

Busting the Paper Ballot: Voting Meets Adversarial ML



Image source: ChatGPT.

Aayushi Verma (University of Connecticut)

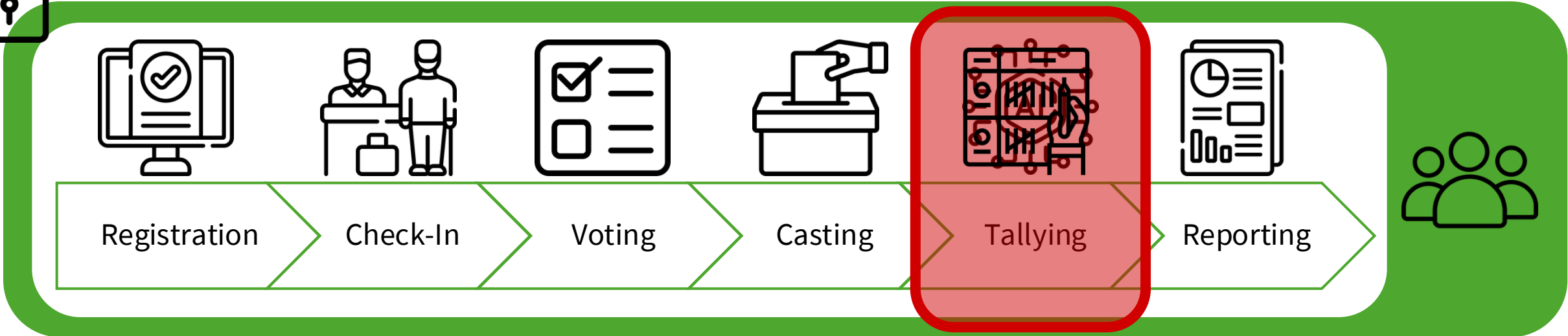
Joint work with: Kaleel Mahmood, Caleb Manicke, Ethan Rathbun, Nicholas Stamatakis, Sohaib Ahmad, Benjamin Fuller, Laurent Michel

Just a *few* **tampered** ballots can
swing a **close** election.

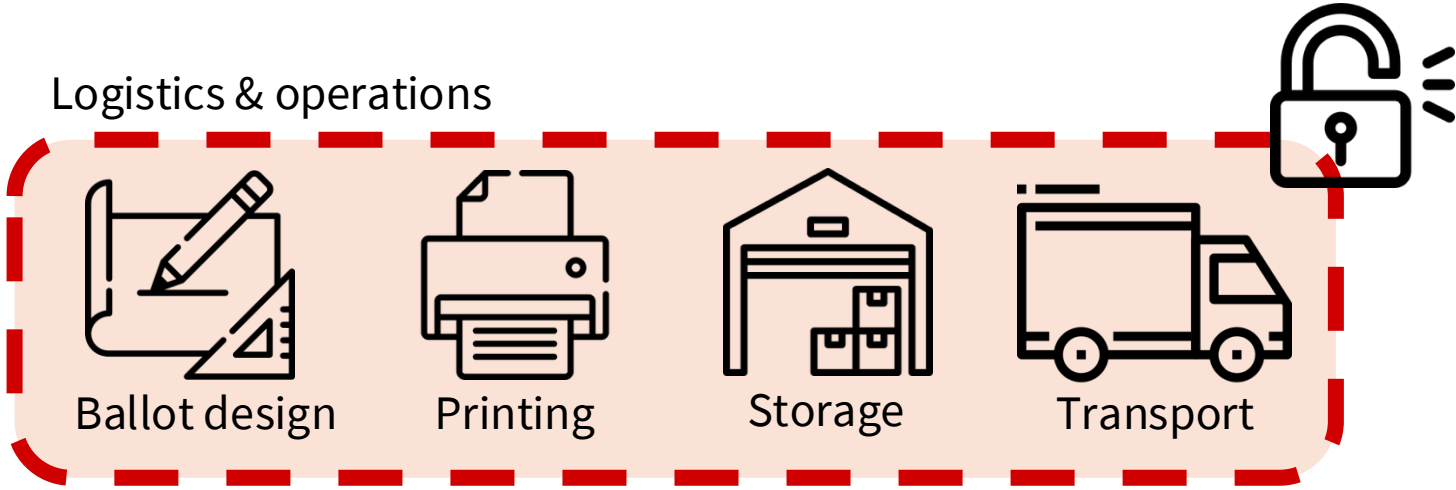
This is a **cautionary** tale about using machine learning in **critical** systems.

Disclaimer: The images of ballots in this presentation are for illustrative purposes only. They are not intended as endorsements of any candidate, political party, or policy. All tested models are entirely created by our team for research purposes and are not intended to represent any vendor product(s).

This is our threat model and adversary.



Logistics & operations



- ✓ Full **knowledge** of ML system (but no access)
- ✓ **Access** to physical pipeline.

Visual representation of attack.



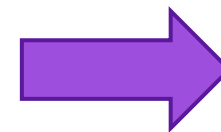
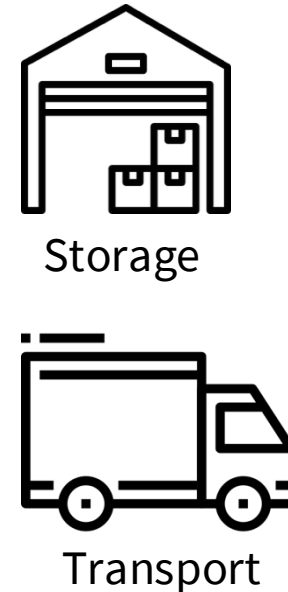
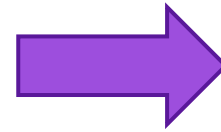
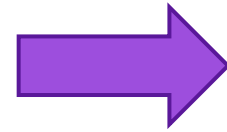
- **Goal:** real Loser wins by at least 0.5%.
- **Attack:** create enough tampered ballots, mix with real ballots, watch chaos unfold.

State of Connecticut Official Ballot
Mansfield Connecticut State Election November 3, 2020
Page 1 of 1
Congressional District 2
Senatorial District 29
Assembly District 54
Voting Districts 1

VOTE ON THE QUESTION(S)
YES NO
1. "SHALL THE TOWN OF MANSFIELD APPROPRIATE \$2,000,000 FOR COSTS WITH RESPECT TO ROOF REPLACEMENT AND PHOTOVOLTAIC SYSTEM INSTALLATION AT MANSFIELD MIDDLE SCHOOL, AND AUTHORIZE THE ISSUE OF BONDS AND NOTES TO FINANCE THE PORTION OF THE APPROPRIATION NOT DEPAID FROM GRANTS?"

| OFFICE | 1 PRESIDENTIAL ELECTOR FOR TWO YEAR TERM | 2 REPRESENTATIVE IN CONGRESS FOR ONE YEAR TERM | 3 STATE SENATOR FOR ONE YEAR TERM | 4 STATE REPRESENTATIVE FOR ONE YEAR TERM | 5 REGISTER OF VOTING FOR ONE YEAR TERM |
|------------------------|---|---|--------------------------------------|---|---|
| DEMOCRATIC PARTY | 1A BRIAN AND HARRIS JOE COURSEY MAE FLECK GREG HASKAN RANE GREINER | 2A JOE COURSEY | 3A MAE FLECK | 4A GREG HASKAN | 5A RANE GREINER |
| REPUBLICAN PARTY | 1B TOMMY AND FINCH | 2B JUSTIN ANDERSON | 3B JESSICA ALBA | 4B VINA STARKS WARD | 5B |
| INDEPENDENT PARTY | 1C | 2C JESSICA ALBA | 3C | 4C | 5C |
| WORKING FAMILIES PARTY | 1D JOE COURSEY | 2D MAE FLECK | 3D GREG HASKAN | 4D | 5D |
| LIBERTARIAN PARTY | 1E JOSHUA AND COHEN | 2E DANIEL STALE | 3E | 4E | 5E |
| GREEN PARTY | 1F HANNAH AND WALSH | 2F CASANDRA MATRICCHI | 3F | 4F | 5F |
| WRITE-IN VOTES | 1G | 2G | 3G | 4G | 5G |

Be sure to read the instructions on the reverse side of this ballot.



Real Loser → more votes
Real Winner → less votes

Election flipped!

Attack happens *before* election day.

Votes are classified by individual bubbles.

State of Connecticut Official Ballot

Mansfield Connecticut State Election November 3, 2020

Congressional District 2
Senatorial District 29
Assembly District 54
Voting Districts 1

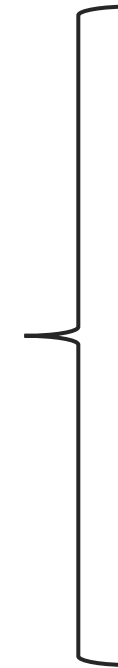
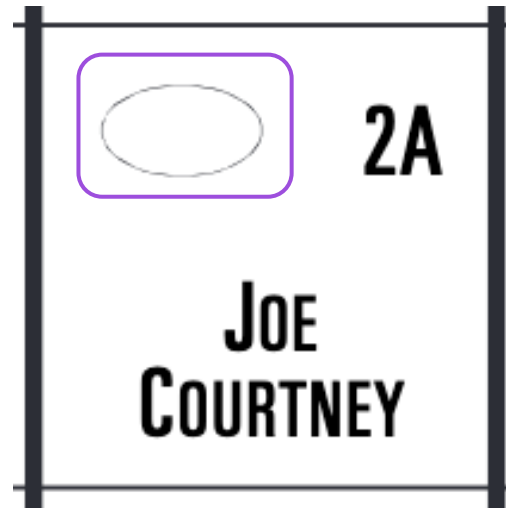
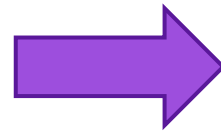
Page 1 of 1

VOTE ON THE QUESTION(S)
YES NO
1. "SHALL THE TOWN OF MANSFIELD APPROPRIATE \$2,800,000 FOR COSTS WITH RESPECT TO ROOF REPLACEMENT AND PHOTOVOLTAIC SYSTEM INSTALLATION AT MANSFIELD MIDDLE SCHOOL, AND AUTHORIZE THE ISSUE OF BONDS AND NOTES TO FINANCE THE PORTION OF THE APPROPRIATION NOT DEFRAYED FROM GRANTS?"

| OFFICE | 1 PRESIDENTIAL ELECTORS FOR VOTE FOR ONE | 2 REPRESENTATIVE IN CONGRESS VOTE FOR ONE | 3 STATE SENATOR VOTE FOR ONE | 4 STATE REPRESENTATIVE VOTE FOR ONE | 5 REGISTRAR OF VOTERS VOTE FOR ONE |
|------------------------|---|--|---------------------------------|--|---------------------------------------|
| DEMOCRATIC PARTY | 1A BIDEN AND HARRIS | 2A JOE COURTNEY | 3A MAE FLEXER | 4A GREGG HADDAD | 5A ANNE GREINER |
| REPUBLICAN PARTY | 1B TRUMP AND PENCE | 2B JUSTIN ANDERSON | 3B JESSICA ALBA | 4B VERA STEARNS WARD | 5B |
| INDEPENDENT PARTY | 1C | 2C | 3C JESSICA ALBA | 4C | 5C |
| WORKING FAMILIES PARTY | 1D | 2D JOE COURTNEY | 3D MAE FLEXER | 4D GREGG HADDAD | 5D |
| LIBERTARIAN PARTY | 1E JURIGENEN AND COHEN | 2E DANIEL RIZALE | 3E | 4E | 5E |
| GREEN PARTY | 1F HAWKINS AND WALKER | 2F CASSANDRA MARTINEAU | 3F | 4F | 5F |
| WRITE-IN VOTES | 1G | 2G | 3G | 4G | 5G |

Be sure to read the instructions on the reverse side of this ballot.

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32



Empty bubble = non-vote

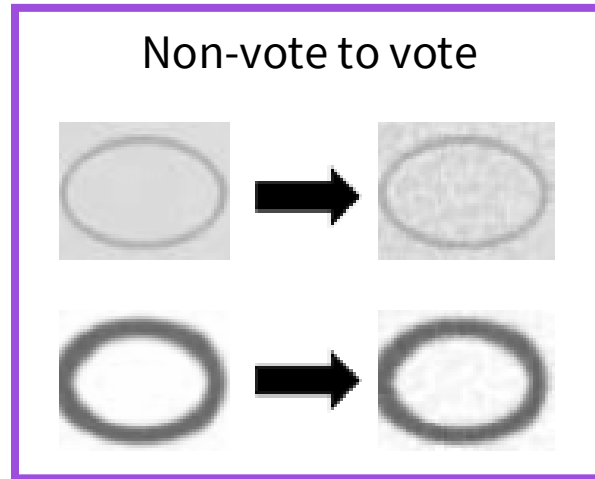


Marked bubble = vote

Binary image classification problem!

Attack Phase One: adversarial images to fool classifier.

Goal: human-*imperceptibility*.

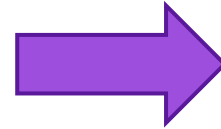
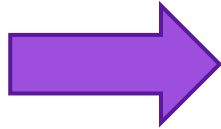
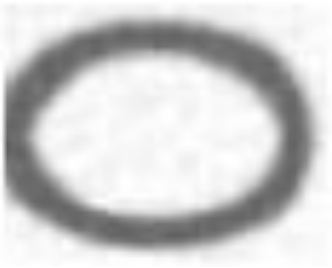


Attack specs:

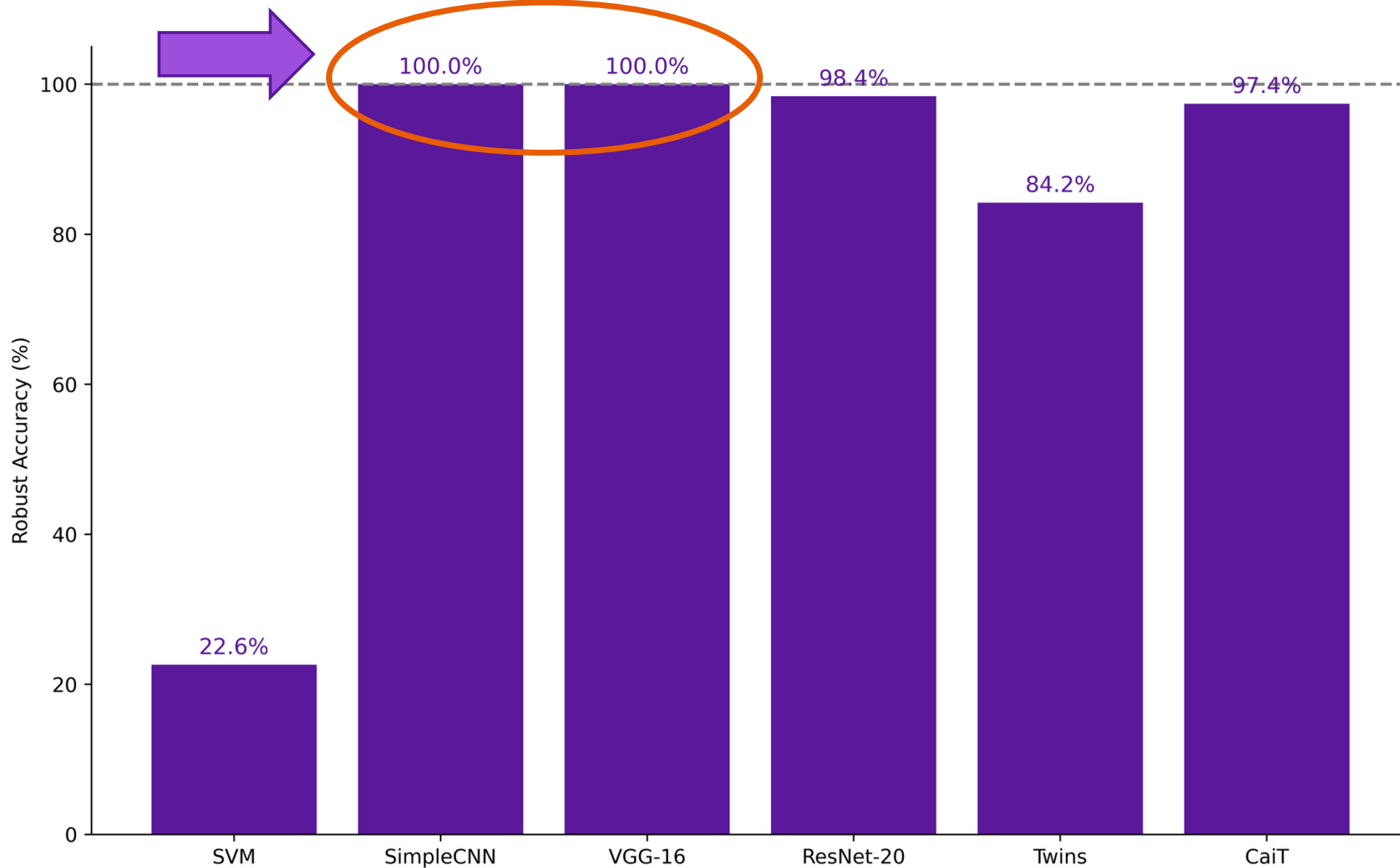
- APGD (Auto-Projected Gradient Descent)
- L_∞ norm
- DLR loss
- $\epsilon = 8/255$

Attack Phase Two: print tampered ballots (simulated).

Adversarial
bubbles



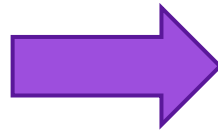
Not all models can resist this physical attack.



This is just a baseline – attacks only get better!

Adversary needs *just 1* successful example.

Adversarial bubble



State of Connecticut Official Ballot

Mansfield Connecticut

State Election

November 3, 2020

Page 1 of 1

Congressional District 2
Senatorial District 29
Assembly District 54
Voting Districts 1

VOTE ON THE QUESTION(S)

YES NO

1. "SHALL THE TOWN OF MANSFIELD APPROPRIATE \$2,800,000 FOR COSTS WITH RESPECT TO ROOF REPLACEMENT AND PHOTOVOLTAIC SYSTEM INSTALLATION AT MANSFIELD MIDDLE SCHOOL, AND AUTHORIZE THE ISSUE OF BONDS AND NOTES TO FINANCE THE PORTION OF THE APPROPRIATION NOT DEFRAID FROM GRANTS?"

| OFFICE | 1 PRESIDENTIAL ELECTORS FOR VOTE FOR ONE | 2 REPRESENTATIVE IN CONGRESS VOTE FOR ONE | 3 STATE SENATOR VOTE FOR ONE | 4 STATE REPRESENTATIVE VOTE FOR ONE | 5 REGISTRAR OF VOTERS VOTE FOR ONE |
|------------------------|---|---|---|---|---|
| DEMOCRATIC PARTY | <input type="radio"/> 1A BIDEN AND HARRIS | <input type="radio"/> 2A JOE COURTNEY | <input checked="" type="radio"/> 3A MAE FLEKER | <input checked="" type="radio"/> 4A GREGG HADDAD | <input type="radio"/> 5A ANNE GREINER |
| REPUBLICAN PARTY | <input type="radio"/> 1B TRUMP AND PENCE | <input type="radio"/> 2B JUSTIN ANDERSON | <input type="radio"/> 3B JESSICA ALBA | <input type="radio"/> 4B | <input type="radio"/> 5B VERA STEARNS WARD |
| INDEPENDENT PARTY | <input type="radio"/> 1C | <input type="radio"/> 2C | <input type="radio"/> 3C JESSICA ALBA | <input type="radio"/> 4C | <input type="radio"/> 5C |
| WORKING FAMILIES PARTY | <input type="radio"/> 1D | <input type="radio"/> 2D JOE COURTNEY | <input type="radio"/> 3D MAE FLEKER | <input type="radio"/> 4D GREGG HADDAD | <input type="radio"/> 5D |
| LIBERTARIAN PARTY | <input type="radio"/> 1E JORGENSEN AND COHEN | <input type="radio"/> 2E DANIEL REALE | <input type="radio"/> 3E | <input type="radio"/> 4E | <input type="radio"/> 5E |
| GREEN PARTY | <input type="radio"/> 1F HAWKINS AND WALKER | <input type="radio"/> 2F CASSANDRA MARTINEAU | <input type="radio"/> 3F | <input type="radio"/> 4F | <input type="radio"/> 5F |
| WRITE-IN VOTES | <input type="radio"/> 1G | <input type="radio"/> 2G | <input type="radio"/> 3G | <input type="radio"/> 4G | <input type="radio"/> 5G |

Be sure to read the instructions on the reverse side of this ballot.

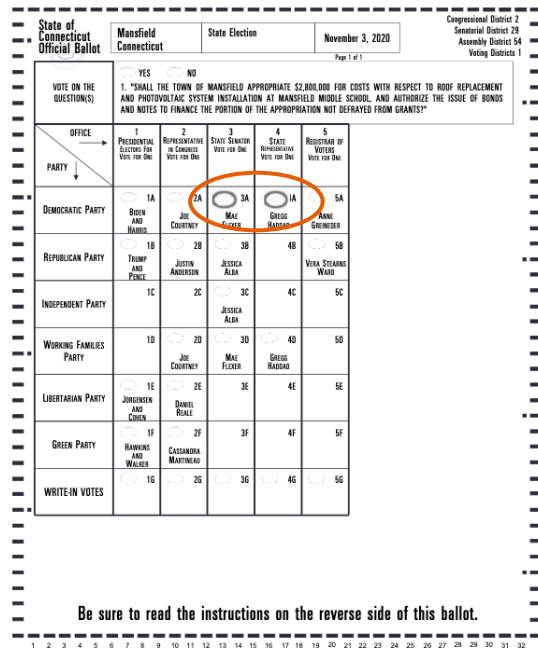
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32



Adversarial ballots can change the margin by 2.5%.



Election day scenario:

- Local, 2-party race
- Tight margin of 2%
- 12% of ballots left blank
- Mail-in ballots only



Race left empty →  

Vote for preferred candidate →  

Voted for opponent → overvote*.  

*typically. Other possibilities: new ballot requested, ballot nullified.

| | Real Results | Adversarial Interference |
|-------------|--------------|--------------------------|
| Real Loser | 0.395 (-2%) | 0.407 (+0.5%) |
| Real Winner | 0.415 | 0.402 |

Final Takeaways

Just a *few* **tampered** ballots can **swing** a **close** election.

ML in voting → risky!

For trusted election security:

- NEVER replace humans in the loop!
- View physical world pipeline as part of defense.
- More transparency, and shared models/data!

Request to community:
How can we better defend these models for trustworthiness?



Thank you! Check out our work here:



Aayushi Verma

PhD student @UConn

 aayushi.verma@uconn.edu

 [awesomecosmos](#)



Paper pre-print

arxiv.org/abs/2506.14582



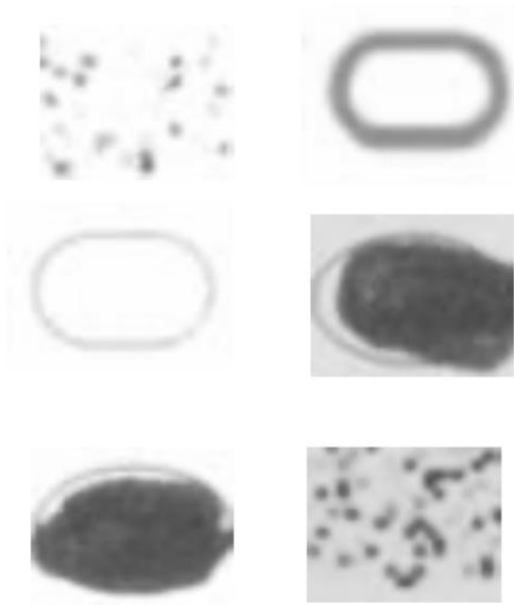
Dataset v1

zenodo.org/records/15458710

(v2 coming soon!)

Backup Slides for Q&A

Dataset for model training matters.



Our current dataset with synthetic 'swatch' marks, designed to be close to the boundary.

Our upcoming dataset with realistic marginal marks.

