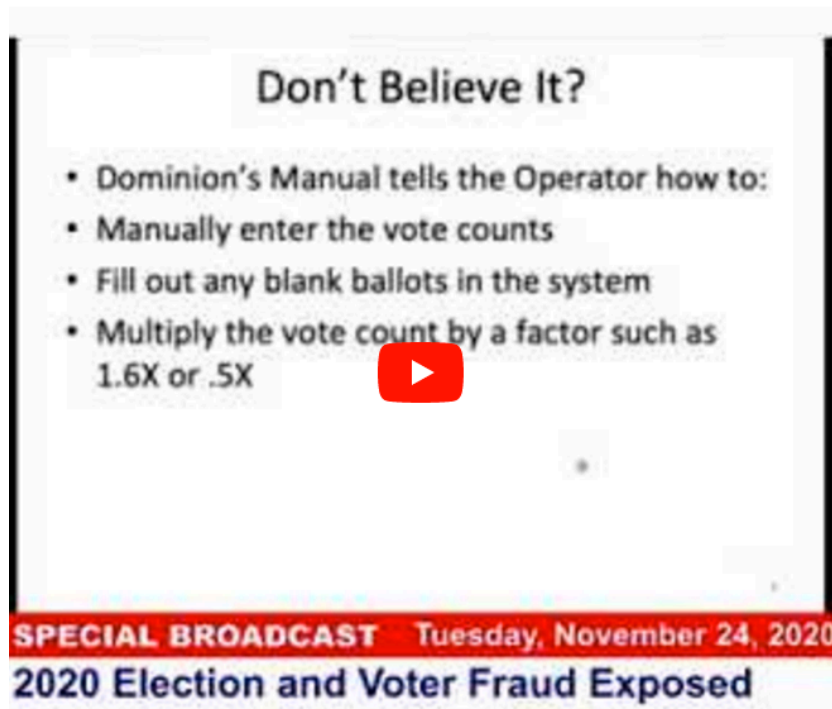


Election fraud in-depth data analysis: Russell Ramsland, Co-founder of Allied Security Operations.

78 views • 25 Nov 2020

<https://www.youtube.com/watch?v=sVGSr15ySQs>

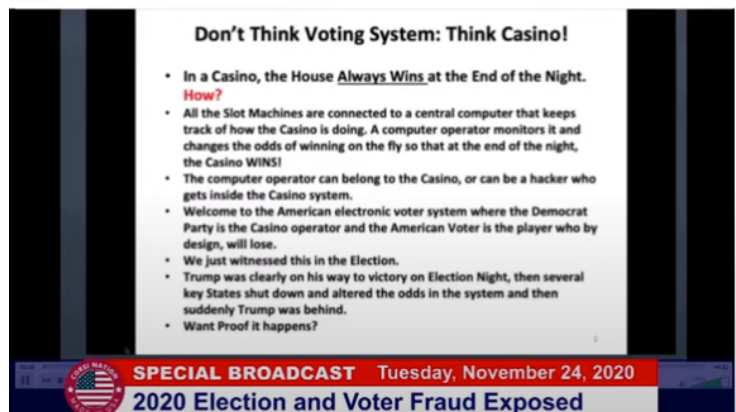


Don't Believe It?

- Dominion's Manual tells the Operator how to:
- Manually enter the vote counts
- Fill out any blank ballots in the system
- Multiply the vote count by a factor such as 1.6X or .5X

SPECIAL BROADCAST Tuesday, November 24, 2020
2020 Election and Voter Fraud Exposed

This is a YouTube video player thumbnail. It features a white background with a black border. At the top, the text "Don't Believe It?" is centered. Below it is a bulleted list of four items. A red play button icon is overlaid on the list. At the bottom, there is a red banner with white text and a blue banner with white text.



Don't Think Voting System: Think Casino!

- In a Casino, the House Always Wins at the End of the Night.
How?
- All the Slot Machines are connected to a central computer that keeps track of how the Casino is doing. A computer operator monitors it and changes the odds of winning on the fly so that at the end of the night, the Casino WINS!
- The computer operator can belong to the Casino, or can be a hacker who gets inside the Casino system.
- Welcome to the American electronic voter system where the Democrat Party is the Casino operator and the American Voter is the player who by design, will lose.
- We just witnessed this in the Election.
- Trump was clearly on his way to victory on Election Night, then several key States shut down and altered the odds in the system and then suddenly Trump was behind.
- Want Proof it happens?

SPECIAL BROADCAST Tuesday, November 24, 2020
2020 Election and Voter Fraud Exposed

This is a YouTube video player thumbnail. It features a white background with a black border. At the top, the text "Don't Think Voting System: Think Casino!" is centered. Below it is a bulleted list of seven items. At the bottom, there is a red banner with white text and a blue banner with white text. A small circular logo is visible in the bottom left corner.

Very High Level View of Voting System, Networks and Attack Entry Points
There are no security standards, it's easy to change votes with no audit trail at all

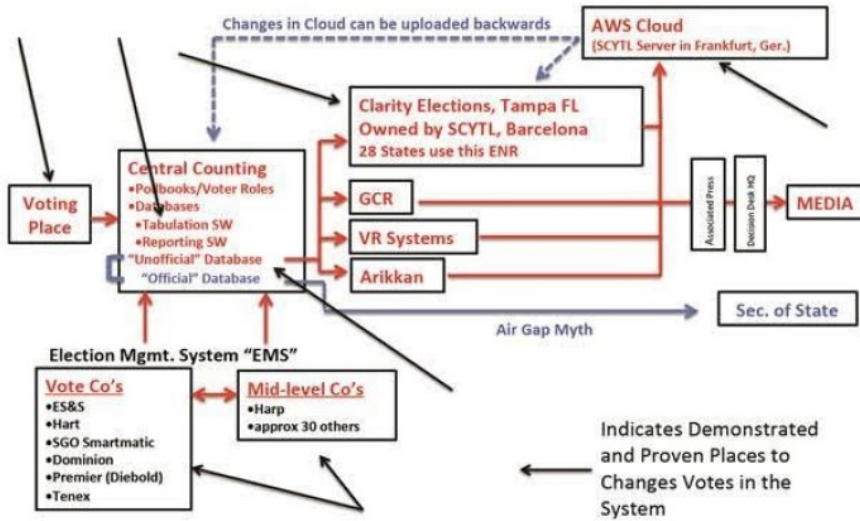


Abbildung 3

Computer Voting Has to Go

<https://fcpp.org/2020/12/19/computer-voting-has-to-go/>

..... Some voting machines could be disabled in ten seconds just by tilting them, and its memory cards replaced with new information. Malware was another possibility. "It is not a high level of sophistication to compromise these systems," the panelists reported.

... Russell Ramsland, co-owner of Allied Security Operations Group (ASOG), reported in a YouTube interview that one of his team hacked into a polling station using a cell phone in just three minutes. He could hardly believe the blatant and numerous proofs of vote manipulation in Dallas County during the 2018 midterm election.

Ramsland's team found that most of the problems identified by Coherent Cyber had never been rectified. They also reported at least 12 "entry points where votes can and are being switched and the audit trails changed or erased so that a forensic investigation finds no trace. It has to be caught in real time. Even the operator of the election system can change votes undetected."

Es folgt Abbildung 3

ASOG looked at six companies that accounted for 92 per cent of the computer voting market, including ES&S, Tenex, SGO/Smartmatic, **Dominion Voting Systems**, Hart, and Demtech. In all cases,

- the admin names and passwords for critical files were "in the open" with no hacking necessary.
- Voter registration lists that included private information were also available.

Ramsland said the voting companies used a similar source code structure. Their software was so porous that

- operators and outside players could change votes "utterly undetected."
- Any candidate could be made to win or lose by directly altering votes at the server or database level.
- An audit trail was non-existent for Hart, but was erasable or changeable with ES&S or Dominion so that no evidence of vote changing could be found

In 2017, Coherent Cyber conducted a security audit assessment of the Elections Systems and Software electronic voting system used in California. Electionware servers and clients were missing many critical or important operating system patches and had 176 Security Content Automation Protocol (SCAP) misconfigurations.

Election Systems and Software (ES&S) EVS 5.2.1.0 electronic voting system – Security Audit

2017

from the Executive Summary

.... An analyst was able to make a copy of the DS200 Electionware software, decompile all binaries into human - readable code, introduce a Proof - of - Exploitation code, recompile the source and introduce the modified version of the software back into the system. This code was, in fact, run without evidence of any tampering and cleared all cast votes once the "Close Poll" button was pushed.

Version: 11.1.2021
[Adresse](#) dieser Seite
[Home](#)
[Joachim Gruber](#)