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%)
- PA 22,146 (0.4%)
- FL 56,455 (0.6%)
- WI 11,374 (0.4%)
- AZ 45,617 (1.8%)
- NC 86,657 (1.8%)

Any Two

Any Three States

27,500 of 137 million (0.02%)
Flashback: 2016 Election Recounts

**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?
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”
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

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

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
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
**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*

*Source: News reports and public statements*
Russian General Staff Main Intelligence Directorate actors 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)
In July 2018, prospectors indicted GRU officers in connection with the email theft, registration system attacks, and attempts to phishing local election officials.

More to come?
What Happened in 2018?
Continued social media influence operations
U.S. intel claims Russia, China, Iran involved

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

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
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.
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.

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.

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.

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.

They chose not to pull the trigger.
Vulnerable Election Infrastructure
“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?
<table>
<thead>
<tr>
<th>Position</th>
<th>Candidate</th>
<th>Party</th>
</tr>
</thead>
<tbody>
<tr>
<td>President of the United States</td>
<td>George Washington</td>
<td>Framers Party</td>
</tr>
<tr>
<td></td>
<td>Benedict Arnold</td>
<td>Redcoat Party</td>
</tr>
</tbody>
</table>
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.
Pervasive Security Problems

Calandrino, Feldman, Halderman, Wagner, Yu, and Zeller
Part of the California Secretary of State’s “Top-to-Bottom” Voting System Review.

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

“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

Calandrino, Feldman, Halderman, Wagner, Yu, and Zeller
Part of the California Secretary of State’s “Top-to-Bottom” Voting System Review.
States that still use the AccuVote TS-X

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

Data: Verified Voting (2018/04)
U.S. Elections

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 or statement of your choice in each race by darkening the oval provided to the left of the name of that candidate or 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 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 any opponent of one of that party's nominees, your vote for the opponent will be counted as one of your votes for 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 (Gm).

**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 o la declaración de su preferencia en cada cámara electoral al llenar el oval 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 oval 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 unponente de uno de los nominados de ese partido, su voto para el oponente será counted 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 Demócrata (Dem), Partido Libertario (Lib), Partido Verde (Gm).

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 oval provisto a la izquierda de la línea.

**UTILICE EL MARCADOR PROPORCIONADO**

| United States Representative, District 24 (Representante de los Estados Unidos, Distrito Núm. 24) |
|-----------------|-----------------|-----------------|-----------------|
| **Vote for One (Votar por Uno)** |
| Kenny E. Marchant | Rep |
| Jan McDowell | Dem |
| Mike Kolls | Lib |
| Kevin McCormick | Gm |

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

| United States Representative, District 30 (Representante de los Estados Unidos, Distrito Núm. 30) |
|-----------------|-----------------|-----------------|-----------------|
| **Vote for One (Votar por Uno)** |
| Charles Lingerfelt | Rep |
| Eddie Bernice Johnson | Dem |
| Jarrett R. Woods | Lib |
| Thom Prentice | Gm |

| United States Representative, District 32 (Representante de los Estados Unidos, Distrito Núm. 32) |
|-----------------|-----------------|-----------------|-----------------|
| **Vote for One (Votar por Uno)** |
| Pete Sessions | Rep |
| Ed Rankin | Lib |
| Gary Starnes | Gm |

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

| Railroad Commissioner (Comisionado de Ferrocarriles) |
|-----------------|-----------------|-----------------|-----------------|
| **Vote for One (Votar por Uno)** |
| Wayne Christian | Dem |
| Crissy Zeszyt | Lib |
| Mark Miller | Gm |
| Martina Salinas | Gm |

| Justice, Supreme Court, Place 3 (Juez, Corte Suprema, Lugar Núm. 3) |
|-----------------|-----------------|-----------------|-----------------|
| **Vote for One (Votar por Uno)** |
| Debra Lehrmann | Rep |
| Mike Westergren | Dem |
| Kathleen Gwinn | Lib |
| Rodolfo Rivera Kruz | Gm |

| Justice, Supreme Court, Place 5 (Juez, Corte Suprema, Lugar Núm. 5) |
|-----------------|-----------------|-----------------|-----------------|
| **Vote for One (Votar por Uno)** |
| Paul Green | Rep |
| Don Conneres Garza | Dem |
| Tom Oxford | Lib |
| Charles E. Waterbury | Gm |

| Justice, Supreme Court, Place 9 (Juez, Corte Suprema, Lugar Núm. 9) |
|-----------------|-----------------|-----------------|-----------------|
| **Vote for One (Votar por Uno)** |
| Eva Guzman | Rep |
| Savannah Robinson | Lib |
| Dan Fulton | Gm |

**President and Vice President (Presidente y Vice Presidente)**

**Vote for One (Votar por Uno)**

- Donald J. Trump / Mike Pence (Rep)
- Hillary Clinton / Tim Kaine (Dem)
- Gary Johnson / William Weld (Lib)
- Jill Stein / Ajamu Baraka (Gm)

**Write-In (Voto Especial)**
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.
Hacking an Election?
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
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
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
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.
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

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
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.
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

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

Easier than we thought!

**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

Data: Verified Voting (2018/03)
Are votes on paper and robustly audited?

- **Yes**
- **Somewhat**
- **No**

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

Data: Verified Voting; Center for American Progress (2018/02)
$380M in Emergency Election Cyber Fundings

“... 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.”

Pro: States can start fixing some problems now

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

Paper Ballots? Yes

Paperless AccuVote TS

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

![Image of Paperless DREs]

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]

**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

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
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

“AFTER FAILED HACKING ATTEMPT, SOS LAUNCHES INVESTIGATION INTO GEORGIA DEMOCRATIC PARTY.”
Secure Elections Act

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