voting system technology is used by Los Angeles County, which does *not* use Dominion products; and SOE results reporting software is used to present the *data* from voting systems, but does *not* directly connect to those voting systems (Dominion or otherwise). Affiant claims to have conducted "more than a dozen experiments combined with analyzing the 2020 Election data sets" but offered no published results of his findings.

Point 15. This is a remarkable conclusion that "anomalies are caused by fraudulent manipulation of the results" rather than a statement of belief or an assertion of fact supported by evidence. Affiant clearly states that he had not been granted access to examine any of the systems used in the 2020 Election, so how can he *reliably* report that a fraud occurred without any empirical evidence from the machines.

Point 15a-c. This concerns analysis of The New York Times datasets and the public data on which it is based.

Professional journalists, statisticians, and academics performed this analysis. Affiant's beliefs stated in points #15a and #15b of "unusual" or "not … normal" behavior does not appear to be based on the expertise of professional journalists, statisticians, academics, and election professionals. In addition, he offers no evidence that software developed by Smartmatic was implemented in DVS machines.

Point 15d. This assertion concerns "Reported evidence" that is not cited.

It is a counterfactual statement that ballots have signatures; combined by illogic to a conclusion (neither belief nor an assertion of fact supported by evidence) of malicious tampering with DVS configuration data.

Point 15e. This concerns a counterfactual claim that absentee ballot verification is done by the DVS ImageCast.

In reality, it is elections office staff that verify the identity and eligibility of the voter of each absentee ballot, to determine whether it should be counted. Affiant's assertion combined by the same illogic to conclude that "the only way" that the claimed (not cited)

malfunction could occur is via fraudulent manipulation of configuration data. In fact, November 2020 election experience includes instances (notably in Antrim County) of *accidental use* of incorrect versions of configuration data creating malfunctions that were *detected and corrected*.

Point 15f. This is a repeat of affiant's error in point #12 about the Philadelphia incident.

This is a repeat of the misunderstanding of the nature of cryptographic keys, both coupled to a broad claim (neither a belief nor a claim supported by evidence) that the Philadelphia ES&S (not Dominion) key data could be used for "massive attacks on all battleground state" without any explanation of what form that attack might have taken.

ES&S keys would not work in DVS devices and general practice in cryptographic systems is to use different keys for every device used in an election.

Point 15g-h. Affiant's understanding of data variance, and opinions of "not normal" are not matched by the scrutiny of this highly visible public data by professional journalists, statisticians, academics, and election professionals.

Also note that there is no "Edison County" in Michigan or any other state in the U.S., which completely undermines affiant's assertions.

Point 15i. This is a combination of uncontroversial facts about PC hardware supply chains, coupled with what appears to be a disclosure of intelligence information yielding a conclusion (not belief nor claim supported by evidence) that "China's espionage activities" were involved the cyber operation that the affiant believes occurred.

Point 15j. This is an assertion of covert operations that repeats affiant's misunderstanding of election results reporting systems in point #7.

The assertions also display a complete misunderstanding of how Man-in-the-Middle (MITM) attacks are carried out and the circumstances that must be present for these attacks to work.

Point 15k. This is a broad and unsubstantiated claim of widespread malfeasance by local elections officials in not performing validation and record keeping function that are legally required of them.

Overall, the several parts of point #15 (a-k) in toto, assert nothing about the affiant's primary claim of a cyber operation on DVS EMS systems. Rather point #15 appears to be a recitation of a variety of unrelated theories that attempt to distract from the absence of any details whatsoever of a successful cyber operation against a DVS EMS that the affiant believes occurred.

Moreover, recounts and audits have been conducted in several states that substantiate that election officials kept adequate records and that the counts were not significantly different from those reported immediately after the election.

Point 16. This is a restatement of several factually incorrect assertions in earlier points.

Affiant repeats:

- A previous a factual error about lost cryptographic keys and their relevance; and
- A repeat of the counterfactual claimed combination of DVS, Scytl, SOE, and Smartmatic.

The affiant concludes that these created the conditions for fraud, without stating who committed what fraud. At the outset of this affidavit, affiant states a *personal belief* in a cyber operation on the DVS EMS to alter vote totals. In this first of two concluding statements, affiant is additionally leveling an allegation of election fraud by parties unstated.

Point 17. This is a restatement of an initial statement of belief regarding alteration of vote totals absent sufficient specificity to establish credibility.

This is a second conclusion that is simply a restatement of initial belief of alteration of vote totals by a believed cyber operation that exploited the vulnerabilities that affiant recited earlier; and again without any specific claim of what specific systems were targeted "in all battleground states," or any identification of the "operators."

In summary, points #16 and #17 appear to indicate affiant both:

1. Believes that unknown or undisclosed operators successfully breached every election management system (EMS) in every "battleground state" by remote access means across the Internet to alter vote totals and change the presidential election result, and
2. Believes that in addition to the criminality of that cyber operation itself, people unknown or undisclosed committed unspecified election fraud.

Further, affiant's beliefs include states in which the EMS is *not* connected to the Internet, states in which manual inspection of paper ballots confirmed the machine counts, and states in which rigorous state-level pre-certification "canvass" process exists precisely to uncover: the malfeasance claimed in point #15k, election fraud broadly alleged in point #16, and voting system technology malfunction alleged in several places in this affidavit.

Notwithstanding: a) rehashing old news from a prior DEFCON computer security conference; b) similar voting system analyses done earlier, elsewhere on different machinery; and c) restating well-known concerns about cyber-attack potential and potential election compromise from the same, the affiant's claims appear entirely without merit.

In summary, the claims of "Navid Keshavarz-Nia" makes in his November 25th written legal declaration (Affidavit) lack any direct evidence, are based on speculation (his "beliefs"), and demonstrate a lack of understanding of cybersecurity, cryptography, and election administration processes. This is the OSET Institute's professional analysis based on the authors' *combined total* of 96 years of direct experience in computer and network information security; election administration technology architecture, engineering and deployment; and national digital security.

E. John Sebes
Chief Technology Officer, OSET Institute, Inc.[7]

Edward P. Perez
Global Director, Technology & Standards, OSET Institute, Inc.[8]

William P. Crowell
Strategic Board Advisor, National Security Matters, OSET Institute, Inc.[9]

7 See: https://www.osetfoundation.org/about-us#sebesbio

8 See: https://www.osetfoundation.org/eddie-perez

9 See: https://www.alsop-louie.com/team/bill-crowell/