

A stylized, monochromatic American flag in shades of gray, featuring a field of stars in the upper left and horizontal stripes across the rest of the page.

# Election Cybersecurity

## 2018 Progress Report

J. Alex Halderman  
University of Michigan

# Flashback: 2016 U.S. Presidential Election

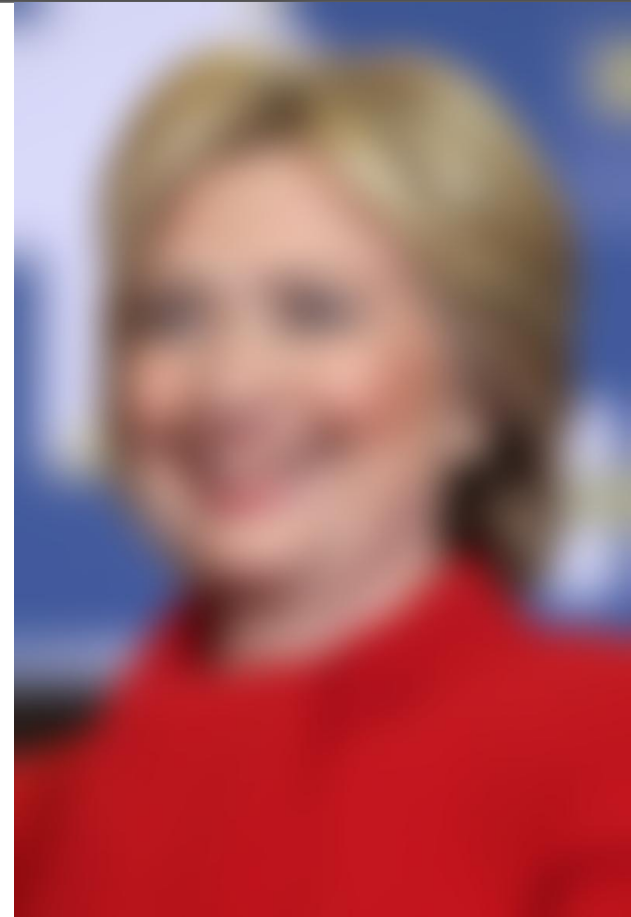


**November 8, 2016**

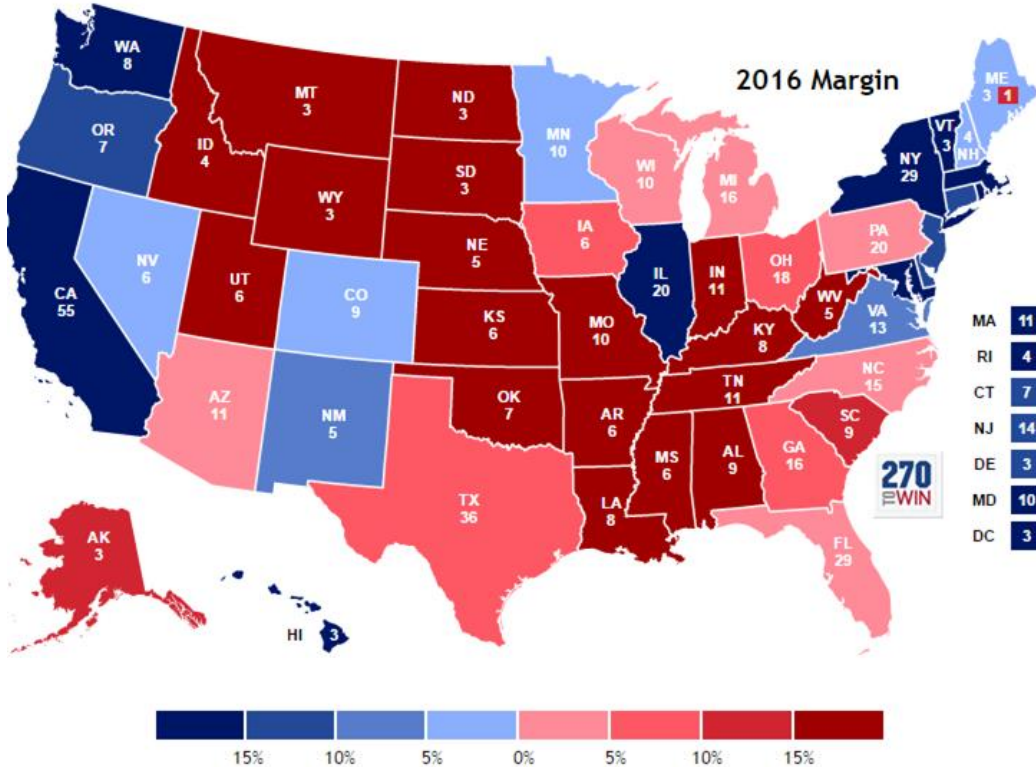
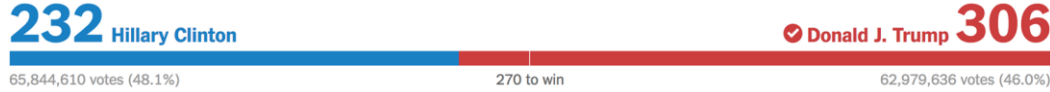


**Donald Trump**  
Republican

**(Opponent)**  
Democrat



# How Close was the 2016 Election?



Trump received nearly 3 million fewer votes, but won the **electoral college**.

How many votes would need to be **changed** to tie?

MI	5,352 (0.1%)	Any Two
PA	22,146 (0.4%)	
FL	56,455 (0.6%)	Any Three States
WI	11,374 (0.4%)	
AZ	45,617 (1.8%)	
NC	86,657 (1.8%)	

**27,500** of 137 million (0.02%)

# Flashback: 2016 Election Recounts



RECOUNT2016 ▾ MI RECOUNT ▾ PA RECOUNT ▾ WI RECOUNT ▾ MEET JILL ▾ NEWS ▾ THE GREEN FUTURE DONATE

SIGN IN: TWITTER FACEBOOK EMAIL ESPANOL

\$7,179,903.48 RAISED

GOAL: \$9,500,000.00



## Wisconsin

Recounted statewide, though not all by hand

No evidence of fraud

## Michigan

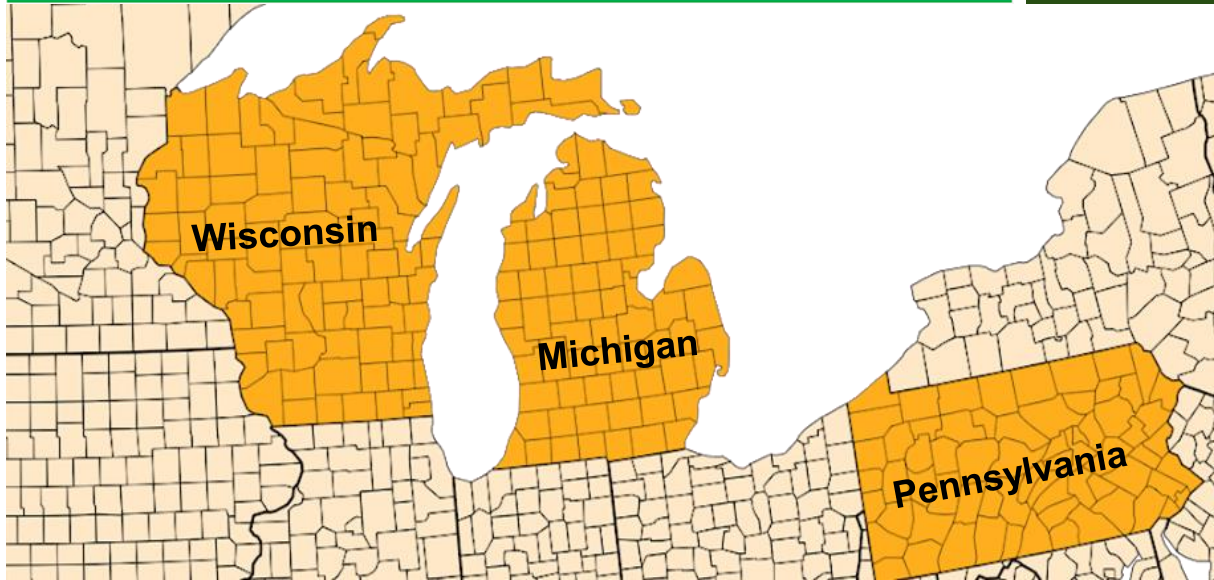
Halted by court with only 43% of votes recounted

No evidence of fraud

## Pennsylvania

Most counties didn't or couldn't recount

No evidence of fraud





What Happened in **2016**?

# 2016 Russian Election Interference

Confident assessment of U.S. intelligence is that **Vladimir Putin** ordered influence operations to **weaken Clinton, boost Trump, and discredit electoral process.**

A “**significant escalation**” of “longstanding Russian efforts to undermine the U.S.-led liberal democratic order”

This report is a declassified version of a highly classified assessment; its conclusions are identical to those in the highly classified assessment but this version does not include the full supporting information on key elements of the influence campaign.



ICA  
INTELLIGENCE COMMUNITY ASSESSMENT

## Assessing Russian Activities and Intentions in Recent US Elections

### Key Judgments

Russian efforts to influence the 2016 US presidential election represent the most recent expression of Moscow's longstanding desire to undermine the US-led liberal democratic order, but these activities demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations.

We assess Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency. We further assess Putin and the Russian Government developed a clear preference for President-elect Trump. We have high confidence in these judgments.

- We also assess Putin and the Russian Government aspired to help President-elect Trump's election chances when possible by discrediting Secretary Clinton and publicly contrasting her unfavorably to him. All three agencies agree with this judgment. CIA and FBI have high confidence in this judgment; NSA has moderate confidence.

# Precedent: 2014 Ukrainian Presidential Election

## Targeted political leaks

Stolen emails leaked online

## Attacks on vote reporting

Hacked Election Commission servers to display wrong result, narrowly averted

## DDoS attacks

Attempt to delay final result



The screenshot shows the top portion of a news article. At the top, the logo for 'The CHRISTIAN SCIENCE MONITOR' is displayed in white on a dark background. To the right of the logo are links for 'Log In | Register' and 'FREE E-mail Newsletters'. Below the logo, the text 'breakfast | EqualEd' is visible. The main headline of the article is 'Ukraine election narrowly avoided 'wanton destruction' from hackers'. Below the headline is a sub-headline: 'A brazen three-pronged cyber-attack against last month's Ukrainian presidential elections has set the world on notice – and bears Russian fingerprints, some say.' The author information reads 'By Mark Clayton, Staff writer | JUNE 17, 2014'. To the right of the author information is a 'Save for later' button with a bookmark icon. The first paragraph of the article text is: 'A three-pronged wave of cyber-attacks aimed at wrecking Ukraine's presidential vote – including an attempt to fake computer vote totals – was narrowly defeated by government cyber experts, Ukrainian officials say.'

WORLD | PASSCODE

## Ukraine election narrowly avoided 'wanton destruction' from hackers

A brazen three-pronged cyber-attack against last month's Ukrainian presidential elections has set the world on notice – and bears Russian fingerprints, some say.

By Mark Clayton, Staff writer | JUNE 17, 2014

Save for later

A three-pronged wave of cyber-attacks aimed at wrecking Ukraine's presidential vote – including an attempt to fake computer vote totals – was narrowly defeated by government cyber experts, Ukrainian officials say.

The still little-known hacks, which surfaced May 22-26, appear to be among the most dangerous cyber-attacks yet deployed to sabotage a national election – and a warning shot for future elections in the US and abroad, political scientists and cyber experts say.

# 2016 Russian Interference in the U.S.

## **Targeted political leaks**

Stolen emails leaked online

## **Trolling/message amplification**

Propaganda and political discord

## **Attacking election infrastructure**

Registration systems and vendors



# 2016 Russian Interference in the U.S.

## Targeted political leaks


Stolen emails leaked online

## Trolling/message amplification

Propaganda and political discord

## Attacking election infrastructure

Registration systems and vendors



The image is a composite graphic. On the left, a cartoon depicts a woman with blonde hair sitting at a laptop. Above her are thought bubbles containing dollar signs and stacks of money. To her left is a stylized hourglass with a globe as the top bulb and another globe as the bottom bulb. The text 'WikiLeaks' is written in a blue box at the bottom left of the cartoon. A signature 'LAFSE 2016 WIKILEAKS' is visible. On the right, a red banner contains the text 'BREAKING' in large white letters, followed by 'New Hillary Leaks Series' in smaller white text. Below this, in large white font, it reads 'Wikileaks releases 19,252 DNC Emails'.



The navigation bar of the WikiLeaks website. It features the WikiLeaks logo (an hourglass with a globe) and the text 'WikiLeaks' on the left. On the right, there are two buttons: 'Shop' and 'Donate'.

Search

## The Podesta Emails

WikiLeaks series on deals involving Hillary Clinton campaign Chairman John Podesta. Mr Podesta is a long-term associate of the Clintons and was President Bill Clinton's Chief of Staff from 1998 until 2001. Mr Podesta also owns the Podesta Group with his brother Tony, a major lobbying firm and is the Chair of the



# 2016 Russian Interference in the U.S.

## Targeted political leaks

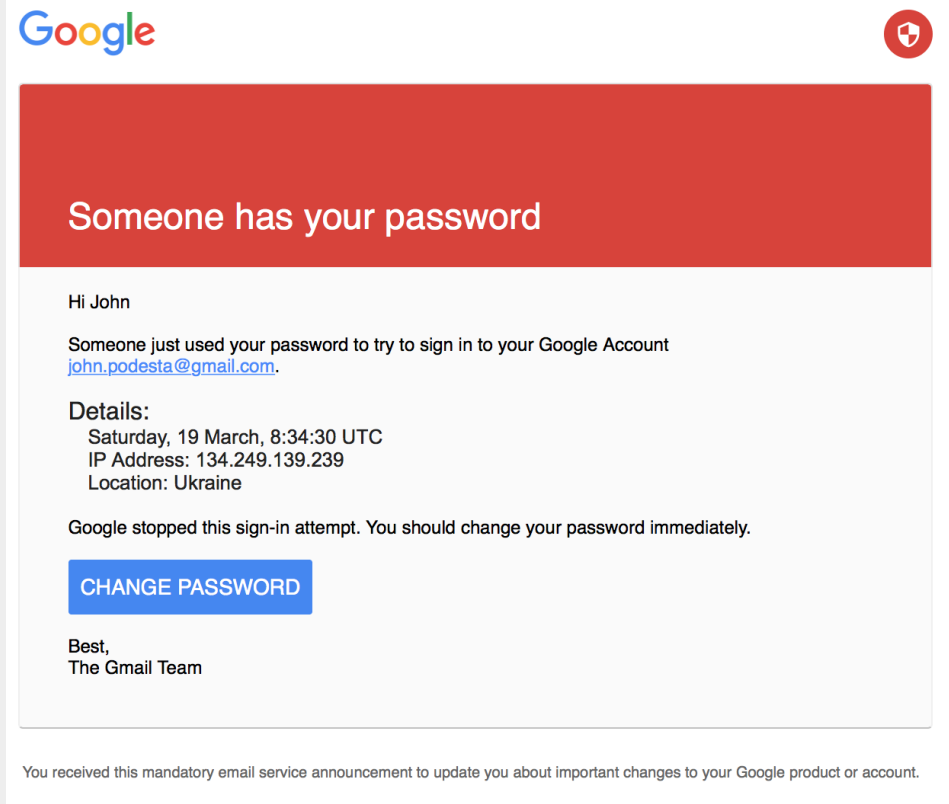
Stolen emails leaked online

## Trolling/message amplification

Propaganda and political discord

## Attacking election infrastructure

Registration systems and vendors



The image shows a screenshot of a security notification email from Google. At the top left is the Google logo, and at the top right is a red shield icon. Below the logo is a large red banner with the text "Someone has your password". The main body of the email is white and contains the following text: "Hi John", "Someone just used your password to try to sign in to your Google Account", and a blue link "john.podesta@gmail.com". Underneath, it says "Details:" followed by "Saturday, 19 March, 8:34:30 UTC", "IP Address: 134.249.139.239", and "Location: Ukraine". A blue button labeled "CHANGE PASSWORD" is positioned below the details. The email concludes with "Google stopped this sign-in attempt. You should change your password immediately." and "Best, The Gmail Team". At the bottom of the email, there is a small line of text: "You received this mandatory email service announcement to update you about important changes to your Google product or account."

# 2016 Russian Interference in the U.S.

## Targeted political leaks

Stolen emails leaked online

## Trolling/message amplification

Propaganda and political discord

## Attacking election infrastructure

Registration systems and vendors



Melvin Redick ▸ BREAKING NEWS - WORLD

June 8, 2016 · 🌐

These guys show hidden truth about Hillary Clinton, George Soros and other leaders of the US. Visit #DCLeaks website. It's really interesting!  
<http://dcleaks.com/>



👍 Like

➦ Share

👍 1

# 2016 Russian Interference in the U.S.

## Targeted political leaks

Stolen emails leaked online

## Trolling/message amplification

Propaganda and political discord

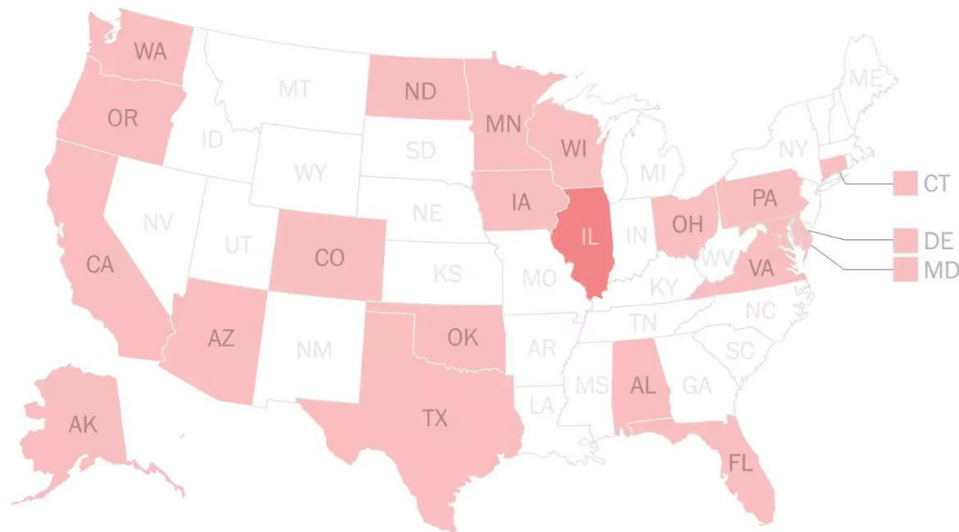
## Attacking election infrastructure

Registration systems and vendors

- Up to 21 states probed
- Multiple states infiltrated (SQL injection, etc.) and Registration data exfiltrated

### States notified by DHS of Russian hacking attempts

● Breached ● Sorta breached ● Targeted ○ Not notified of targeting



Source: News reports and public statements

THE FIX

# 2016 Russian Interference in the U.S.

TOP SECRET//SI//ORCON/REL TO USA, FVEY/FISA



## National Security Agency

(TS//SI//OC/REL TO USA, FVEY/FISA) Russian General Staff Main Intelligence Directorate actors [REDACTED] [REDACTED] executed cyber espionage operations against a named U.S. Company in August 2016, evidently to obtain information on elections-related software and hardware solutions, according to information that became available in April 2017. The actors likely used data obtained from that operation to create a new email account and launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations. The spear-phishing emails contained a Microsoft Word document trojanized with a Visual Basic script which, when opened, would spawn a PowerShell instance that was potentially used to offer election-related products and services, presumably to U.S.-based targets. Lastly, the actors sent test emails to two non-existent accounts ostensibly associated with absentee balloting, presumably with the purpose of creating those accounts to mimic legitimate services.

**Campaign Against U.S. Company 1 and Voter Registration-Themed Phishing of U.S. Local Government Officials (S//SI//REL TO USA, FVEY/FISA)**



**Reality Winner**  
NSA contractor

# Special Counsel Investigation

In July 2018, prospectors indicted GRU officers in connection with the email theft, registration system attacks, and attempts to phish local election officials.

More to come?

## COUNT ELEVEN

### **(Conspiracy to Commit an Offense Against the United States)**

68. Defendant ANATOLIY SERGEYEVICH KOVALEV (Ковалев Анатолий Сергеевич) was an officer in the Russian military assigned to Unit 74455 who worked in the GRU's 22 Kirova Street building (the Tower).

69. Defendants OSADCHUK and KOVALEV were GRU officers who knowingly and intentionally conspired with each other and with persons, known and unknown to the Grand Jury, to hack into the computers of U.S. persons and entities responsible for the administration of 2016 U.S. elections, such as state boards of elections, secretaries of state, and U.S. companies that supplied software and other technology related to the administration of U.S. elections.

### **Object of the Conspiracy**

70. The object of the conspiracy was to hack into protected computers of persons and entities charged with the administration of the 2016 U.S. elections in order to access those computers and steal voter data and other information stored on those computers.



What Happened in **2018**?

# So what happened in 2018 ... ?

- Continued social media influence operations  
U.S. intel claims Russia, China, Iran involved



US POLITICS

## US Intelligence Report: Russia, China, Iran Sought to Influence 2018 Elections

December 21, 2018 5:40 PM

[Jeff Seldin](#)

WASHINGTON — Russia, China and Iran sought to meddle in the recent U.S. midterm election, but their actions did not compromise the "nation's election infrastructure that would have prevented voting, changed vote counts, or disrupted the ability to tally votes," according to a report released Friday by the Office of the Director of National Intelligence.

Director Dan Coats said U.S. intelligence did find "Russia, and other foreign countries, including China and Iran, conducted influence activities and messaging campaigns targeted at the United States to promote their strategic interests."

But he said the intelligence community "did not make an assessment of the impact that these activities had on the outcome of the 2018 election."



# So what happened in 2018 ... ?

- Continued social media influence operations  
U.S. intel claims Russia, China, Iran involved
- Sporadic voting machine breakdowns,  
with apparently natural causes

## 🗳️ NEW YORK

### **What Went Wrong at New York City Polling Places? It Was Something in the Air. Literally.**

There was almost 100 percent humidity and unusually high precipitation in the five boroughs, not exactly perfect for a widely used ballot scanner. According to its technical documents, the scanner becomes downright uncomfortable when the weather turns sweaty.

by Ian MacDougall, Nov. 6, 9:23 p.m. EST

# So what happened in 2018 ... ?

- Continued social media influence operations  
U.S. intel claims Russia, China, Iran involved
- Sporadic voting machine breakdowns,  
with apparently natural causes
- Ballot usability problems in Florida, again  
In Broward county, 3.7% fewer votes were cast  
for Senate than for governor (26,000 votes).  
The election was decided by 10,033 votes.

Governor

Ballot Style 58		Seq:058
Official General Election Ballot November 6, 2018 Broward County, Florida	Boleta Oficial De La Elección General Noviembre Del 2018 Condado de Broward, Florida	Ofisyèl Jeneral Eleksyon 6 Novanm 2018 Konte Broward, Florid
<b>Ballot Instructions:</b> <ul style="list-style-type: none"> <li>To vote, fill in the oval completely next to your choice. Use only the marking device provided or a black pen.</li> <li>If you make a mistake, ask the poll worker. Do not cross out or your vote may not count.</li> <li>To vote for a write-in candidate, fill in the oval and print the name clearly on the blank line provided by the write-in candidate.</li> </ul>	<b>Governor and Lieutenant Governor Gouvernè Ak Lyetnan Gouvernè (Vote for One/Vote por Uno/Vote pou Youn)</b> <ul style="list-style-type: none"> <li><input type="radio"/> Ron DeSantis Jeanette Nufez REP</li> <li><input type="radio"/> Andrew Gillum Chris King DEM</li> <li><input type="radio"/> Darcy G. Richardson Nancy Argenziano REP</li> <li><input type="radio"/> Kyle Richardson Ellen Wilds NPA</li> <li><input type="radio"/> Ryan Christopher Foley John Tutton Jr NPA</li> <li><input type="radio"/> Bruce Stanley Ryan Howard McJury NPA</li> <li><input type="radio"/> Write-in/Escribir/A lekri</li> </ul>	<b>Fourth District Court of Appeal Tribunal De Apelaciones Del Cuarto Distrito</b> <p>Shall Judge Burton C. Conner of the Fourth District Court of Appeal be retained in office?</p> <p>¿Deberá retenerse en su cargo al Juez Burton C. Conner del Tribunal del Cuarto Distrito de Apelaciones?</p> <p>Èske se pou jis Burton C. Conner nan katyèm distrik lakou dapèl rete nan pòs li a?</p> <p><input type="radio"/> Yes/Si/Wi <input type="radio"/> No/No/Non</p>
<b>Instrucciones Para La Boleta:</b> <ul style="list-style-type: none"> <li>Para votar, llene completamente el óvalo junto a su selección. Use sólo un lápiz de punta negra o una pluma de tinta negra para marcar la boleta.</li> <li>Si se equivoca, pida una nueva boleta. Si borra algo o hace marcas, es posible que su voto no se cuente.</li> <li>Para Votar por un candidato cuyo nombre no está impreso en la boleta, llene el óvalo y escriba el nombre del candidato en la línea en blanco provista para un candidato agregado.</li> </ul>	<b>Attorney General Fiscal General Pwokirè Jeneral (Vote for One/Vote por Uno/Vote pou Youn)</b> <ul style="list-style-type: none"> <li><input type="radio"/> Ashley Moody REP</li> <li><input type="radio"/> Sean Shaw DEM</li> <li><input type="radio"/> Jeffrey Marc Siskind NPA</li> </ul>	<p>Shall Judge Jeffrey T. Kuntz of the Fourth District Court of Appeal be retained in office?</p> <p>¿Deberá retenerse en su cargo al Juez Jeffrey T. Kuntz del Tribunal del Cuarto Distrito de Apelaciones?</p> <p>Èske se pou jis Jeffrey T. Kuntz nan katyèm distrik lakou dapèl rete nan pòs li a?</p> <p><input type="radio"/> Yes/Si/Wi <input type="radio"/> No/No/Non</p>
<b>Enfòmasyon Sou Bilten Vot:</b> <ul style="list-style-type: none"> <li>Pou vote, byen kolore tout andan oval ak ekote respons ou chwazi a. Sèlman sévi ak yon plim nwa oubyen ak yon kreyon pou ekri sou bilten vòt la.</li> <li>Si w fè yon erè, mande yo ba w yon nouvo bilten vò. Si w efase oubyen fè novuo mak, I ap posib pou vòt ou pa valab ankò.</li> <li>Pou vote pou yon kandida ki pa gen non l enprime sou bilten vòt la, kolore ti oval la ak epi ekri non kandida a sou liy vid la rezève pou ekri</li> </ul>	<b>Chief Financial Officer Controlador Estatal Chéf Ofisyè Finans (Vote for One/Vote por Uno/Vote pou Youn)</b>	<p>Shall Judge Carole Y. Taylor of the Fourth District Court of Appeal be retained in office?</p>

# So what happened in 2018 ... ?

- Continued social media influence operations  
U.S. intel claims Russia, China, Iran involved
- Sporadic voting machine breakdowns,  
with apparently natural causes
- Ballot usability problems in Florida, again  
In Broward county, 3.7% fewer votes were cast  
for Senate than for governor (26,000 votes).  
The election was decided by 10,033 votes.

Ballot Style 58	Boleta Oficial De La Eleccion General	Ofisyél Jeneral Eleksyon
November 6, 2018 Broward County, Florida	Noviembre 6 de 2018 Condado de Broward, Florida	6 Novann 2018 Konte Broward, Fl
<b>Ballot Instructions:</b> <ul style="list-style-type: none"><li>To vote, fill in the oval completely next to your choice. Use only the device provided or mark pen.</li><li>Do not make a mistake. Ask for a new ballot, or a new device, if you need it.</li><li>To vote for a write-in candidate, fill in the oval and print the name on the blank line provided in the write-in candidate.</li></ul>	<b>Governor and Lieutenant Governor</b> Gobernador y Teniente Gobernador Goverinor i Lyetinan Goverinor <b>Vote for One/Vote por Uno/Vote pou Youn</b> <ul style="list-style-type: none"><li><input type="radio"/> Ron DeSantis Jeanette Nuñez</li><li><input type="radio"/> Andrew Gillum Chris King</li><li><input type="radio"/> Darcy G. Richardson Nancy Arpericano</li><li><input type="radio"/> Kyle Ellen Wildt</li><li><input type="radio"/> Ryan Christopher Foley John Turton Jr</li><li><input type="radio"/> Bruce Stanley Ryan Howard McJury</li><li>Write-in/Escribir/A letri</li></ul>	<b>Fourth District Court of Appeal</b> Tribunal De Apelaciones Del Cuarto Distrito <b>Write-in/Escribir/A letri</b> ¿Deberá retenerse en su cargo al Juez Jeffrey T. Kuntz del Cuarto Distrito de Apelaciones? <input type="radio"/> Yes/Sí/We <input type="radio"/> No/No/Non
<b>Enformasyon Sou Biten Vot:</b> <ul style="list-style-type: none"><li>Pou vote, brien kolore tout anvan oval. ● Li akole respons ou chevi a. Sèlman sèl ak yon plim nwa oubyen ak yon krasyon pou ekri sou biten vot la.</li><li>Si wè ak yon etik, mande yo ba w yon nouvo biten vo. Si w estase oubyen fè nouvo mak, li ap posib pou vot ou pa valab anvan.</li><li>Pou vote pou yon kandida ki pa nan oval la, ekri non kandida sou lyè vò la rezeve pou yon kandida.</li></ul>	<b>Attorney General</b> Fiscal General Pwolikè Jeneral <b>Vote for One/Vote por Uno/Vote pou Youn</b> <ul style="list-style-type: none"><li><input type="radio"/> Ashley Moody</li><li><input type="radio"/> Sean Shaw</li><li><input type="radio"/> Jeffrey Marc Siskind</li></ul>	<b>Chief Financial Officer</b> Controlador Estatal Chif Ofisyè Finans <b>Vote for One/Vote por Uno/Vote pou Youn</b> <ul style="list-style-type: none"><li><input type="radio"/> Jimmy Patronis</li><li><input type="radio"/> Jeremy Ring</li><li>Write-in/Escribir/A letri</li></ul>
<b>United States Senator</b> Senador De Los Estados Unidos Senatè Etazini <b>Vote for One/Vote por Uno/Vote pou Youn</b> <ul style="list-style-type: none"><li><input type="radio"/> Rick Scott</li><li><input type="radio"/> Bill Nelson</li><li>Write-in/Escribir/A letri</li></ul>	<b>Commissioner of Agriculture</b> Komisyonè de Agricoltura Komisyòn Agrikilti <b>Vote for One/Vote por Uno/Vote pou Youn</b> <ul style="list-style-type: none"><li><input type="radio"/> Matt Caldwell</li><li><input type="radio"/> Nicole "Nikki" Fried</li></ul>	<b>Justice of the Supreme Court</b> Magistrado en el Tribunal Supremo Jistis Nan Lakou Siprem <b>Vote for One/Vote por Uno/Vote pou Youn</b> <ul style="list-style-type: none"><li><input type="radio"/> Jason Allen-Rosner</li><li><input type="radio"/> Stefanie Camille Moon</li></ul>

# So what happened in 2018 ... ?

- Continued social media influence operations  
U.S. intel claims Russia, China, Iran involved
- Sporadic voting machine breakdowns,  
with apparently natural causes
- Ballot usability problems in Florida, again  
In Broward county, 3.7% fewer votes were cast  
for Senate than for governor (26,000 votes).  
The election was decided by 10,033 votes.
- Old-fashioned ballot tampering  
In a North Carolina house race decided by only  
900 votes, a candidate's operatives allegedly  
manipulated large numbers of absentee ballots.

Vex



## More evidence piles up in North Carolina election fraud scandal

The Republican candidate who won in November likely won't be seated before an official hearing in January.

By Dylan Scott | @dylanlscott | dylan.scott@vox.com | Dec 26, 2018, 12:30pm EST

The new Congress will be seated in a matter of days — but it is almost certain that the seat from **the North Carolina Ninth Congressional District** will be left empty, as more evidence of **a brazen vote-tampering scheme** piles up.

The bipartisan state elections board has refused to certify the results of **Republican Mark Harris's win** and instead set a hearing on the election fraud scandal for January 11, a week after new members are sworn in.

Harris beat Democrat Dan McCready by roughly 900 votes on Election Day. But those results have been marred by explosive allegations that an operative working for the Harris campaign collected, tampered with or even destroyed absentee ballots. The alleged plot is now the subject of a state inquiry: the

# So what happened in 2018 ... ?

Overall ... it was eerily quiet.

In 2016, “in a number of states, [Russian] cyber actors were in a position to, at a minimum, alter or delete voter registration data.

—U.S. Senate Intelligence

Committee

**They chose not to pull the trigger.**



# Vulnerable Election Infrastructure

# Senate Intelligence Committee Russia Investigation



Wednesday

C-SPAN  
c-span.org  
@cspan

“The key lesson from 2016 is that election infrastructure hacking threats are real.”

“As James Comey testified here two weeks ago, we know ‘They’ll be back.’”

# Are U.S. Voting Machines Secure?



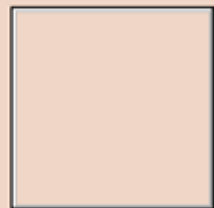
AccuVote TS-X



## President of the United States



George Washington  
Framers Party



Benedict Arnold  
Redcoat Party



1. Attacker infects memory card containing ballot programming files.





2. When officials place the card into the machine, it becomes infected.

AccuVote TS-X can be infected through:

- Unauthenticated **software update** mechanism;
- **Buffer overflows** in code that reads ballot design; or
- **Interpreted programming language** (AccuBasic) used to print result tape.



3. Malware running on the machine can arbitrarily change electronic records and printouts.

```
*****
President of the United States
RACE # 0
# Running                2
# To Vote For            1

# Times Counted          5
# Times Blank Voted      0
# Times Over Voted       0
# Number Undervotes      0
George Washington        2
Benedict Arnold          3
*****
WE, THE UNDERSIGNED,
DO HEREBY CERTIFY THE
ELECTION WAS CONDUCTED
IN ACCORDANCE WITH THE
```

# Pervasive Security Problems

## Source Code Review of the Diebold Voting System (2007)

Calandrino, Feldman, Halderman, Wagner, Yu, and Zeller

Part of the California Secretary of State's "Top-to-Bottom" Voting System Review.

“5.2.1 The AV-TSX automatically installs bootloader and operating system updates from the memory card **without verifying the authenticity**

5.2.2 The AV-TSX automatically installs application updates from the memory card **without verifying the authenticity**

5.2.3 **Multiple buffer overflows** allow arbitrary code execution on startup

5.2.4 Setting a jumper enables a bootloader menu that allows the user **to extract or tamper with** the contents of the internal flash memory

5.2.5 Keys used to secure election data are **not adequately protected**

5.2.6 Malicious code running on the machine could **manipulate election databases, results, and audit logs**

5.2.7 The smart card authentication protocol can be broken, providing access to administrator functions and the **ability to cast multiple votes**

5.2.8 Security **key cards can be forged** and used to change system keys

5.2.9 A local user can get to the Setup menu **without a smart card or key**

5.2.10 The protective counter is **subject to tampering**

5.2.11 SSL certificates used to authenticate can be stolen and have **an obvious password**

5.2.12 OpenSSL is **not initialized with adequate entropy**

5.2.13 Multiple vulnerabilities in the AccuBasic interpreter allow **arbitrary code execution**

5.2.14 Tampering with the memory card can result in **code execution during voting**

5.2.15 A malicious election file on the memory card could exploit **multiple vulnerabilities to run arbitrary code**

5.2.16 Malicious election files can cause **arbitrary code execution** on the AV-TSX when uploading elections

5.2.17 A buffer overflow in the handling of IP addresses **might be exploitable by voters**

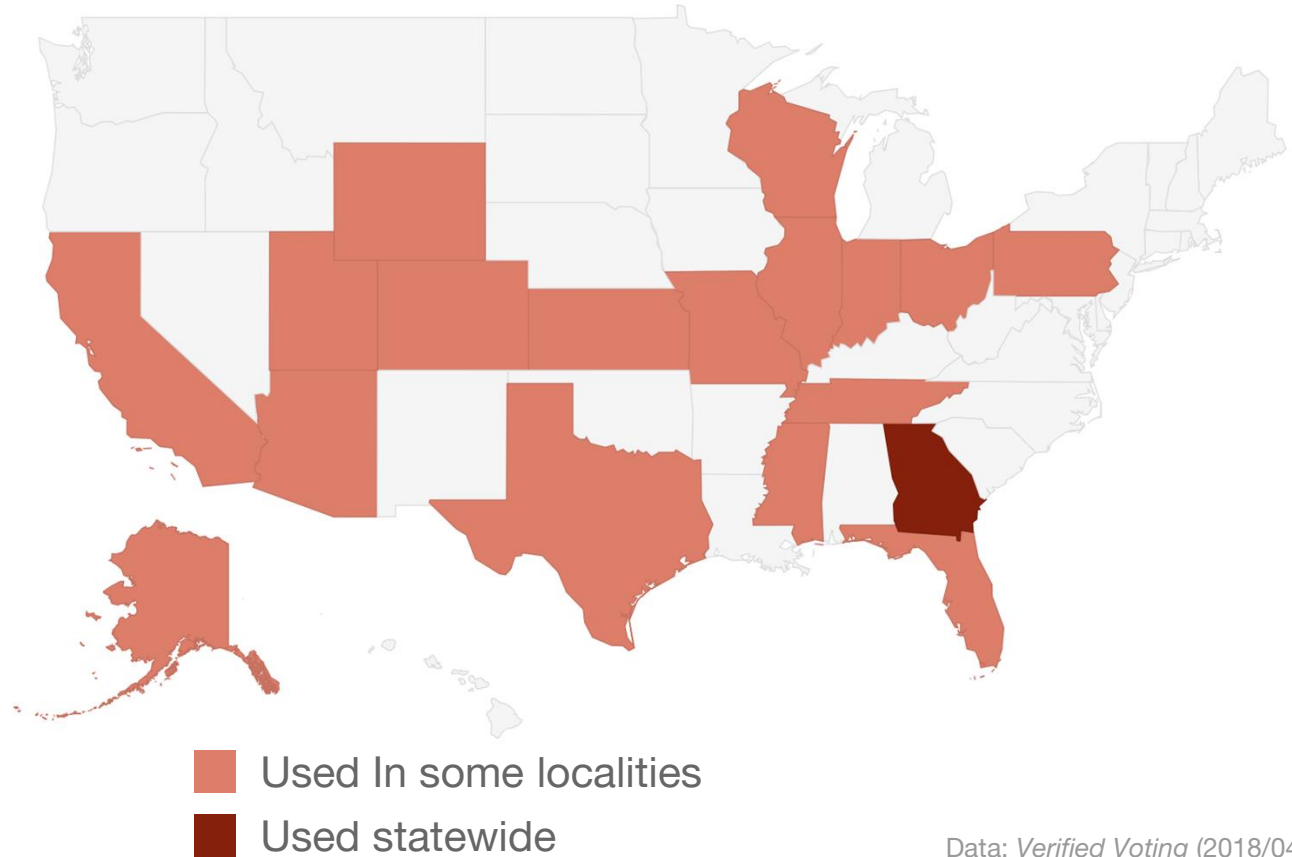
5.2.22 Files on the voting machine are **not securely erased** when they are deleted

5.2.23 **Logic errors may create a vulnerability** when displaying bootloader bitmap images

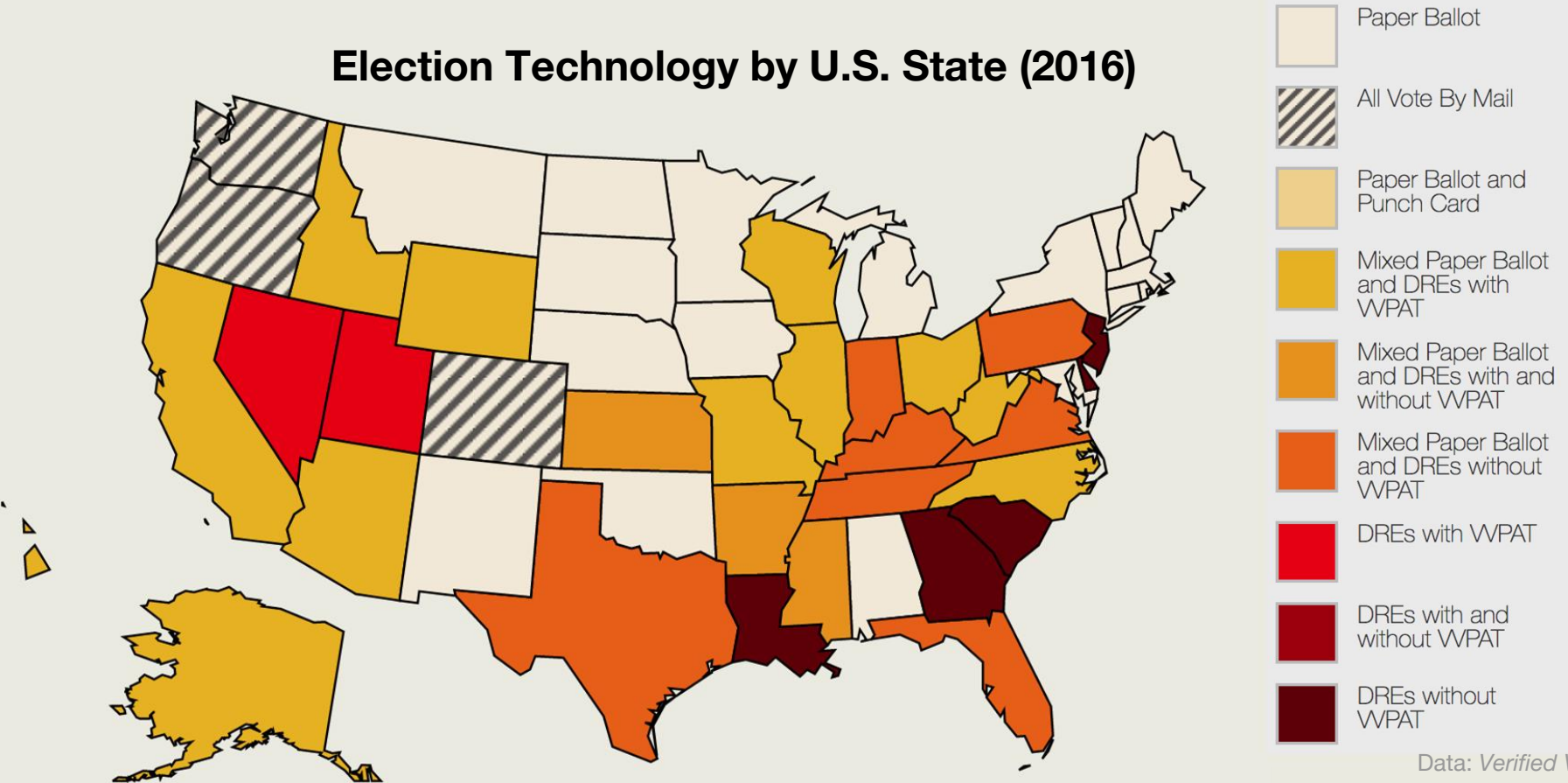
5.2.24 AV-TSX startup code **contains blatant errors**

# States that still use the AccuVote TS-X

**AccuVote TS/TS-X  
machines are still  
used in 18 states**



## Election Technology by U.S. State (2016)



Data: Verified Voting

# U.S. Elections

# Long, Complicated Ballots

## November 8, 2016 (8 de noviembre de 2016) Dallas County, Texas (Condado de Dallas, Texas) SAMPLE BALLOT (BOLETA DE MUESTRA)

**INSTRUCTION NOTE:** Vote on the candidate/statement of your choice in each race by darkening in the oval provided to the left of the name of that candidate/statement.

**Straight-Party Vote:** You may cast a straight-party vote (that is, cast a vote for all the nominees of one party) by darkening in the oval provided to the left of the name of the party of your choice. If you cast a straight-party vote for all the nominees of one party and also cast a vote for an opponent of one of that party's nominees, your vote for the opponent will be counted as well as your vote for all the other nominees of the party for which the straight-party vote was cast. Party Abbreviations, Republican Party (Rep); Democratic Party (Dem); Libertarian Party (Lib); Green Party (Grn).

**Voting for a Declared Write-In Candidate:** You may vote for a declared write-in candidate by writing in the name of the candidate on the line provided and darkening in the oval provided to the left of the line.

### USE THE MARKING DEVICE PROVIDED

**NOTA DE INSTRUCCIÓN:** Vote sobre el candidato/declaración de su preferencia en cada compañía electoral al llenar el óvalo provisto a la izquierda del nombre de ese candidato/declaración.

**Voto de Partido Completo:** Usted puede emitir un voto de partido único (es decir, emitir un voto para todos los candidatos de un solo partido) al llenar el óvalo provisto a la izquierda del nombre del partido de su selección. Si usted emite un voto de partido único para todos los nominados de un solo partido y también emite un voto para un oponente de uno de los nominados de ese partido, su voto para el oponente será contado tanto como su voto para todos los demás nominados del partido por el cual fue emitido el voto de partido único. Abreviaturas, Partido Republicano (Rep); Partido Democrático (Dem); Partido Libertario (Lib); Partido Verde (Grn).

**Votando por un Candidato Declarado por Escrito:** Usted puede votar por un candidato declarado por escrito al escribir el nombre del candidato en la línea provista para ese cargo y al llenar el óvalo provisto a la izquierda de la línea.

### UTILICE EL MARCADOR PROPORCIONADO

Straight Party (Partido Completo)	
Republican Party (Partido Republicano)	Rep
Democratic Party (Partido Democrático)	Dem
Libertarian Party (Partido Libertario)	Lib
Green Party (Partido Verde)	Grn

President and Vice President (Presidente y Vice Presidente)		
<b>Vote for One (Votar por Uno)</b>	Donald J. Trump / Mike Pence	Rep
	Hillary Clinton / Tim Kaine	Dem
	Gary Johnson / William Weld	Lib
	Jill Stein / Ajamu Baraka	Grn
	Write-In (Voto Escrito)	

United States Representative, District 24 (Representante de los Estados Unidos, Distrito Núm. 24)		
<b>Vote for One (Votar por Uno)</b>	Kenny E. Marchant	Rep
	Jan McDowell	Dem
	Mike Kolls	Lib
	Kevin McCormick	Grn

United States Representative, District 26 (Representante de los Estados Unidos, Distrito Núm. 26)		
<b>Vote for One (Votar por Uno)</b>	Michael C. Burgess	Rep
	Eric Mauck	Dem
	Mark Boler	Lib

United States Representative, District 30 (Representante de los Estados Unidos, Distrito Núm. 30)		
<b>Vote for One (Votar por Uno)</b>	Charles Lingerfelt	Rep
	Eddie Bernice Johnson	Dem
	Jarrett R. Woods	Lib
	Thom Prentice	Grn

United States Representative, District 32 (Representante de los Estados Unidos, Distrito Núm. 32)		
<b>Vote for One (Votar por Uno)</b>	Pete Sessions	Rep
	Ed Rankin	Lib
	Gary Stuard	Grn

United States Representative, District 33 (Representante de los Estados Unidos, Distrito Núm. 33)		
<b>Vote for One (Votar por Uno)</b>	M. Mark Mitchell	Rep
	Marc Veasey	Dem

Railroad Commissioner (Comisionado de Ferrocarriles)		
<b>Vote for One (Votar por Uno)</b>	Wayne Christian	Rep
	Grady Yarbrough	Dem
	Mark Miller	Lib
	Martina Salinas	Grn

Justice, Supreme Court, Place 3 (Juez, Corte Suprema, Lugar Núm. 3)		
<b>Vote for One (Votar por Uno)</b>	Debra Lehmann	Rep
	Mike Westergren	Dem
	Kathie Glass	Lib
	Rodolfo Rivera Munoz	Grn

Justice, Supreme Court, Place 5 (Juez, Corte Suprema, Lugar Núm. 5)		
<b>Vote for One (Votar por Uno)</b>	Paul Green	Rep
	Dori Contreras Garza	Dem
	Tom Oxford	Lib
	Charles E. Waterbury	Grn

Justice, Supreme Court, Place 9 (Juez, Corte Suprema, Lugar Núm. 9)		
<b>Vote for One (Votar por Uno)</b>	Eva Guzman	Rep
	Savannah Robinson	Dem
	Don Fulton	Lib
	Jim Chisholm	Grn

*(This area contains detailed ballot instructions and candidate information for various offices, including State Representative, State Senator, and State Representative, District 24, 26, 30, 32, and 33. It includes names of candidates and their respective party affiliations.)*

*(This area contains detailed ballot instructions and candidate information for various offices, including Justice, Supreme Court, Place 3, 5, and 9, and Railroad Commissioner. It includes names of candidates and their respective party affiliations.)*



# U.S. Voting Machines

# 2 Styles, 52 Models



## Optical Scan

Computer counts paper ballots as they're placed in ballot box



## DRE (Direct Recording Electronic)

Votes cast on-screen, recorded in memory; some models print paper audit records (VVPAT)

# Every U.S. voting machine subjected to rigorous independent security review suffered vulnerabilities that would enable vote-stealing attacks.



**Hart InterCivic eSlate**  
Cards spread malware (2007)



**AVC Advantage**  
Cards spread malware (2009)



**Sequoia AVC Edge**  
Cards spread malware (2007)



**Optech Insight**  
Cards spread malware (2007)



**ES&S iVotronic**  
Cards spread malware (2007)



**Diebold AccuVote TSX**  
Cards spread malware (2007)



**Diebold AccuVote OS**  
Cards spread malware (2007)



**ES&S Model 100**  
Cards spread malware (2007)



Hacking an Election?

# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



## Challenge 1

Diverse, decentralized voting technology

## Challenge 2

Machines aren't connected to the Internet

## Challenge 3

>70% of U.S. votes have a paper record

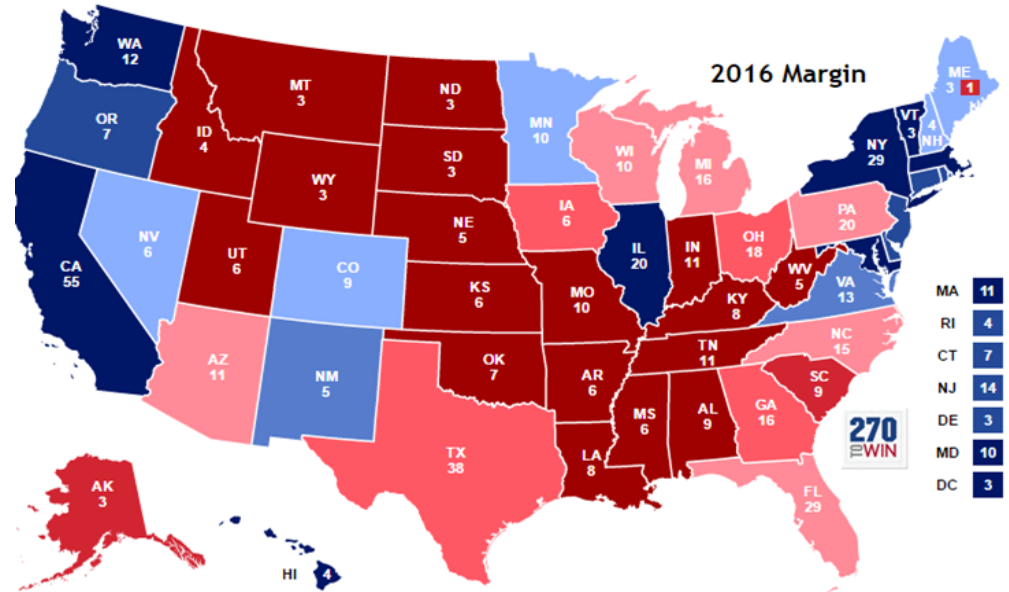
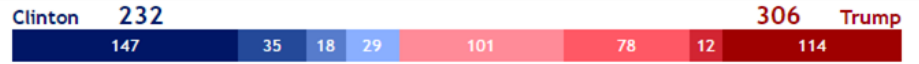
# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?

## Challenge 1

Diverse, decentralized voting technology



# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



## Challenge 1

~~Diverse, decentralized voting technology~~  
**Choose weakest targets in closest states.**

## Challenge 2

Machines aren't connected to the Internet

## Challenge 3

>70% of U.S. votes have a paper record

# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



## Challenge 1

Diverse, decentralized voting technology  
**Choose weakest targets in closest states.**

## Challenge 2

Machines aren't connected to the Internet

## Challenge 3

>70% of U.S. votes have a paper record

Centralized **election management computer** programs ballot design to memory cards before each election



If infected, can spread malware to all machines across one or more counties







How hard would it be to attack an election management computer?

Many jurisdictions outsource their ballot programming to small, outside businesses.

75% of Michigan counties use just two ~20 person companies.

The screenshot shows a web browser window with the URL [www.gbsvote.com/page.asp?p=5&i=5](http://www.gbsvote.com/page.asp?p=5&i=5). The page features the GBS logo (Governmental Business Systems) and a navigation menu with links for About Us, Store, Info, County Directory, and Election Results. Below the navigation is a large heading "Who We Are" and a grid of staff profiles. Each profile includes a photo, name, title, and email contact information.

Name	Title	Email
Larry Mandel	President	Email Larry
Sue Rippe	Administrative Assistant	Email Sue
Gary Ingelson	Senior Vice President Sales Administration	Email Gary
Larry Calvert	Director of Election Services	Email Larry
John Vold	Director of IT Services	Email John
Tiffany Tuominen	Election Service Specialist	Email Tiffany

# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



## Challenge 1

Diverse, decentralized voting technology  
**Choose weakest targets in closest states.**

## Challenge 2

Machines aren't connected to the Internet  
**Target election management computers to spread malware to the voting machines.**

## Challenge 3

>70% of U.S. votes have a paper record

# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



## Challenge 1

Diverse, decentralized voting technology  
**Choose weakest targets in closest states.**

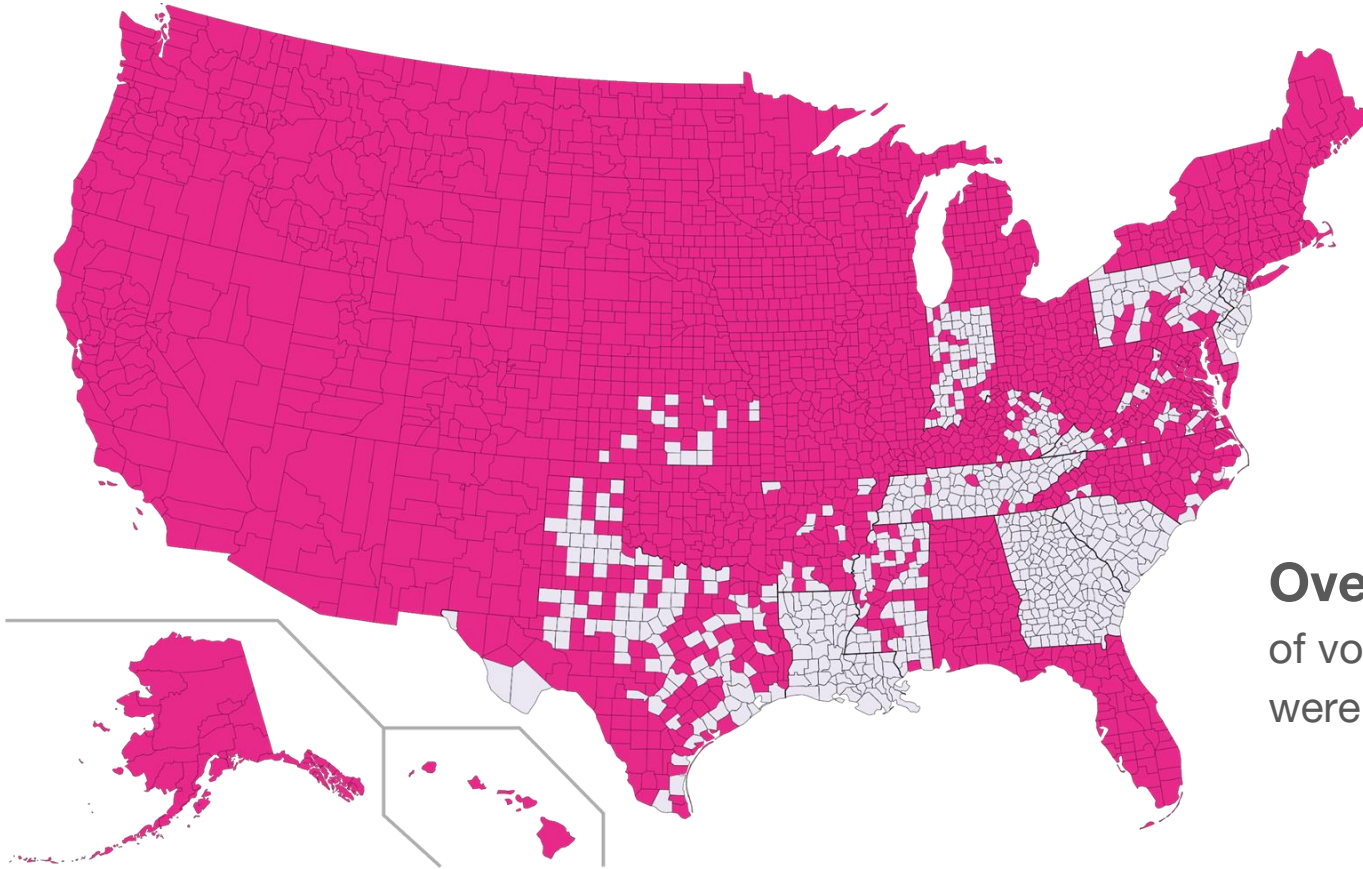
## Challenge 2

Machines aren't connected to the Internet  
**Target election management computers to spread malware to the voting machines.**

## Challenge 3

**>70% of U.S. votes have a paper record**

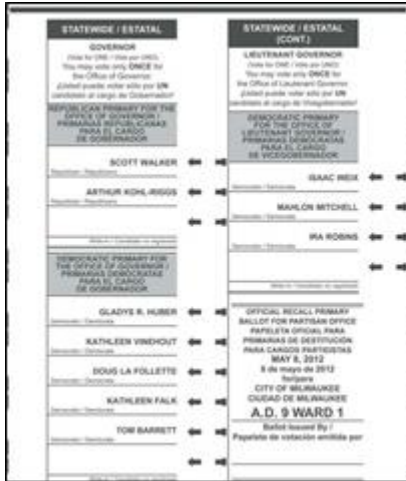
# Use of Paper has Increased



**Over 70%**  
of votes cast in 2016  
were recorded on paper.



# Paper as a Defense



Slow/expensive to tally  
**Verified by voter**

Fast/cheap to tally  
**Unverified**

# Paper as a Defense



## Risk-Limiting Audit (RLA)

**Hand count randomly selected ballots** until you establish, with high statistical confidence, that hand-counting all paper records would yield the same winner.

Various ways to implement RLAs, depending on local constraints.



# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?



## Challenge 1

~~Diverse, decentralized voting technology~~  
**Choose weakest targets in closest states.**

## Challenge 2

~~Machines aren't connected to the Internet~~  
**Target election management computers to spread malware to the voting machines.**

## Challenge 3

~~70% of U.S. votes have a paper record~~  
**Most states won't look at the paper!**

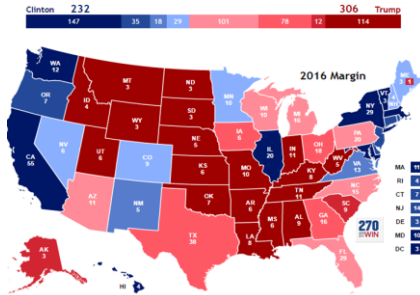


# Election Hacking

# Invisible Attacks

How hard would it be to invisibly change a national election outcome, by tampering with voting machines?

**Easier than we thought!**



Sue Rippe

Administrative Assistant

Email Sue



## Step 1

Use pre-election polls to identify likely close states, choose weakest targets.

## Step 2

Target large counties or service providers, and compromise election management computers.



## Step 3

Infected memory cards exploit vulnerable voting machines to run malware, swap, e.g., 10% of votes.



## Step 4

Most states will throw away the paper ballots without checking.



# Defending U.S. Elections

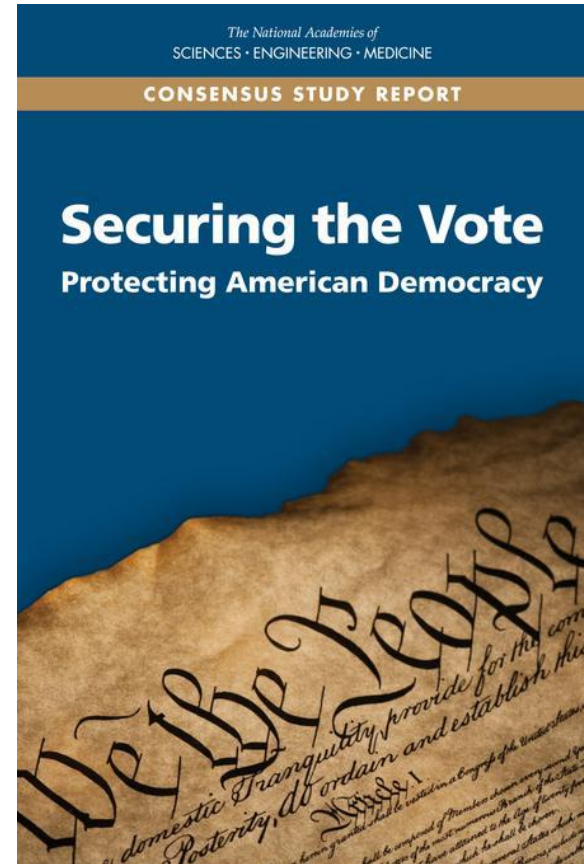
# Key Defenses

**Consensus** of election security experts and election officials:

**Paper Ballots + Post-Election Audits**

are pragmatic, robust, and **necessary**.

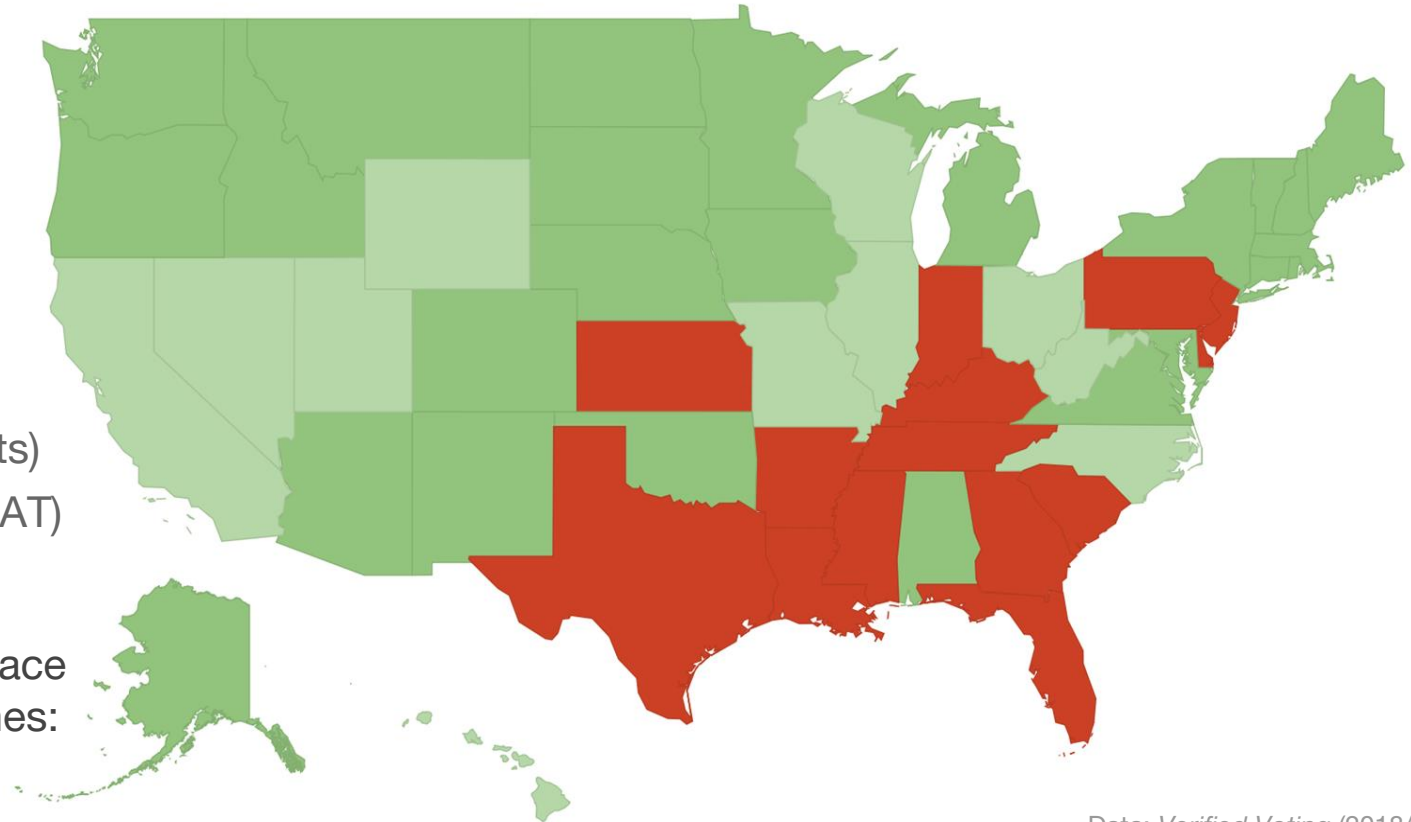
An opportunity for a major cybersecurity win!



# National Progress: Paper

**Are all votes recorded on paper?**

- Yes (paper ballots)
- Yes (ballots/VVPAT)
- No



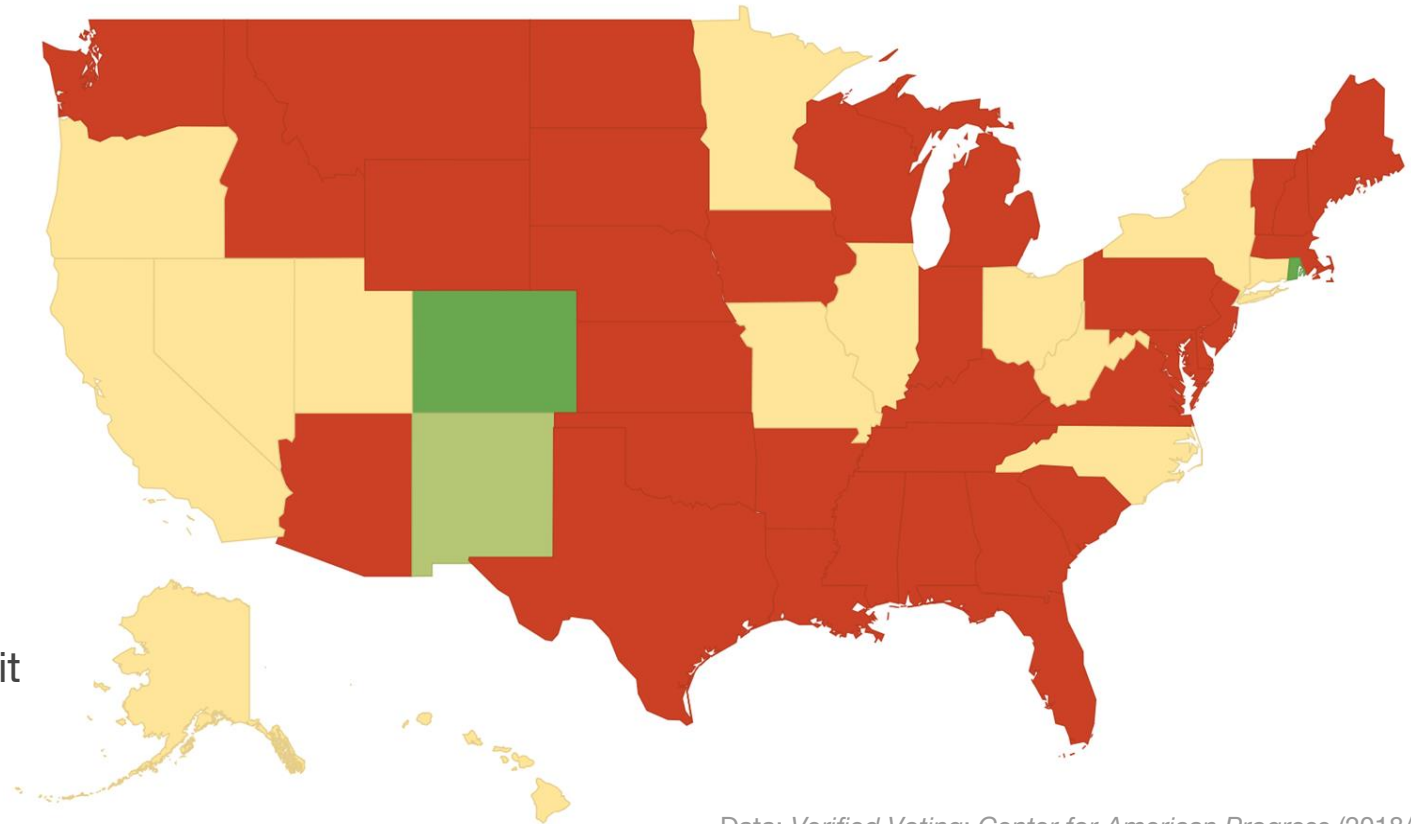
National cost to replace all paperless machines:

**\$130-420M**

# National Progress: Paper+Auditing

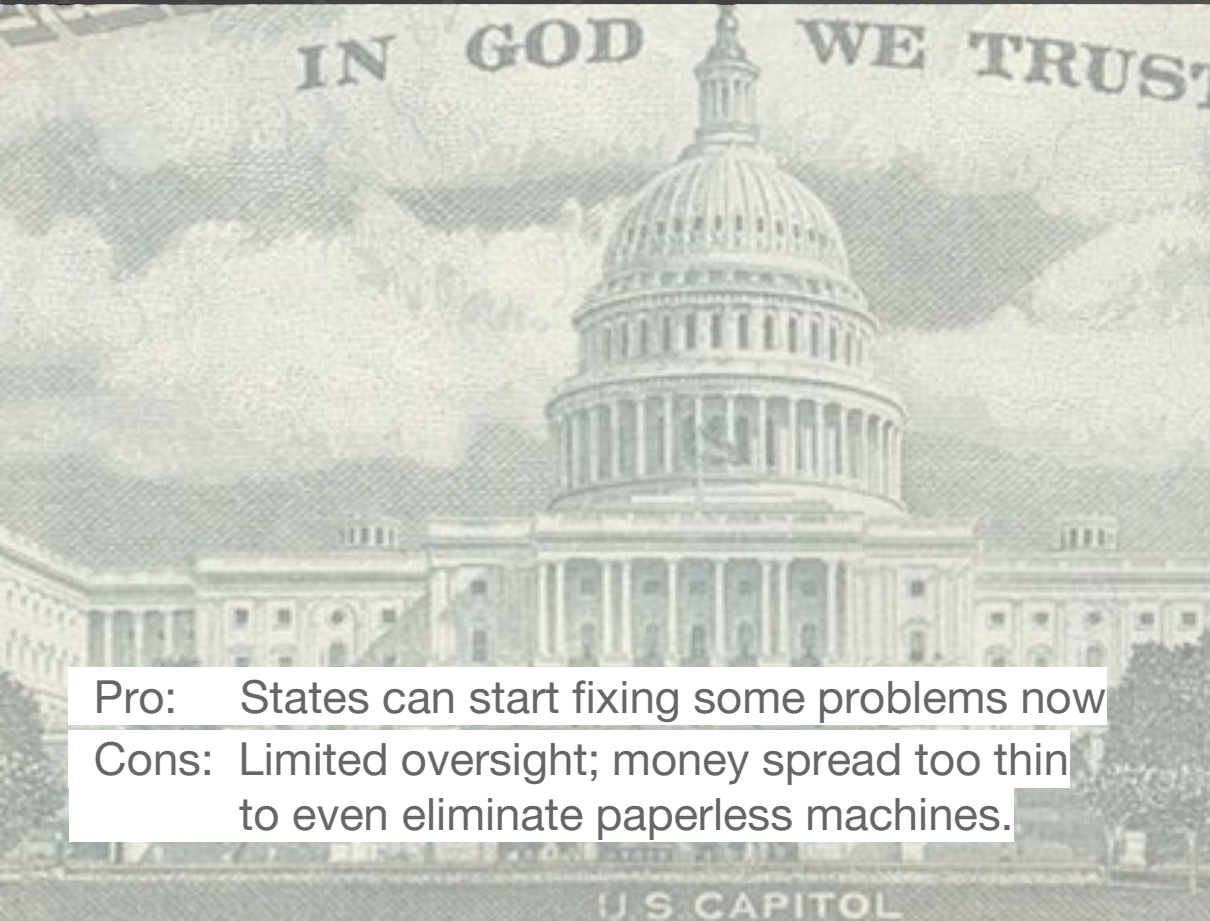
Are votes on  
paper and  
robustly  
audited?

- Yes
- Somewhat
- No



National cost to audit  
every federal race:  
< \$25M/year

# \$380M in Emergency Election Cyber Fundings



Pro: States can start fixing some problems now

Cons: Limited oversight; money spread too thin to even eliminate paperless machines.

“... states may use this funding to:

1. Replace voting equipment that only records a voter’s intent electronically with equipment that utilizes a voter-verified paper record;
2. Implement a post-election audit system that provides a high level of confidence in the accuracy of the final vote tally;
3. Upgrade election-related computer systems to address cyber vulnerabilities [...];
4. Facilitate cybersecurity training [...];
5. Implement established cybersecurity best practices for election systems; and
6. Fund other activities that will improve the security of elections for Federal office.”

# Case Study: Maryland

Paper Ballots?

Yes



Replaced in 2016



Robust Audits?

No



**Maryland's audits  
are security theater.**

Only inspect digital images  
from the voting machines.

Easily fooled by malware!



Overall Grade

**C**

**Needs  
Additional  
Improvement**

# Case Study: Pennsylvania

Paper Ballots?

Soon



Replacing by 2020



Robust Audits?

2022

Pennsylvania has **committed** to performing “robust” post-election audits beginning in 2022

Will they be truly risk-limiting?



Overall Grade

**B**

Good Plans for  
Improvement

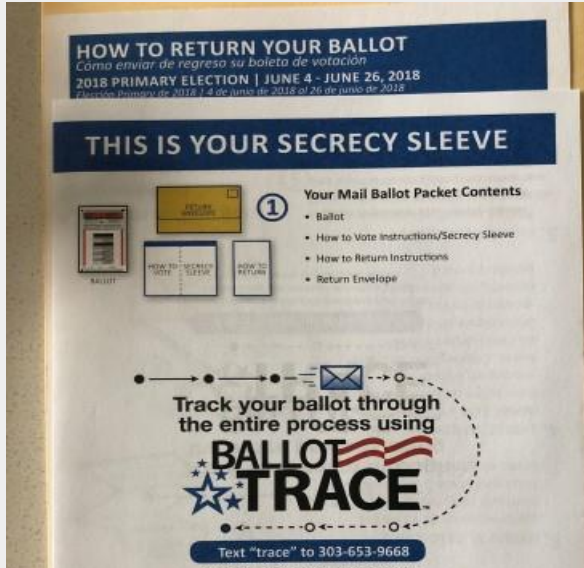


# Case Study: Colorado

Paper Ballots?

Yes

Colorado uses paper ballots statewide (mostly vote-by-mail)



Robust Audits?

Yes

Colorado has required risk-limiting audits since 2017



Overall Grade

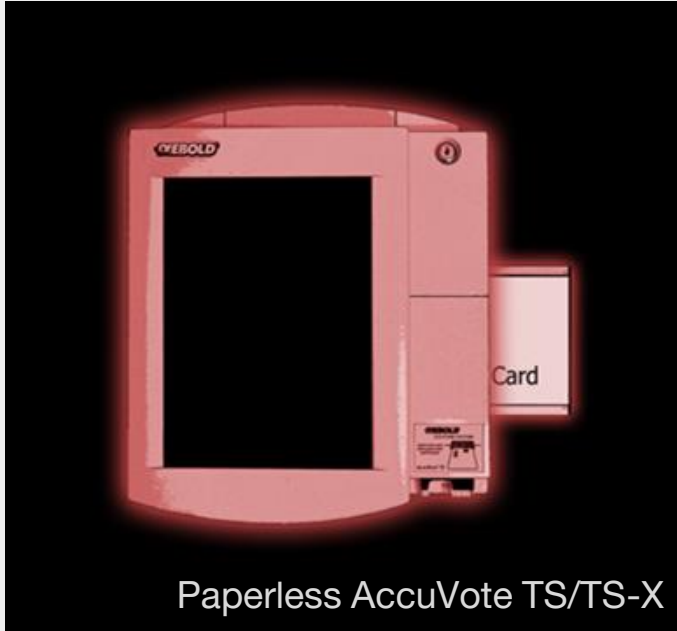
A

Very Well  
Protected

# Case Study: Georgia

Paper Ballots?

No



Paperless AccuVote TS/TS-X

Don't worry, they're "air gapped"...

Robust Audits?

No

Georgia doesn't record votes on paper, so **meaningful post-election audits are impossible.**

Secure Voter Registration?

No



Overall Grade

**F**

**Very High Risk**

# Georgia's Voter Registration System

Days before the November 2018 election, Georgia democrats uncover vulnerabilities:

- **Read and manipulate anyone's records** by changing voter ID number in URL
- **Read entire server filesystem** by changing another URL

Disclosed to the Secretary of State's office

MY VOTER PAGE  
GEORGIA SECRETARY OF STATE ROBYN A. CRITTENDEN

Securities Charities

MVP Login:

Your Name and County

First Initial:\*

Last Name:\*

County:\*

Date of Birth:\*

(mm/dd/yyyy)

**“AFTER FAILED HACKING ATTEMPT,  
SOS LAUNCHES INVESTIGATION INTO  
GEORGIA DEMOCRATIC PARTY.”**



Secretary of State  
Governor-elect  
**Brian Kemp (R)**

vote for *success*  
with the Secretary of State Elections Division

Georgia Voter ID  
Learn more about Georgia Voter Identification Requirements

Stop Voter Fraud  
Do Your Part to Help Ensure Secure and Fair Georgia Elections

Georgia Secretary of State's Elections Division

Share Your Ideas to Help Strengthen Georgia Elections

Learn more about the Georgia VoteSafe Program

# Secure Elections Act

Develops election security guidelines.  
Improves information sharing.  
Requires paper and post-election audits.

115TH CONGRESS  
2D SESSION

## S. 2593

To protect the administration of Federal elections against cybersecurity threats.

IN THE SENATE OF THE UNITED STATES

MARCH 22, 2018

Mr. GRAHAM, Ms. HARRIS,  
and Mr. WARNER) introduced  
referred to the Committee



Lankford (R-OK)



Klobuchar (D-MN)



Harris (D-CA)



Collins (R-ME)



Heinrich (D-MN)



Graham (R-SC)



Burr (R-NC)



Warner (D-VA)



Rounds (R-SD)



Nelson (D-FL)



Moran (R-KS)



King (I-ME)



Hatch (R-UT)



Feinstein (D-CA)

# Defending U.S. Elections

No proof past election results were hacked ... *what about next time?*

**U.S. urgently needs to better defend election infrastructure.**

- Make attacks more difficult: **Apply best practices and security testing**
- Ensure attacks are detectable: **Record every vote on paper**  
States that need to act: PA, IN, TX, NJ, DE, SC, GA, MS, TN, NC, LA, AR, KS, KY
- Use the physical evidence: **Audit the paper trail to high confidence**  
Manual, risk-limiting audits are a common-sense quality control to detect and recover from attacks.  
Only a few states routinely perform them today.

States are beginning to make progress, but Federal leadership is necessary to ensure all states have essential protections in place for 2020

# What You Can Do

## As a hacker:

- Explain election cybersecurity threats to the public.
- Engage with election officials and offer your technical expertise.
- Build technology to help make voting on paper easier and more efficient.

## As a citizen:

- Demand that officials implement paper and risk-limiting audits.
- Get involved with local election integrity advocacy groups.
- Urge U.S. Congress to pass the Secure Elections Act or similar bills.
- Learn more! Sign up for “*Securing Digital Democracy*” on Coursera.

**2020 Presidential Election about 22 months away. Time to get moving!**

A stylized, monochromatic American flag in shades of gray, featuring a field of stars in the upper left and horizontal stripes across the rest of the page.

# Election Cybersecurity

## 2018 Progress Report

J. Alex Halderman  
University of Michigan

# What about blockchain?

**Blockchain solves stolen votes about as well as Bitcoin solves stolen money.**

Safely voting online requires solving **three major challenges**:

- Casting securely from untrusted user devices.
- Defending servers against nation-state attackers.
- Remotely authenticating voters.

**Blockchain solves none of these.**

Blockchain-based Internet voting piloted by West Virginia in 2018 for overseas voters.

- Closed source
- Non-peer reviewed
- Snakeoil?

