Technical Critique of Election Hacking Claims

From a technical perspective, the letter presents several flawed assumptions about the operation and security of U.S. election systems. Here are the key points:

1. Voting Machines Do Not Actively Network During Elections

A central premise of the alleged hack relies on the claim that voting machines are networked in real-time, either through the internet or private networks like Starlink. This is fundamentally incorrect. Voting machines are designed to operate offline during elections, with no internet connectivity, to prevent remote hacking. Vote tallies are transferred only after polls close, usually via secure physical media such as USB drives. Without real-time connectivity, the described coordinated hack through network-based exploits is impossible.

2. Firmware Updates Require In-Person Access

The claim that voting machine firmware was manipulated on a large scale ignores the reality of how such updates are implemented. Firmware updates require physical access to each machine. Election officials or authorized personnel must upload the software manually, machine by machine. This process involves stringent security protocols, including logging of the updates and verification steps to ensure the integrity of the software.

For a coordinated attack of the scale described, hundreds or thousands of machines across multiple jurisdictions would need to be physically accessed. Such an effort would require a large team, significant time, and the ability to bypass numerous layers of oversight. Moreover, these updates would leave an auditable trail—physical logs, version history, and cryptographic signatures that would expose any tampering.

3. ePollBooks Are Separate Systems

The letter conflates ePollBooks, which track voter check-ins, with vote-tallying systems. These systems are entirely separate. Even if ePollBooks were compromised, they do not interact with voting machines or tabulation systems. Any mismatch between voter check-ins and ballots cast would be flagged during standard reconciliation processes. Additionally, many jurisdictions maintain paper poll books as backups, ensuring accountability.

4. Decentralized Election Administration

U.S. elections are managed by thousands of independent jurisdictions, each with distinct systems, protocols, and oversight mechanisms. This decentralization makes a coordinated attack across multiple states extraordinarily difficult. Even within a single state, counties often use different voting systems and tabulation software. The logistical challenge of infiltrating this patchwork of systems without detection is immense.

5. Paper Ballots and Audits

Nearly all voting systems in the U.S. produce a voter-verifiable paper trail. Whether voters use hand-marked paper ballots or ballot-marking devices, these physical records are the definitive source of truth. Any manipulation of digital vote totals without corresponding paper ballots would be exposed during routine audits or hand recounts. These safeguards make it nearly impossible to alter election outcomes undetected.

6. Starlink and Wireless Networks

The suggestion that Starlink or other wireless networks were used for real-time manipulation is unfounded. Voting machines are explicitly designed to function offline during elections, with no authorized network connectivity. Unauthorized connections, even if attempted, would trigger alarms and violate established security protocols.

7. The Implausibility of Large-Scale Hacking

The scenario described in the letter requires:

• Physical access to potentially thousands of voting machines for firmware manipulation.

• A coordinated effort to upload tampered firmware while avoiding detection during pre-election testing.

• Real-time exploitation of ePollBooks to monitor turnout and create fake ballots.

• Matching fabricated ballots to tabulation records without leaving discrepancies.

Executing such an attack across multiple states would involve hundreds of operatives and substantial resources, creating numerous opportunities for

exposure. Each step of this process—from firmware updates to ePollBook manipulation—would leave behind an auditable trail, further increasing the risk of detection.

8. Statistical Anomalies and “Bullet Ballots”

The letter raises concerns about “Trump-only” votes, suggesting they were fabricated. However, these anomalies are more plausibly explained by voter behavior:

• Swing-state voters are subject to intense campaigning, with a disproportionate focus on the presidential race. As a result, some voters may cast “bullet ballots” for the presidency while skipping down-ballot races.

• While statistical anomalies can merit investigation, they do not inherently prove fraud. Routine audits and recounts are designed to address such concerns.

Conclusion

The described hacking scenario fails to account for the technical realities of U.S. election infrastructure. Voting machines are not networked during elections, and firmware updates require in-person access that would leave a clear trail. The decentralized nature of election administration, coupled with robust paper ballot auditing, makes a coordinated attack of this scale both logistically and technically implausible. These safeguards collectively ensure the integrity of U.S. elections and strongly counter the claims made in the letter.