Cabal Tactics

May 31, 2026
NOTE 1: The most up-to-date version of this is at https://HandCountRoadShow.org/cabal-tactics.

NOTE 2: If you don't realize this has been going on for decades, immediately watch https://TheLostInterview.com.

Introduction

This document is a catalog of observed, documented, and logically interconnected tactics, vulnerabilities, and methods used to compromise the integrity of American elections. It is not speculation—it is a synthesis of patterns reported by citizens, election observers, whistleblowers, data analysts, and independent investigators across multiple states and election cycles.

These tactics do not operate in isolation. They form a deliberate, multi-layered system designed to achieve one overriding objective: to control election outcomes while maintaining the appearance of a free, fair, and secure process.

The system works through:

- **Psychological preparation** of the public to accept manipulated results
- **Infiltration and capture** of institutions, organizations, and officials
- **Financial and candidate suppression** to eliminate genuine opposition
- **Legal and legislative embedding** of exploitable rules
- **Inflation of voter rolls** to create cover for phantom

ballots
- **Procedural sabotage** to block oversight and transparency
- **Exploitation of mail, early, and absentee voting** for real-time data and injection opportunities
- **Physical and digital vulnerabilities** that allow undetectable alterations
- **End-to-end control mechanisms** (feedback loops, weak audits, forced certification) that seal manipulated results

Each category in this list represents a phase or vector in that system. When viewed together, they reveal not random errors or isolated incidents, but a coordinated architecture that distributes risk, diffuses accountability, and exploits every point of trust in the modern election process—from voter registration to final certification.

The goal is simple: produce the desired result while making meaningful investigation, challenge, or reversal prohibitively difficult, expensive, or legally impossible.

This compilation exists so that citizens, legislators, sheriffs, attorneys, and election integrity advocates can see the full picture, recognize overlapping patterns, anticipate next moves, and prioritize countermeasures that address the system as a whole—not just its individual symptoms.

Read it sequentially to understand the progression. Refer to it modularly to identify specific attack surfaces in your jurisdiction. Share it widely. The more people recognize the playbook, the harder it becomes to run it in the shadows.

Outline

This outline serves as a table of contents for the reorganized list below. It summarizes the high-level categories, their focus, and key sub-items, providing a structured overview of how various tactics, vulnerabilities, and methods interconnect to undermine election integrity.

1. **Psychological / Perception / Influence Operations**
   Focus: Shaping public opinion, misinformation, and demoralization to control narratives and suppress opposition.
   - Linguistic Deception
   - Psychological Operations
   - Influence Operations
   - Media
   - Suppression-Based Perception Framing
   - Forced Opposition Projection
   - Fear/Discredit Tactics; Intimidation
   - Fake polling results
   - Manipulated betting markets

2. **Infiltration, Controlled Opposition & Institutional Capture**
   Focus: Inserting agents or co-opting organizations and officials to monitor, disrupt, or redirect efforts from within.
   - Fake Groups
   - Infiltrators
   - Infiltration of Grass Root Orgs
   - Infiltration of Offices
   - Usurpation of Election Officials
   - County Clerks Association

- Law Enforcement
- Political Parties

3. **Financial / Campaign / Candidate Manipulation**
   Focus: Controlling resources, candidates, and primaries to limit viable options and waste opposition efforts.
   - Cost to run
   - Campaign Consultants
   - Campaigns
   - Candidate Engineering
   - Districting/Gerrymandering
   - Primaries
   - Ranked-choice voting.

4. **Legislative & Legal Barriers**
   Focus: Using laws, bills, and legal tactics to enable manipulation, restrict access, and delay accountability.
   - Legislation
   - Lawfare
   - Delay Tactics in fixing election issues
   - Public Information Requests

5. **Demographic & Registration Manipulation**
   Focus: Inflating voter rolls with phantom or low-propensity entries to create opportunities for ballot injection.
   - Population
   - Illegal Immigration
   - Demographic manipulation
   - Colleges
   - Accessibility Sleight of Hand
   - Registration; Voter Rolls

6. **Process & Procedural Interference**
   Focus: Sabotaging meetings, events, and oversight to limit participation and awareness.
   - Public Meetings
   - Date/Time games
   - Electronic Date/Time Manipulation
   - Polling Places
   - Polls
   - Election Workers
   - Poll Watchers

7. **Voting Methods & Early / Mail / In-Person Exploitation**
   Focus: Exploiting extended voting periods and mail systems for data collection and ballot insertion.
   - Early Voting; Election ‘Day’
   - In-Person Voting converted to Mail-in
   - Ballot Harvesting
   - Low-Propensity Voter Record Harvesting
   - Mail ballots
   - Drop-Boxes
   - USPS
   - UOCAVA
   - Chain of Custody sleight of hand

8. **Ballots & Physical / Printing Vulnerabilities**
   Focus: Manipulating physical ballots through design flaws, errors, or handling to enable fraud.
   - Ballots

9. **Technology, Software & Cyber Vulnerabilities**
   Focus: Backdoors and weaknesses in digital systems for undetected alterations.
   - Fake Testing and Certification

- Technology / Cyber-Security
- Data Breaches; Software
- Electronic Poll Books
- Electronic Voting Machines
- Mobile Voting and “shiny new object” technology
- Election Code.

10. **Overall Systems & End-to-End Manipulation Framework**
    Focus: Comprehensive methodologies tying together injection, flipping, and verification evasion across the election lifecycle.
    - Overall Manipulation Methodology
    - Feedback Loop
    - Tabulation
    - Reporting; Records
    - Certification
    - Auditing
    - Canvassing
    - Recalls
    - Election Contest

Detail

1. Psychological / Perception / Influence Operations

- Linguistic Deception
    - Exploit public ignorance and ambiguity in terminology. Examples:

- “Hand-Marked Paper Ballots” Deception: Citizens are directed to demand “hand-marked paper ballots” as a perceived solution for verifiable elections. The term is exploited because it only requires voters to mark paper ballots by hand, which are then fed into electronic tabulation machines for counting. Once implemented, officials claim compliance (“You already have hand-marked paper ballots”), while the actual counting remains opaque and machine-dependent. This channels public energy into an ineffective reform that fails to deliver hand-counted results, creating frustration and demoralization without achieving meaningful transparency.
- “Air-Gapped” Systems Deception: Election officials and the public are told that electronic voting systems are “air-gapped” (completely isolated from networks), implying they are secure from external interference or remote manipulation. The term is misused because many systems are not truly isolated in practice—due to memory cards, USB transfers, wired/wireless/modem connections, or administrative access—yet officials, lacking deep technical understanding, accept the claim and project false confidence. This discourages scrutiny from citizen experts, reinforces institutional dismissal of concerns, and maintains the illusion of security while vulnerabilities persist undetected.
- “Encryption” Deception: Voting system vendors and officials promote “encryption” as a key security feature that protects election data.

In reality, encryption serves primarily as a form of obfuscation that conceals potential manipulation from public view. What should be prioritized instead is verifiable data integrity through full transparency, where all processes and data remain visible and auditable at every step. Transparency and verifiable integrity supersede hidden mechanisms; that which cannot be seen cannot be independently verified. This semantic framing creates a false sense of protection while enabling undetectable alterations.

- Psychological Operations
    - Misinforming the public with information dominance
        - will not understand the battlefield
        - will fight each other
        - will not listen to each other
    - Distracting the public
        - will waste their resources
        - will drain them emotionally
        - will dilute their efforts
    - Demoralizing citizens
        - causes loss of hope
        - causes loss of courage
        - causes loss of confidence
- Influence Operations

        - Create another media system, ‘social media’
        - Incentivize people to become influencers
        - Use influences to manipulate public opinion

- Media
    - Push the narrative of ‘security’ and ‘accuracy’ until people start believing it.
    - Discredit any entity that questions security or accuracy of election, so the people ignore or discount the presented facts.

- Suppression-Based Perception Framing
    - Suppressing visible support (flags, signs, stickers) makes it seem as though there’s less backing for one side than actually exists.
    - This alters perceptions so that when results are falsified to favor another candidate, those manipulated believe the stolen victory was more plausible because they were misled about how popular their preferred candidate truly was.
    - The tactic leverages fear and self-censorship to create a false reality where fraud is harder to detect.
    - Examples:
        - Targeted Removal: Removing candidate signs or flags from lawns through vandalism, theft, or staged incidents makes it seem as though support isn’t widespread.
        - Public Shaming/Intimidation: Attacks on individuals wearing pro-Trump gear create a climate where others self-censor to avoid harassment.
        - Media Pressure: News coverage exaggerating the

lack of visible support for one side further distorts perceptions before an election.

- Forced Opposition Projection
    - Manufactured rallies and similar orchestrated protests function as a display of opposition designed to distort perceptions about public sentiment.
    - Artificial Crowd Generation: organizers bus in supporters from outside local areas instead of relying on organic turnout. This creates the illusion that there's wider support for a particular agenda than actually exists, making it seem more mainstream and legitimizing attacks against certain supporters.
    - How It Works:
        - Bus-In Tactics: Protesters are brought in from cities or regions where political opposition is already concentrated, ensuring a larger-than-realistic crowd presence. This bypasses the need for local grassroots support.
        - Media Amplification: Media coverage focuses on the size of the "organic" protest rather than questioning its artificial nature, creating the perception that there's overwhelming public demand against a movement.
        - Suppression Reinforcement: The illusion of widespread opposition normalizes hostility towards those who support a particular movement, further suppressing visible allegiance through fear and self-censorship. If a rally looks large and popular, others

will be less likely to openly oppose it for risk of backlash or social ostracization. The tactic is effective because many people base their opinions on surface appearances (e.g., how “big” something appears in media) rather than deeper engagement with issues. It works best when combined with other suppression strategies like attacking certain supporters, making the fake rally look more credible by association.

- Fear/Discredit Tactics
  - Compromise some people by getting them to commit election crimes
  - Target/attack/discredit everyone that reports or discusses election crimes to make them an example and scare others from reporting election crimes
  - Target/attack/discredit any attorneys/election officials/legislators/judges/etc to dissuade them and any others from getting involved

- Intimidation: reference is The Virginia Project Intimidation Tactics and You: Beating the Zerg Rush
  - It generally starts with hate spam – messages delivered to you in some fashion, whether by phone, email, over social media or some other form of communication. People you don’t know, who don’t know anyone who knows you, and who don’t appear to have any particular connection to anything you are involved in, suddenly decide they hate you in particular and they want you to know it, repeatedly, in volume. It is phony, contrived and organized. It

is called inorganic intimidation because it is not natural.

- The main characteristic of inorganic intimidation and interference operations is that the point is to stop you from doing whatever you were doing – the attacks sustain over time rather than waning. You were successful at something they didn't like, therefore they will shut you down.
- To bring this home, almost every Republican campaign and organization gets hit by mailing list stuffing attacks, the purpose of which is to load you up with spam flags so that your emails no longer reach inboxes, effectively silencing you in that medium. This was discussed at length in a pair of Virginia Project newsletters last year (Losing the War in Cyberspace | Alice in Cyberspace). These are swarm-intimidation events.
- The ranks of conservatives and Republicans who have been targeted by this means are already considerable – they include, among others, the current Virginia Lieutenant Governor – as is the material damage done to GOP electioneering operations. It will only increase over time – unless we put our foot down and end the proliferation of these unlawful practices with robust application of the law.
- We know how to handle brute-force intimidation through multiple communication vectors: do not react fearfully; never respond; do not read threatening communications, just record everything; and when the evidence you collect crosses the threshold of probable cause, bring in law enforcement and/or call in a lawyer to collect damages from perpetrators. This intimidation is unlawful interference against our campaigns and activism.

- We know that Virginia Democrats will, in fact, conspire amongst themselves to raise money to hire criminal hackers to attack your online assets. This likely happens across the country.
- To combat the above: Re-code websites from the ground up with an integrated software firewall with enhanced traffic analysis and reporting capabilities, and a component what I suppose marketing agencies might these days call a “network application security AI.” Develop an entire security layer of an application that can execute in less than 50 milliseconds, distinguishing real “customers” from both the ongoing hostile background noise of the Internet as well as targeted and sustained cyberattacks from abroad.
- Social media companies are avenues by these gangs to hijack their content moderation processes. Never rely on a social media platform alone, but if it happens exchange with that company’s litigation team to expose unfair tactics against GOPers and candidates.
- As a Republican, you need this system to protect yourself from the illegal things that Democrats, as well as other enemies of the American people, will do to your communications. So say goodbye to “my county GOP committee doesn’t have a website” and all the votes left on the table.
- The Virginia Project believes they have gotten the mission of helping Twitter fix its account exploitation bugs. If you have been the victim of an unexplained account lock out on that platform, please email a description of your experience and the username of the account.
- The Biden Administration is using, among other

things yet to be explained, the EU ‘Digital Services Act’ to censor domestic opposition on social media.

2. Infiltration, Controlled Opposition & Institutional Capture

- Fake Groups
  - Claim to be on our side
  - Suck up money
  - Suck up attention
  - Redirect the citizens away from real solutions

- Infiltrators
  - These will inject themselves into existing groups
  - They will make themselves sound great
  - They may even provide some help to gain people’s confidence
  - Then they start playing people against each other
  - They cause disruptions
  - They cause distractions
  - They may get the group to do something that can then be used to discredit the group
  - Sometimes they do this work through another unsuspecting person in the group so nobody expects it.

- Infiltration of Grass Root Orgs
  - Cabal may co-op the Leader of grassroots election org and pass / receive info thus monitoring and controlling efforts. The leader/org may have no idea they are being used.

- Cabal may bait honest citizens into frivolous lawsuit to discredit and demoralize group.

- Infiltration of Offices
  - We have seen many of the following individuals be put into positions over a period of time, operating in lock-step inhibiting transparency and verifiability in elections:
    - Governor
    - Secretaries of State
    - County Attorneys
    - County Sheriffs
    - County IT Staff
    - County Judges

- Usurpation of Election Officials
  - The systems are too complex and vulnerable for election officials to understand
  - Election officials must completely rely on assigned ‘cybersecurity’ experts who are in effect actually controlling our elections
  - They have election security/information dominance, controlling exactly what our representative officials know
  - Election Officials that resign prior to the end of their term could be replaced by an ‘appointed’ individual not beholden to the citizens

- County Clerks Association
  - NGO paid by counties and unaccountable to county’s electors
  - Instruct clerks they serve as “Agents of the

Secretary of State”
    - Instruct clerks to trust machines and vendors
    - Convince clerks that electors are dangerous and to be feared
    - Instruct clerks to “forget” to notify (Republican) party chairmen to appoint Canvass Board members, so clerks can appoint them on behalf of party
    - Intimidate Canvass Board members who don’t certify elections
    - Work closely with Secretary of State to pass rules, statutes, and laws centralizing elections under government control

- Law Enforcement
    - Sheriffs are being sequestered into the service of the county (corporation) and state through interlocal agreements and county policies.
    - Training for sheriffs is provided by the county attorney’s office. This is an usurpation of the People’s protection against government officials acting unlawfully.
    - Push out good officers to make room for bad officers that will not uphold the constitution.
    - Media attack on law enforcement
    - Turn citizens against police, police against citizens
    - Force retirement of law enforcement by making it miserable to be a good officer
    - Lack of education of Sheriff’s rights/duties
    - Compromised and blackmailed judges/prosecutors

- Political Parties
    - Fuel further division rather than unity on fair

elections.
- Make non-partisan positions, partisan.
    - AZ Clerk and Recorder
    - DASS – Democratic Secretaries of State
    - etc.

- Do not adhere to (or don't know) their duties to provide Election Judges, Poll Watchers, and Audit and Canvass Board members
- Don't exert their authority over election operations as representatives of the electors, which is greater than that of the clerks and SOS who are "elected"
- Don't hold the election officials accountable for providing honest elections
- Fail their constituents by not demanding honest elections
- Are likely gaining power or monetary benefits by their complicity in election manipulation
- There are no teeth (consequences) in many of the laws, therefore nothing to prohibit people breaking the laws, paving the way for abuse under false sense of security.

3. Financial / Campaign / Candidate Manipulation

- Cost to run
    - Increase cost to run for office/positions, so only someone with big money behind them can afford run, disenfranchising ordinary American Citizens.

- Campaign Consultants – There is a group of consultants coordinating to covertly subvert the candidates they

represent

- Suck money
- Subtly sabotage campaigns
- Share information with cabal
- Control information flow
- Block opportunities

- Campaigns
  - Many campaign managers are controlled opposition and attempt to control and spy on citizen candidates
  - Campaign financial manager may waste funds or violate laws in order to compromise the candidate they pretend to support

- Candidate Engineering
  - Candidates changing parties to give themselves a competitive advantage while deceiving the citizens.
  - Sleeper Candidates – They have their people already embedded in opposite party, positioned to be placed in a race to split votes.
  - Bad Candidates – They purposely support candidates on our side that:
    - Are controllable through compromise
    - Don’t have what it takes to pull through, sucking up donor dollars and wasting resources.
    - Will cause chaos

  - They find a candidate B with a similar name to run against candidate A to confuse the voters to bleed votes

- Districting/Gerrymandering

- Primaries – Cheat every way possible to control the endorsed candidates
    - Bribe others to run to split the vote
    - Hire people to Bad-mouth opponents
    - Open-Primaries – These can be used to cheat! They allow the opposing party to control who is on the ticket. Open-Primaries are a trojan horse.
    - Cheat using the voting system
        - Allow ‘delegate’ votes, then control the delegates
        - Add ‘anonymous’ votes during voting process (see CA GOP)
        - Pre-make slides to show pre-determined outcomes, and show those instead of the real-time votes (citizens don’t know the difference)

- Ranked-choice voting (See @Ranked Choice Voting (RCV))
    - There are many reasons this is a bad idea. One of them is that it is so complicated that it REQUIRES a computer tabulate and LOCKS us into using computerized tabulation. That ALONE is reason to boot it.
    - Allows covert election manipulation hidden in the complexity of the calculations
    - RCV information:
    - Behind RCV:
        - Open Society – ‘Fair Vote’
        - Tides Foundation – ‘Unite America’
        - GEHL – ‘Action Now’

    - Beware of RCV implemented under a different name.

4. Legislative & Legal Barriers

- Legislation
  - They inundate legislators with so many lengthy bills, nobody has a chance to read them.
  - They get naïve legislators to carry ‘election integrity’ bills as a good ‘compromise’ (e.g., 2026 HB95 in AL)
  - They disguise bills building in trojan horses
  - They create legislation, then later change the definition of the terms used in the previous legislation. Bait and switch.
  - They create a sacrificial bill to put on the ballot that gets a certain group riled up in order to increase biased voter participation.
  - They sneak legislation changes into the state budget (including legislation that moves representation away from the governed)
  - Passing bills to eliminate hand counted ballots (e.g., AB969 in CA).
  - Laws are created to give people the sense of security, which turns false because they then don’t follow the laws.
  - Laws are created to restrict access by the citizens, blocking us from being able to see or verify our own election system. This is done SUBTLY, and/or hidden in other legislation. They SNEAK THESE LAWS IN! (e.g., 2026 HB67 in AL)
  - There is no reasonable penalty attached to breaking election laws.
  - Requiring municipalities to use county election systems in order to centralize and control downstream elections.

- Lawfare
    - Out-lawyer the citizens so they cannot afford representation to fight with equal force
    - Attack the citizen attorneys (personal attacks, lawsuits, go after their license, etc.)
    - Refuse to hear case and evidence due to ‘lack of standing’
    - Blocking evidence:
        - Play word games and feign confusion with the information requests (they play stupid on purpose)
        - Push citizens to the point of lawsuit, then claim they cannot release the records due to lawsuit
        - Delay information release until suddenly the information is gone for some reason (hard drive crash, backup failure, etc.)

    - Cases are moved to jury trials to induce additional costs to pursue.
    - Delay tactics are frequently used to kick the can down, then leave no time to get anything fixed.
    - Harassing and countersuing the plaintiffs and asking judges for motions to reconsider to drain our finances and harass plaintiffs

- Delay Tactics in fixing election issues
    - Policy analyses
    - Feasibility studies
    - Impact assessments

- Public Information Requests
    - Election Database Backups – Vendors and some

Counties use a myriad of excuses to deny access to these databases as well as charge exorbitant fees:

- Intellectual property – They claim that there is IP in the database backups. There shouldn't be any, of course. If there is, then the company is incompetent in putting their intellectual property inside a file meant to serve as an archive of election data. There is no need to put any IP in that, so if they are doing so on purpose, they are doing so in order to use this as an excuse to block citizens from accessing it.
- Critical Infrastructure – They claim there is information in the database backups that would compromise the security of their 'critical infrastructure' election systems. Then I suppose their 'critical infrastructure' election systems are for some reason storing information that could compromise the security of their systems in files that should never have this kind of information. This would violate critical infrastructure best practices. So, which is it? Are they critical infrastructure and they incompetently or maliciously violated those best practices, or are they not and they're just using this lie to restrict access to information?

5. Demographic & Registration Manipulation

- Population

    - Population numbers are increased by every available means, in order to have headroom to increase registered voters.
    - Prior to 2010, the Census Form had a citizenship question on it. In 2010, the form was replaced with a different form that had no citizenship question on it. California even sued to keep the citizenship question OFF the census form.
    - Open-borders substantiate higher population numbers that include illegal aliens with no way to verify them.
    - There are cases of census ‘miscounting’ the population as well.

- Illegal Immigration
    - Mass immigration combined with a census that now counts them allows justification for higher population, and creates more headroom of justifiable registered voters and enables gerrymandering.
    - Allows creation of voter registration records that don’t actually need to be tied to a real citizen
    - The voter registration records allow ballots to be created, mailed, cast, and tabulated.
    - There are not adequate protections in place to protect elections from this (by design, most-likely)

- Demographic manipulation
    - Move people into cities to run for offices in order to start shifting political demographics at county/state levels
    - Artificial entities act as a form of “phantom” or non-human voters that dilute the weight of actual resident human votes. (For instance, Delaware

allowing LLCs, Trusts, and Companies to vote in elections.)

- Colleges
  - They bring groups in from other states to harvest voters from young populations
  - Our kids are targeted on campuses to capture their votes

- Accessibility Sleight of Hand
  - Felon Voting Rights – This isn't really for felons to actually vote. It is to pave the way for the cabal to inject more phantom ballots into the system. It merely provides justification for the value to be there. This creates yet another huge abuse vector.
  - Minor Voting Rights – This allows children who are easily manipulated and persuaded, who's brains aren't even fully developed yet and aren't even mature enough to sign a legal contract, serve on a jury, file a lawsuit, open a bank account, buy a stock, rent an apartment, consent to their own medical care, register to give blood, get a tattoo, buy a car, etc, to change laws, choose judges, local/state/federal officials, and even the President of the US.

- Registration
  - Some 'requirements' allow:
    - no driver's license, ID card, SS card
    - no physical address, mailing address only
    - entries for people that are only 15 years old but warn them not to vote because it is

illegal
        - have to be in the state for at least 22 days (this would allow state-hopping) to cover staggered elections.)

- Increase numbers of independent registrations
    - Independent are more universal manipulation purposes
    - Inflating independent voter rolls gives fake results a plausible cover – more ‘wiggle room’ to explain whatever outcome is needed
    - Illegal or ‘gray-area’ voter registration drives
    - NGO’s going performing voter registration
        - They target vulnerable parts of our communities
        - It gives them direct access to people’s information (violation of privacy)
        - In at least Maricopa County, the county provided registration NGO’s URL/API access directly to their county voter registration system (to be confirmed with @Shelby Busch)

    - If the elected county officials are not in full control of all registrations, it leaves a huge attack surface open
    - Youth Pre-registration – In some states, children are allowed to be ‘pre-registered’ to vote.
        - Allows plausible excuses for procedural ‘mistakes’ that allow indirect manipulation of elections

        - Send out ballots to the youth. If caught, just claim it was a mistake. If not, free uninformed voters!

    - As soon as those pre-registrations hit the 18 yr old mark, they are automatically changed to active status which allows them to be used an excuse for injection of phantom ballots.

- They are changing people from their designated party to PND status (party not designated) in order to vote for use their record to inject votes.
- Voter registration records will be changed to inactive without the voter knowing, causing the not to be able to vote. In many states, this can happen even on election day prior to voting. If you vote by mail, you won't know until it is too late. If you vote in person, you'll find out right then and you can make them fix it right then.
- No responsible party / accountability for keeping the voter rolls accurate
- Voter registration databases do not mandate or even include the SOURCE of the registration record (the individual that caused the registration, and the full path it took to arrive in the database in the first place)
- People go to graveyards and find names off of tombstones
- Traveling Voter Operations

- Recruit individuals willing to travel (college students, transient workers, activists, or paid operatives).
- Pre-register them in multiple early-voting states using forwarding addresses, sympathetic roommates, or vacant properties (a practice already documented in some voter-roll studies).
- Starting with the earliest-opening states (e.g., Minnesota and South Dakota open ~46 days out; New Jersey, New York, Virginia ~45 days), the travelers vote in person during the early period.
- Move immediately to the next cluster of states whose early voting has opened but whose rolls have not yet received updated “voted” flags from the previous states—flaws amplified by ERIC’s batch processing and spotty detection.
- Repeat across the country, hitting battleground states in waves (Midwest → Southeast → Southwest → West Coast) over the 2–6 week early-voting calendar.
- In states with same-day registration, simply show up, register, and vote—no pre-planning needed.

- Voter Rolls
  - Their goal is to increase the registered voters by as much as possible, especially with low-to-no-propensity voters, because they need those database

entries to attach votes to.

- Motor-Voter system is a gateway for illegitimate voter registrations. They utilize weaknesses in obtaining driver's licenses in order to create a voter registration record.
    - Voter Reg Entries are also being created for those too young to vote, but old enough to drive.

- Loose or no ID requirement to register to vote in many cases
- Proof of residence not being required or confirmed.
- Mass change of party affiliation to unaffiliated in order to manipulate – Look for affiliation changes before and after primaries
- Change of party affiliation prior to becoming poll-workers in order to pose as different party.
- Leaving bad records in (not purging them – why are they not purging? by who's instruction?)
- Injection of bad records
- Loose security in access controls
- Loose access logging
- No change-tracking
- Duplicate entries of individuals with name changes (maiden/married names)
- Addresses modified (street names) to send ballots to know bad addresses
- Outsourcing the responsibility of maintaining voter rolls to entities that fail to maintain them properly (through incompetence or maliciousness), also allowing the rolls to be indirectly manipulated by a fourth-party.
- Adjustments to voter rolls are made in real-time, even during the election

- No data consistency
- No change-tracking
- No referential integrity
- Same-day voter registration paves the way for last-second ballot injections.

6. Process & Procedural Interference

- Public Meetings
  - They get rescheduled to cause conflicts
  - People are assigned to run out the clock to eliminate or reduce our time
  - Public speaking time is continually reduced
  - Microphones are shut off
  - Livestreams/recordings sometimes have audio ‘issues’ that result in the public not being able to hear

- Date/Time games
  - They advertise incorrect dates/times for events in order to cause people to miss events (one example: publishing LAT at 9a, but starting at 8a so poll watchers miss the first hour).

- Electronic Date/Time Manipulation
  - There are many instances of date/time not being accurate on various parts of the voting systems.

- Polling Places
  - Enact laws that make it prohibitive to qualify many locations as polling places to force the centralization of polling centers.

- Implement “County-Wide Voting”
    - Sold as conveniences
    - Centralizes control
    - Centralizes manipulation
    - Allows undetectable laundering of votes

- Nothing wrong with reasonable ADA requirements for our disabled citizens, but we do need to take these into account: 2016-06 US DOJ Civil Rights ACA Checklist for Polling Places (votingchecklist).pdf

- Polls
    - They prohibit anyone wearing political attire at the polls to protect the Election Illusion.

- Election Workers
    - They make it seem like anyone can apply, but they choose who becomes election workers. The election workers are their people.

- Poll Watchers
    - They make it seem like anyone can apply, but they choose who becomes poll watchers. The poll watchers are their people.
    - They mis-train poll watchers so they don’t know what to look for.
    - They keep watchers and observers from access to polls, testing so that they can’t view anything that matters

7. Voting Methods & Early / Mail / In-Person Exploitation

- Early Voting
  - They collect data and build a model of the election results prior to tabulation:
    - Mail-in Ballot-Tracking – They tell the citizens that the ballot tracking is so citizens can track their ballots. However, the ballot tracking allows the cabal to know who has voted. Combined with databases of party affiliation and other online profiling, the vote of each returned ballot can be estimated without even needing to look at the ballot.
    - Electronic Poll Books – When someone checks in to vote, this data is put into a central database. Combined with databases of party affiliation and other online profiling, the vote of each returned ballot can be estimated without even needing to look at the ballot.

  - They can calculate how much of an adjustment to the votes needs to be made, then take advantage of voter registration database manipulation to utilize phantom records or records of low-propensity voters to inject ballots into the system to shift the results organically before anything goes to tabulation.
  - Early voting makes it more challenging and costly to perform exit polling.
  - GOP's "Bank Your Vote" https://bankyourvote.com/
  - Some states claim they do not tabulate during early voting, however, feeding ballots through a machine

that can scan and/or tabulate that ballot is tabulated and certain people would have access to the results in real-time.

- Election ‘Day’
    - Allowing voting before Election Day allows bad actors to gain necessary information to more accurately estimate the results to manipulate the results by injecting ballots.
    - Allowing voting after Election Day allows bad actors to make final adjustments to the results by injecting ballots.
    - All of this turns the election into a feedback control system that bad actors can use the control the results of elections with high precision.
    - Deprive voting centers of enough ballots or ballot paper to service the voters. (eg Harris County TX)

- In-Person Voting converted to Mail-in
    - Colorado and other states force citizens to convert their in-person votes to mail/drop-box in order to launder them all into one voting type.

- Ballot Harvesting – Harvest signatures from elderly citizens
    - Retirement communities
    - Nursing homes

- Low-Propensity Voter Record Harvesting – Records that have a low propensity to vote are used to attach ballots to.
    - Hospitals
    - Mental health institutions
    - College dorms/fraternities

- Mail ballots – Injection of ballots with broken chain of custody
    - Declare an emergency to force the use and relax/ignore other election laws
    - Real-time tracking systems allow bad actors to track ballots to gain realtime information to abuse.
    - Postal carriers instructed to NOT deliver ballots to the address in which no residents with that name reside so that the ballot can be routed elsewhere, thus avoiding alerting of multiple ballots registered to that address.
    - Addresses copied from one locality to another, but changing the street name, generating returned ballots
    - Mail ballots create many chain-of-custody vulnerabilities, which make it easy for error and manipulation to occur.
    - They claim drop-boxes have 100% surveillance, when they do not!
    - Many states have permanent mail in ballot registration causing a perpetual flood of ballots in the mail.
    - No poll watchers at the post offices, where millions of ballots are flowing through.
    - Missing Postmarks
    - Fake Postmarks (postmarks can be dated whatever the person operating the machine wants to date them)
    - Mail-in ballots severely cripples the ability to perform exit polling (This is KEY for those that would want to manipulate elections, because it destroys this additional verification component)
    - Signature Verification
        - The Gatekeeper of fraudulent ballots entering the system

- Initiate “updated” signature drives for all registered “voters” and inject fake “updated” signatures.
- Designed to be defective in order to manipulate
    - Many citizens are not trained at all
    - Citizens that are trained are not properly trained
    - Proper training takes 2 years of certified document examiner schooling
    - There is not testing prior to allowing a citizen to verify signatures
    - Citizens are fired if they reject too many signatures

- Drop-Boxes – Injection of ballots with broken chain of custody, avoiding any tracking by USPS.
    - Public/Private money funding setting these up all over
    - Many boxes that require surveillance cameras don’t have them
    - Public has limited/no access to surveillance footage
    - No control of what gets put in or by who
    - Provides an open path to easily inject ballots into the system without even USPS tracking of mail-in ballots.

- USPS
    - When the USPS classifies a ballot as ‘undeliverable’, they gather them in one or more facilities.

    - Several USPS workers have told @Mark Cook that those stacks of undeliverable ballots mysteriously decrease toward the election.
    - The USPS is billing the counties for undelivered ballots (typically by weighing them instead of counting them – total loss of chain of custody).
    - The USPS then delivers far less undelivered ballots to the county, and the county typically reflects that amount in their reports.
    - The people in the county don't notice, seem to know why, or care that they received less undelivered ballots than they were billed for.
    - Mail ballots are BIG BUSINESS for the USPS (yet another private organization

- UOCAVA – Uniformed and Overseas Citizens Absentee Voting Act
    - This system makes it easier for our military and overseas voters to vote, at the expense of making the entire system much more vulnerable to manipulation.
    - Nobody seems to be asking the question "How could a bad guy manipulate this?" in every new part of UOCAVA that is brought forward.
    - For example, look what this organization is doing: VoteFromAbroad.org
    - More vulnerabilities listed at www.verityvote.us/overseas-voting-vulnerabilities/.

- Chain of Custody sleight of hand allows opportunities to distract or avoid detection while manipulating ballots/records.

- Water main breaks
- Power outages
- Bomb threats

8. Ballots & Physical / Printing Vulnerabilities

- Ballots
  - Ballots in multiple languages adds to complexity (increasing numbers of different ballot styles) forcing the use of computers to tabulate
  - Consolidate many smaller elections into less frequent larger elections makes ballots more complex and hand count more difficult
  - Textual ‘Mistakes’ on ballots (names spelled wrong, names missing, geographical differences)
  - Wrong ballot styles being given to people to affect who they can vote for. Then they claim ‘mistakes’.
  - Markers are used so they don’t leave kinematic artifacts (indentations) that could be used to discern a copied ballot vs a real ballot (a photocopied ballot may look like a pen filled it out, but it won’t have indentations in the paper). Pen indentations are a critical secondary artifact against fraud.
  - Mix any questionable ballots in with the rest to make it impossible to find them again should they be ruled ineligible, making any argument moot.
  - Misalignment between front and rear of ballot will cause misread resulting in easy redirection to adjudication for manipulation
  - Shrink or enlarge the ballot image slightly to skew the alignment marks will cause misread resulting in

easy redirection to adjudication for manipulation

9. Technology, Software & Cyber Vulnerabilities

- Fake Testing / Certification
  - Vendors pay the ‘testing’ labs.
  - Test procedures designed to avoid finding real issues.
  - Labs approve systems.
  - Systems are certified.
  - Everyone downstream ‘trusts’ because they were ‘tested’ and ‘certified’.

- Technology / Cyber-Security
  - Instead of handling security locally, many counties and states are outsourcing those services, which puts that at risk and displaces the responsibility
  - Creates a much more attractive attack surface
  - Bad actors can then exploit to cause a much larger blast radius
  - Decentralization is defeated when certain components are centralized

- Gradual Network Interconnection Strategy
  - Install wireless cards, modems, additional connectivity (even covert) so the citizens and election officials aren’t aware. Take advantage of the fact that election officials are not cyber-security experts and they don’t know what they don’t know, in order to manipulate the system right under their noses.
  - Start with the systems in a disconnected state, tell

the citizens they are all isolated and ‘air-gapped’, then once they are used to that, start mandating that parts of them become connected, until after several years/cycles, they are all interconnected via a network.

- Data Breaches
    - Beyond the original breach are usually hidden higher-order breaches as a results that can be leveraged by bad-actors.

- Software
    - Lack of downstream verification
        - Officials that are conducting elections using black-box systems that:
            - They blindly trust (voluntarily and involuntarily)
            - Don’t look ‘under the hood’ to ensure their security
            - They aren’t allowed to look ‘under the hood’ to ensure
                - The software that is running on their systems is what was originally tested
                - Doesn’t have any malicious programming embedded in it

    - Update Scam
        - Vulnerabilities are found or ‘found’ in order to spur states and counties to buy NEW

equipment/software to ‘fix’ the problems. The new stuff can have even more sophisticated methods to manipulate elections built in to them. Then vulnerabilities are ‘found’ on those, and counties are pressured to buy NEW equipment again. Continual income for the vendors, and manipulation becomes continually more sophisticated. This applies to the entire ecosystem from voter reg, ‘sig-ver’, poll books, tabulation, and reporting.

- Electronic Poll Books
  - These are typically connected to each other over insecure wireless connections, then all connected to a central database outside of the polling location, and sometimes outside of the state they are operating in. Unknown parties have control of these databases, therefore can view/add/change/delete records at their will, without the knowledge of the poll workers, county officials, or state officials.
  - These can be abused wirelessly from the parking lot, wired from within the polling location, on the cellular network or internet anywhere in the world. The counties and states do not have control of these regardless of what they claim.
  - Data from poll books can be read by others and used to know how to manipulate the election by adding phantom ballots, then injecting phantom electronic check-ins.
  - Electronic Poll Books usually consist of common Android tablets or Windows laptops (all easily abused by people that know how), hidden in a custom

frame.

- Electronic Voting Machines
    - For D.R.E. (Direct-Recording Equipment – touch-screen voting)
        - Change the touch-screen calibration so when someone selects their candidate, the other candidate is selected. Many won't notice.
        - Program the system to select whichever candidate you like regardless of which candidate name is touched. Set up a counter in the software so after X number of tries, the correct candidate is selected. This can be easily explained away as 'calibration error'. Most will fall for this explanation. It's been going on for over a decade.

    - Show one thing on the screen and the printout, but record the votes any way you like in the database.
    - Record the votes properly in the database initially, then change them later.
    - Show one thing on the printout, but put different results in the QR-code, then encrypt the QR-code so humans can't see what's been done.
    - Put the software you want them to see in escrow. They won't know that it isn't the same as on the voting machines.
    - Use QR-codes to covertly make adjustments to the votes/feed algorithms. Then put them in the mail or drop-boxes. The election staff will be delivering the payload themselves without having a clue.
    - If they figure out the QR code con, then use what appears as random dots on the page, but watch for

them in the programming and make adjustments with those instructions.
    - If they figure out the ‘random’ dot approach, then use very light color like yellow that the scanner can pick up, but the human eye will not without a magnifying glass.

- Mobile Voting and “shiny new object” technology
    - Since machines and mail-in voting will be seen as rife with fraud, they will attempt to introduce/implement “mobile voting”
        - Will use the “proven track record” with UOCAVA as evidence that it is “safe and secure”
        - Will appeal to Trump’s love of crypto and the public’s growing acceptance of block chain.
        - Use NASS to push
        - https://www.mobilevoting.org/about

- Election Code
    - Actions that facilitate indirect manipulation of our election system have been put into code.
        - For example, Texas: Sec. 85.072. BRANCH DAILY REGISTER. (a) Each day early voting is conducted at a branch polling place, an election officer in charge of the branch shall prepare a register listing the voters who cast ballots at the branch that day. (g) The Previous early voting clerk shall compile the registers and electronically submit to the secretary of state a record of each voter participating in a primary, a runoff primary, a general election, or any special election

ordered by the governor not later than the day the voter votes in person or the early voting clerk receives a ballot voted by mail.

10. Overall Systems & End-to-End Manipulation Framework

- Overall Manipulation Methodology
  - Injection of phantom voters and corresponding votes (votes not correlated to real citizens)
    - Combat at voter registration and validation legs
  - Injection of votes for existing voters (stealing their identity)
    - Combat at validation leg
  - Vote-flipping
    - Combat at validation, tabulation, and reporting legs
  - Result-shifting/flipping
    - Combat at result leg. Set up parallel reporting at precinct levels (or county level if precinct not available)
  - Distribute the manipulation across states, counties, precincts to keep below margin of error
  - Distribute the manipulation across states, counties,

precincts to keep below margin of recounts

- Feedback Loop
    - Inject phantom voter registrations
        - Use plausible deniability in duplicating existing records (make sure every duplicate can be explained away as a mistake)
            - Change spellings of names slightly. Examples:
                - Bob Smith
                - Bob Smyth
                - Bobby Smith
                - Bobby Smth
            - Slightly change addresses. Examples:
                - 123 Jones St
                - 123 Jones
                - 123 Jones Street
                - 123 Jones Ave
                - 213 Jones St
                - 123 Jons St
            - Duplicate records will have their own voter ID number, allowing a vote to be associated with it. If someone catches the ‘duplicate’, it can be explained as a typo.
    - Encourage everyone to register to vote to put in as many registrations possible
    - Design a system to monitor who has voted

        - Mail in ballots – Design a mail-in-ballot tracking system to give the public a warm fuzzy false sense of security for using mail in ballots. Tell them that they can ‘track their ballot’. The tracking isn’t really for the citizens, it’s used to know when each one of them votes (and to track which ballot belongs to which individual so they can be ‘handled appropriately)
        - In person – Design digital poll book system to track who comes in in person to vote

- Knowing who has voted, use their party affiliation and voting history fortified with social media profiles to determine how they will vote
- Build a model of the election results (without even needing to look at a single ballot)
- Determine how many votes are needed to shift the results
- Choose which voter reg records to associate with phantom votes
    - Use the existing voter registration metrics combined with the real-time tracking from mail-in-ballot tracking system and electronic poll books
    - Record preference priority
        - Phantom records – these are best to use first because nobody will ever show up to vote and be told they already voted
        - Low-propensity voters – these are more risky because these voters may actually show up
        - High-propensity voters – these are very risky and should only be used as a last

resort as they are likely to result in voters catching their use

- Record distribution
  - Don’t choose records in the same precinct. Use a distribution of records in different precincts where you think there is room. Remember, STAY UNDER 100% VOTER PARTICIPATION so the injections don’t stick out.

- Inject ballots into the system
  - Mail them in
  - Scatter them in drop-boxes

- If done properly, manipulating the system using the feedback loop will be hidden from the county officials.

- Voting on DRE or BMD
  - Touchscreen voting machines—whether Direct Recording Electronic (DRE) systems or Ballot Marking Devices (BMDs)—rely on software that translates voter taps into selections. Programming such devices to intermittently ignore a tap or register the opposite choice can create ***arbitrary vote alteration***, and requires only a few conditional lines of code: for example, a counter that activates the anomaly after a random number of interactions, or a timer that triggers misregistration within a narrow window, presenting the behavior as ordinary user error (mis-

tap, calibration drift, or capacitive-sensor noise). Because the logic executes silently and only a small percentage of the time, it evades routine logic-and-accuracy testing while cumulatively shifting vote totals in targeted precincts. When combined with other low-visibility tactics, this can materially alter outcomes without triggering detectable anomalies or paper-trail discrepancies in unaudited DRE deployments.

- Security researchers have replicated far more advanced manipulation. At DEF CON Voting Village, participants with ordinary tools gained full control of multiple DRE and BMD models in minutes, enabling arbitrary vote alteration. Princeton and University of Michigan teams demonstrated malware for Diebold and ES&S systems that alters recorded votes or printed ballots only under specific conditions, remaining dormant during testing.
- Such code is trivial to embed by an inside bad-actor or once an attacker obtains physical or supply-chain access to the firmware. The sophistication lies in its deniability: every affected voter experiences what appears to be isolated human or hardware error. Without comprehensive paper ballots, independent audits, and risk-limiting audits, the mechanism remains undetectable at scale.

- Tabulation
  - Change definitions of ‘tabulation’ to legally allow early machine tabulation so long as it isn’t ‘human

readable’; this still fuels their feedback loop

- Logic and accuracy testing: tabulator test ballots are only vendor supplied with TEST in red ink which is not displayed on the digital ballot image during adjudication testing. This is a great way for the software to branch to a test-only code path (operate differently) during L&A testing vs normal tabulation during an election.
- Pre-load votes during early voting in order to establish a 50/50 ratio from the start to be able to stay under the radar as adjustments are made to counter real votes coming in from that point forward. (Colorado, Washington, etc.)
- Use different thickness ballot paper for different areas/voters
    - Use the thickness as excuse to determine which tabulators are used (Sacramento CA does this – they claim the ‘thin’ paper gets jammed in the Hi-Pro scanners, so they scan all the ‘thin’ ballots through the smaller desktop scanners – Mark Cook was told this first-hand)
    - Paper that is too thick used in BMD (Ballot Marking Devices) and tabulators may jam, allowing another path to segregate those ballots. This may have happened in AZ

- Print the ballot image slightly shrunk so citizens don’t notice it, but the tabulators would be unable to scan, causing them to be segregated and an excuse to ‘re-create’ them. (This happened in AZ)
- Print the ballot image lighter than normal so citizens don’t notice it, but the tabulators would be unable to scan, causing them to be segregated and an excuse to ‘re-create’ them. (This happened in AZ)

- Randomize the order of the ballots inside the batches, destroying the time-series recording of the order of ballots as they were scanned (manipulating evidence), making it impossible to determine patterns of manipulation. They also then increase the batch size to launder more ballots per batch. (Montgomery County TX)
- Someone could easily fill in undervotes in ballots to manipulate those races.
- Someone could easily fill in an overvote to cancel a vote (overvotes invalidate the entire race).
- Induce error into the system to obfuscate manipulation (ballot programming mistakes, printing mistakes, mis-spellings, etc. – these aren't all accidents)
- Change database outside of voting system software
- Incomplete tracking
- Incomplete logging
- Self-deleting logs
- Back doors
- Ability to be connected to alternate networks (including the internet)
- Wireless devices installed in hardware
- No visibility to the public
- Secret source code
- Incomplete verifiability
- No way to guarantee they will always operate without error/abuse
- Block all access to ballot images and paper ballots
- Wipe hard drives to ensure no evidence of manipulation is left
- No supply-chain control or controllable chain of custody
- Manipulate programming on thumb/flash drives

- Pre-load votes on thumb/flash drives
- Manipulate votes on thumb/flash drives
- Disable and/or manipulate ballot images on thumb/flash drives
- Broken physical seals destroying chain of custody of the physical ballots
- Mix up thumb/flash drives to cause confusion to inhibit proper audit
- Thumb/flash drives can be easily modified by bad actors in-transit. Some may claim that can't happen because they are 'encrypted'. But those that have the encryption key can get away with it without anyone knowing, and if they are encrypted, nobody may be able to detect modification.
    - For instance, encryption keys for Dominion are stored in cleartext inside the database, and the same keys can be used across different counties, states, or all over the world. The keys can also be stored in accessible folders in the filesystem, and obtainable through side-channel vectors.

- Disable digital images of ballots to be able to thwart their use that evidence in an audit
- Manipulate digital images of the ballots in cases where digital images are made
- THERE IS NO WAY TO SECURE THESE SYSTEMS IN ANY WAY
- Dominion claimed that the existing systems cannot handle a future sized ballot and therefore, the county needed to 'upgrade' (Rio Grande County, CO)

- Reporting
    - Election officials don't even know what really

happens to their totals when they leave
- Totals can be changed and hidden inside aggregation without the public able to detect
- No guarantee to the public that the shown state/fed totals are actually accurate
- No public place that all totals are transparently and additionally posted
- Centralization of results makes it difficult if not impossible to detect fraud. For insurance, Michigan no longer denotes the difference between

- Records
  - Purposely misinterpret the 22-month minimum federal retention period to restrict access to election records for 22 months. That is not the purpose of the minimum retention period. The purpose of the retention period is to make sure the data is RETAINED for the time period so that people can look at it. I believe there is a legal case in some stage regarding setting the record straight on that.
  - Blocked, or complicated, access to cast vote records (CVRs) which can be used to identify many patterns of manipulation
    - They put CVR out as JSON format to make it too complex for the average person to examine the data.
    - They print out the CVR as a PDF to create an additional barrier to easily examine the data.

  - Push citizens to the point they have to file lawsuit to get access to records, then claim they can’t provide access to records due to pending lawsuit.
  - Even some republican states (e.g., South Dakota,

South Carolina) have not provided CVRs.
    - They randomize CVR data claiming that they must do so in order to protect voter privacy. The randomization destroys the time-series aspect of the CVR and therefore cripples their effectiveness at detecting manipulation. Not to mention, this is TAMPERING WITH EVIDENCE at the best, and DESTRUCTION OF EVIDENCE and ELECTION RECORDS at the worst.
    - No access to security logs, has testing, penetration testing, ballot review files

- Certification
    - Forcing certification to be procedurally automatic instead of only happening if evidence supports doing so. This is how they SEAL THE FRAUD!

- Auditing
    - ‘Risk Limiting Audits’ or ‘Partial Manual Counts’ are used to justify auditing only a small portion to convince the public the rest of the tabulation is accurate.
    - Engineered to avoid catching the fraud (easy to do when fraud is algorithmic).
    - Some recount procedures cause the ballot order within batches to be broken. This can unintentionally negatively affect the effectiveness of other audits that rely on order being preserved (to compare with other counts or temporal examinations)
    - Some states redefine what their ‘audit’ is to cripple and make it worthless.

- Canvassing

        - They attempt to claim that citizen canvassing efforts cause voter intimidation

- Recalls
    - Fake recall booths are set up, then sigs are thrown out.
    - Fake recall groups/orgs are set up, then conveniently miss deadlines or make mistakes that invalidate the recall.

- Election Contest
    - Implement a ridiculously short period of time to file a contest, to guarantee that there is not adequate time to investigate the data.

Conclusion: How the Entire System Fits Together

This comprehensive list illustrates a multi-layered, interconnected ecosystem of election manipulation tactics that operate like a sophisticated machine, designed to undermine democratic processes from inception to certification. It begins with psychological operations and perception framing to erode public trust and suppress visible support, creating a fertile ground for infiltration and institutional capture where controlled opposition diverts resources and spies from within. Financial and candidate manipulations ensure only compliant or compromised figures advance, reinforced by legislative barriers that embed vulnerabilities into law while legal tactics delay or block accountability. Demographic and registration exploits inflate voter rolls as a foundation for fraud, enabling

procedural interferences that limit oversight and participation. Extended voting methods like early and mail-in ballots provide real-time data for precise injections via harvesting and chain-of-custody breaks, while physical ballot flaws and technological backdoors allow undetected alterations during tabulation and reporting. Finally, the end-to-end framework—epitomized by feedback loops and weakened audits—seals the results, distributing manipulations subtly to evade detection. Together, these elements form a self-reinforcing cycle that centralizes control, decentralizes blame, and perpetuates fraud under the guise of security and accessibility, ultimately disenfranchising citizens and eroding electoral integrity.

The Solution

The PEP

The Declaration