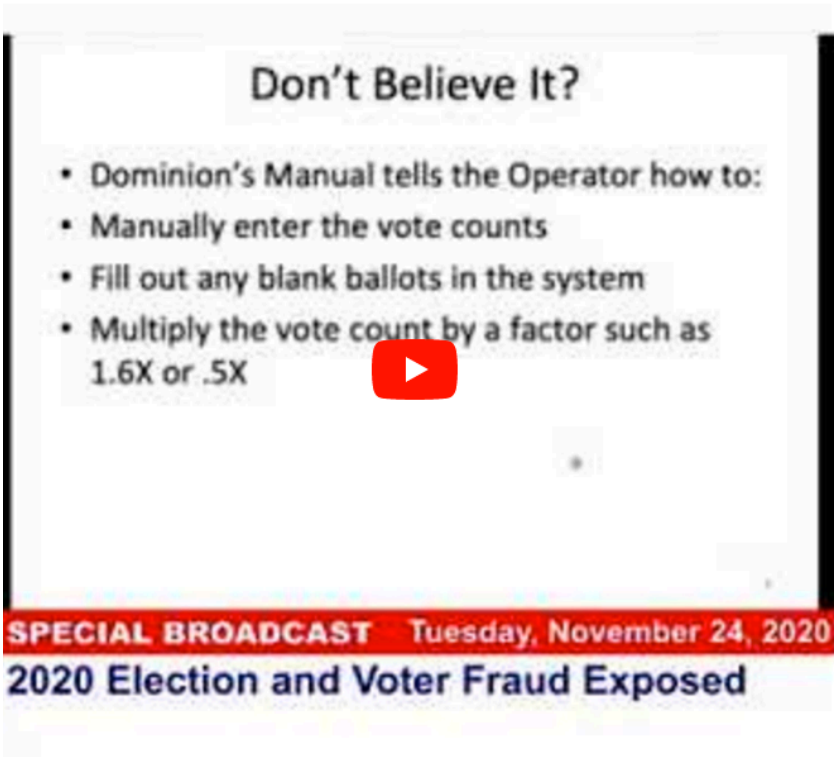
Election fraud in-depth data analysis: Russell Ramsland, Co-founder of Allied Security Operations.
78 views•25 Nov 2020
https://www.youtube.com/watch?v=sVGSr15ySOs



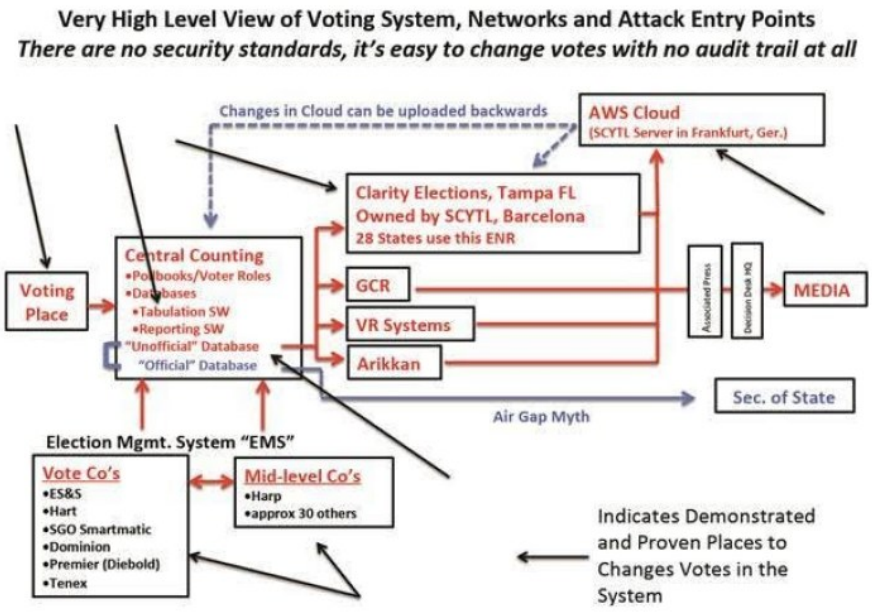


Abbildung 3

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