The Report in Plain Language

What it actually claims

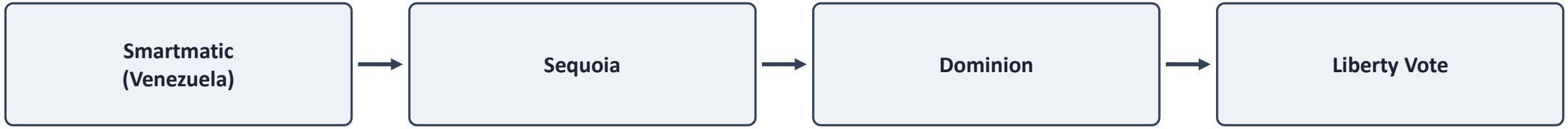
The whole report, in one sentence

The same people and software that ran Venezuela's elections quietly run parts of U.S. elections — and can reach in and change results without the official checks seeing it.

Everything else in the report is an attempt to support that one sentence.

Same people, new names

A small group of engineers built Venezuela's voting system. The report says they carried it — and themselves — into one U.S. election company after another.

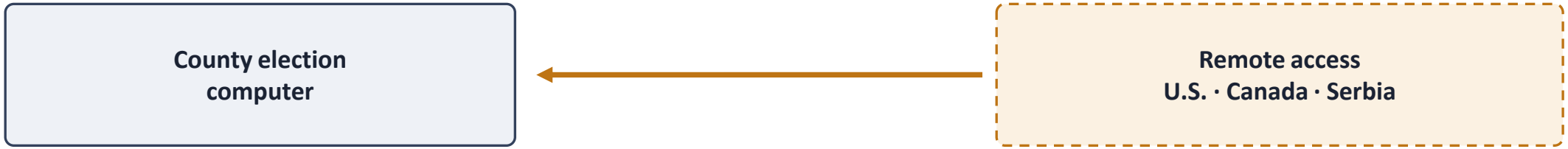


the report says: the same core engineers, the whole way across

In plain terms: if you don't know it's the same group each time, you won't ask the hard questions.

Reaching in from far away

The report says these engineers built a way to reach county election computers remotely — and that the connection links the U.S., Canada, and Serbia.



In plain terms: if someone can reach the system from far away — through a VPN or a "virtual machine" — they can potentially touch the results.

The hidden first computer

What’s supposed to happen

Results go straight into the official counting computer, and that’s what gets reported.

What the report claims

Results pass through a hidden computer first — where they could be changed — before reaching the official one.

In plain terms: the official computer only ever sees the finished numbers — not what happened on the hidden one.

The alarm watches the wrong box

The government’s security alarm — the “Albert sensor” — watches the official computer. The report says the action happens on the hidden one the alarm never sees.

> Think of a camera at the front door: it can spot a known intruder walking in, but it can’t see what happens in a back room it isn’t pointed at.

In plain terms: so “the alarm saw nothing” doesn’t cover the computer where the report says the changes are made.

What sees a hidden virtual machine (VM) — and what doesn't

The Albert sensor

watches the network wire

A VM's traffic rides a virtual switch inside the host — it never crosses the physical tap Albert sits on. An out-of-band link (cellular) bypasses it too.

BLIND

A forensic disk image

reads the drive

The VM lives on the disk: the hypervisor, a signature-identifiable virtual disk, its config and logs. Mount it and the whole guest OS is right there to read.

CATCHES IT

An engineer's laptop

nobody images it

VMs are normal on a developer's laptop — no certified baseline, no forensic review. Hidden by default, not because it's clever, but because no one looks.

NOT EXAMINED

In plain terms: a hidden VM can beat the live network alarm and an unaudited laptop — but not a forensic image of the machine it runs on. That is the one place it can be caught.

Election night 2020, in Chicago

The report points to internal Dominion emails from election night — loading, cloning, splitting, and exporting result files — and reads them as evidence of manipulation.

Establishing as fact requires the cooperation of the Secretary of State, and no Democrat Secretary of State will agree.

The man at the center: Eric Coomer

The report's case against him: under oath, Coomer denied having the access or technical ability to affect an election — then, it says, described his own virtual machines.

His own admissions

- "Multiple virtual machines" on his laptop during the 2020 election
- A March 2020 email asking for "a final VM I can at least download"
- Morales may have given him one during the 2020 Chicago primary

DOCUMENTED

the report's conclusion →

The report's conclusion

Those virtual machines ran inside the county election servers and reshaped the results — before the monitored system ever saw them.

INFERRED

In plain terms: Coomer's own words put the virtual machines in his hands. That they changed votes from inside the servers is the report's inference — not something he admitted.

Who really owns it

The report says the Venezuelan government secretly held a stake in the company behind the voting software — and hid it from the U.S. regulators who screen foreign ownership.

In plain terms: the implication the report draws: a foreign government had a hand in the company behind U.S. voting machines.

Made in China, patched in Serbia

The report says the machines' parts are made in China, their firmware is loaded in China and modified by Serbian engineers, and Dominion's CEO played down the Chinese role to Congress.

In plain terms: the worry it raises: foreign-made and foreign-updated equipment running U.S. elections.

The evidence is locked up — and the ask

The report says the real proof sits in sealed court records from Dominion's lawsuits, and that only the Justice Department can unlock it. On that basis, it asks the President to:

- Investigate the named people and companies.
- Seize and forensically image the election systems before they are wiped or updated.
- Fix the monitoring blind spot — cover the hidden computer, not just the official one.
- Obtain the sealed court records in full.

How to weigh all this

Everything in this deck is what the report claims. As you read it:

- Many of its claims rest on selected exhibits and on sources with their own disputes.
- A documented weakness — “this could happen” — is not the same as a proven act — “this did happen.”
- The strongest part is narrow and honest: the official checks have real limits in what they cover.
- Between "could" and "did" is where the public record ends and the sealed court files begin, which is exactly why the report asks for them to be unsealed..

Understanding the claim is the first step. Seeing the real evidence from sealed court documents is the next.

Source: This presentation summarizes claims from the reports presented by Joe Oltmann. The claims described are allegations and have not been independently verified.