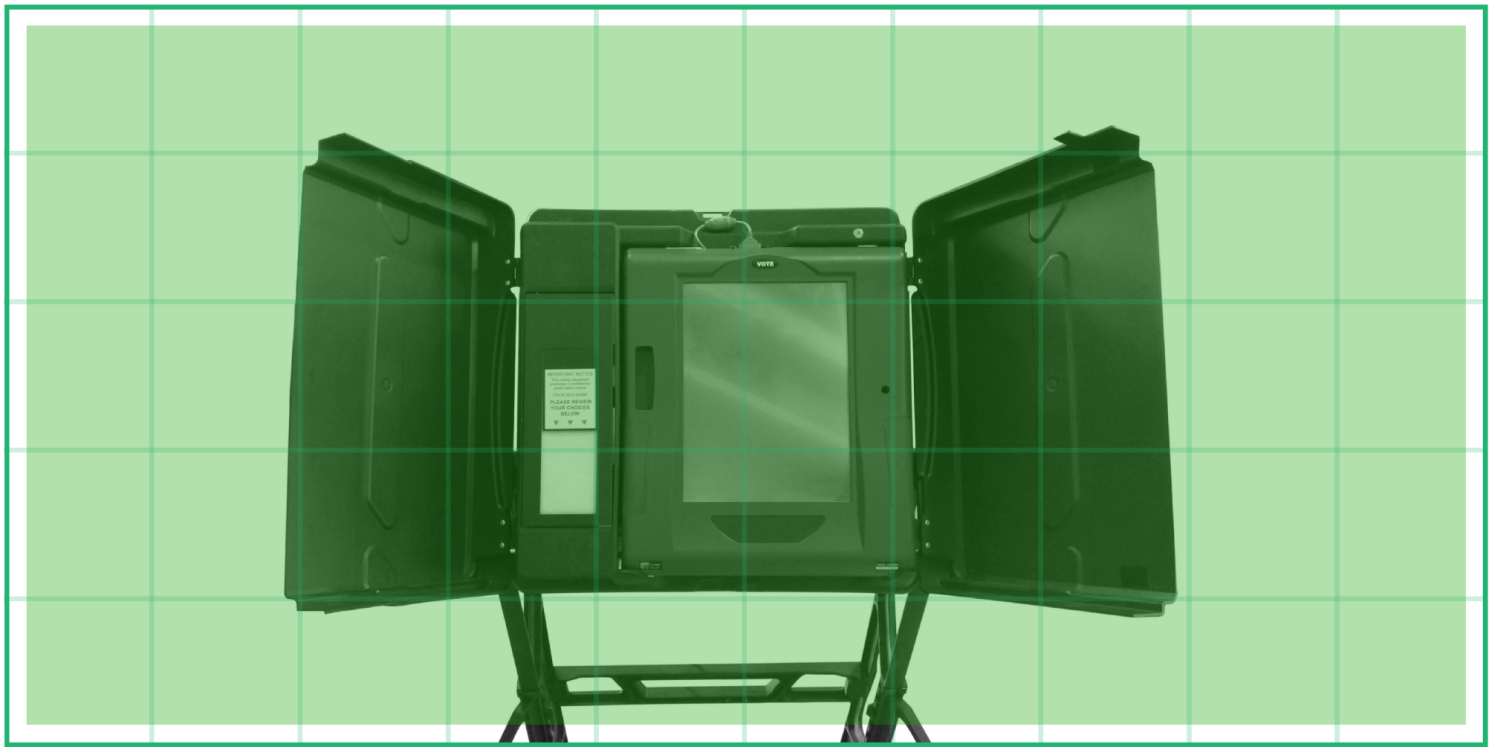
Jesse B. Staniforth Follow
Freelance reporter, covering Indigenous/Northern issues, politics, cybersecurity, and food safety. M...
May 1 · 20 min read

How easy would it be to rig the next election?

If both parties can't soon agree on how to upgrade to crucial systems: very easy.



CREDIT: illustration by Diana Ofosu

On May 25, 2014, Russian state broadcaster Channel One reported the winner of the day's presidential election in Ukraine: with a surprising 37 percent plurality, Dmytro Yarosh, leader of the extreme-right paramilitary group Right Sector, would be the new Ukrainian president. According to Channel One, previous favorite Petro Poroshenko received only 29 percent of the vote.

These numbers were particularly unexpected because only 0.7 percent of voters had voted for Yarosh, versus the 54.7 percent who had voted

for Poroshenko—numbers that news outlets in Ukraine and elsewhere were accurately reporting. Barely a half-hour prior to the announcement of the election results, a cybersecurity team at Ukraine's Central Election Commission (CEC) removed a virus that had been deployed in its computers. That virus was designed to total 37 percent of votes for Yarosh, and 29 percent for Poroshenko.

In the popular imagination, this is what election hacking looks like—dramatic, national-scale interference that manually rewrites tallies and hands the victory to the outlier. Certainly these attacks may occur. However, they're only one of a variety of electoral hacks possible against the United States, at a time when hacking attacks are becoming more accessible to threat-actors and nation-state-sponsored attackers are growing more brazen. Yes, hackers may attempt to change the vote totals for American elections—but they can also de-register voters, delete critical data, trip up voting systems to cause long lines at polling stations, and otherwise cultivate deep distrust in the legitimacy of election results. If hackers wish to rig a national election, they can do it by changing only small numbers on a state level.

Lax oversight and "an impending crisis"

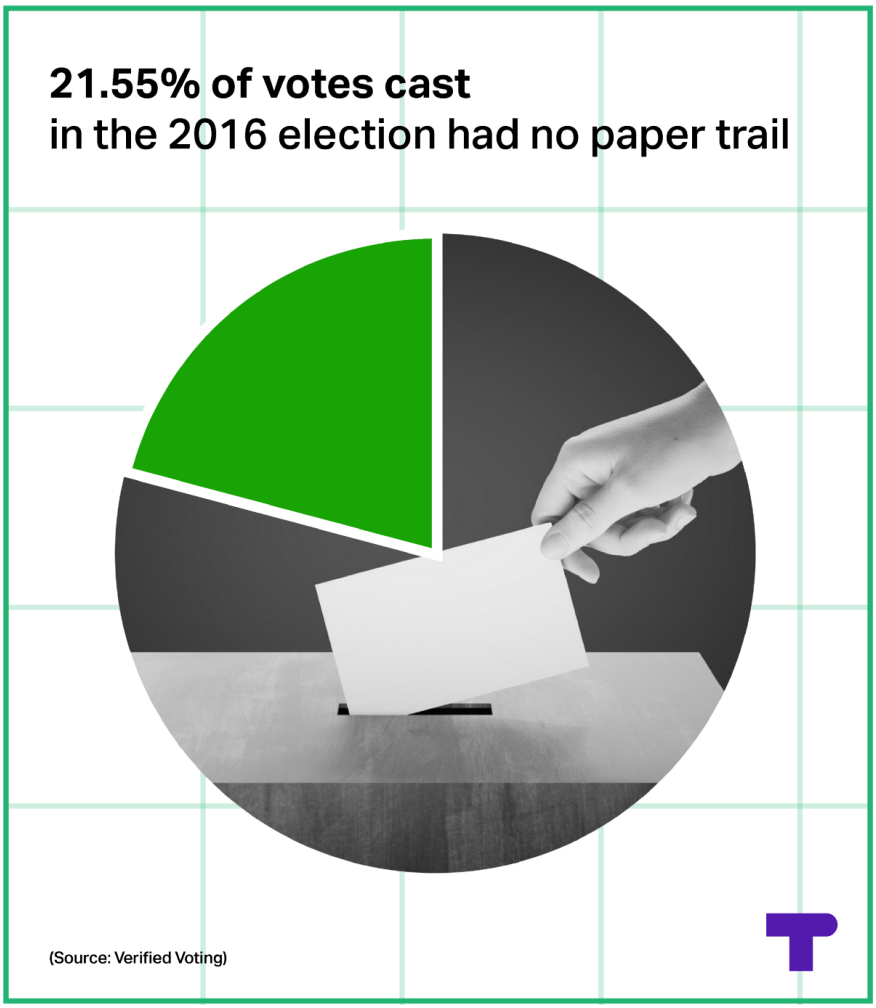
The United States—whose 200 million registered voters mark their votes in roughly 187,000 precincts across 13,000 jurisdictions—has inordinately complex ballots, comprising many separate elections on one day. As University of Michigan computer science professor J. Alex Halderman and PhD student Matt Bernhard note, the U.S. also likes to know the results of its elections the same night as the polls close (Halderman and Bernhard describe this in typically technical terms as "latency sensitivity"). This makes it all but impossible to avoid the use of voting machines, which emerged in the late 19th century and had come into widespread use in the United States by the 1960s.

The 2000 "Hanging Chad" election fiasco revealed significant flaws in lever- and punchcard-systems, at the same time as concerns were rising about the accessibility of traditional voting systems to disabled voters. In response, Congress passed the Help America Vote Act in 2002. It responded to these issues by providing for an upgrade to modernized electronic-voting systems, as well as specifically addressed voting accessibility. Thus, HAVA ushered in machines by

vendors like Diebold and Sequoia—companies that would soon become controversial.

The U.S. voting machine industry is presently dominated by three major companies. Austin, Texas' Hart InterCivic; Toronto's Dominion Voting Services (which owns Premier, formerly known as Diebold, and Sequoia); and Omaha, Nebraska's Election Systems & Software (ES&S), headquartered on the Ayn Rand–themed John Galt Boulevard.

Because states and counties (and sometimes even precincts) are free to decide on their own which systems to purchase, there were a total of 52 different types of voting machines in use in the United States during the last election, varying so widely that a color-coded county-level map of U.S. voting machines presents the country as afflicted by a blotchy, non-localized rash.



CREDIT: Diana Ofosu

Generally speaking, the e-voting machines these vendors (and other smaller manufacturers) produce fall into two categories: optical scanners, and Direct Recording Electronic (DRE) machines. Optical scanners may be small—such as those used in precincts to validate and accept hand-marked ballots—or they may be enormous, used on a county-wide scale to centrally count paper ballots (such as absentees). DREs, meanwhile, are usually touch-screen devices. Some are equipped with a printer that delivers a paper confirmation prior to finalize a voter's choices (known as a "Voter-verified paper audit trail," or VVPAT)—but others are not. As a result, some 21.55 percent of votes cast in the 2016 election did not leave any kind of paper trail, according to Verified Voting.

One thing all voting machines seem to have in common is that whenever they have been subjected to aggressive testing by hackers,

they have fallen apart.

Insecure voting systems are the norm, not the exception

"These machines are just so poorly engineered, the only real way to secure them is to destroy them and start over," said the University of Michigan's Matt Bernhard.

In 2007, two states initiated serious audits of voting machine technology by computer scientists—California's "Top-to-Bottom Review" (TTBR, examining systems by Premier/Diebold, Hart InterCivic, and Sequoia) and Ohio's EVEREST project (examining systems by ES&S, Premier/Diebold, and Hart InterCivic.

In both cases, the results were devastating.

"Every current e-voting system has serious, exploitable vulnerabilities," concluded the University of Pennsylvania's Matt Blaze and Sandy Clark, while presenting the results of their portion of the EVEREST study at the 2008 Hackers on Planet Earth conference. "Serious, practical, undetectable attacks can be carried out by individual voters and poll-workers."

No attempt that Blaze and Clark's team made to breach the ES&S DRE, optical scanner, and batch scanner failed. The locks could be picked with paperclips (though the keys were identical for every machine). The "tamper-proof" seals could be removed and reapplied using liquid nitrogen, lighter fluid, or steam—or they could be bought online and replaced. No password was required to recalibrate touchscreens in such a way as to make some areas of the screen, such as those required to vote for a particular candidate, unresponsive.

In order to tabulate votes, each machine has removable media (such as a memory card) that is physically brought to the county headquarters to be counted by the central computer running the election management system.

The U-Penn EVEREST team discovered in the ES&S machines they attacked that the removable media that stored both the ballot information and the votes was unencrypted. Most importantly, it could be used without a password to alter firmware and upload a

virus that could propagate through the Election Management System to affect results for the entire county. Either a poll-worker or a voter could enter a voting booth, bypass the tamper-proof seals, spring the lock, and introduce a virus that could re-tally results for the entire county.

> *"Every current e-voting system has serious, exploitable vulnerabilities."*

"It's true what they say," Sandy Clark laughed sardonically in her 2008 presentation. "One voter *can* make a difference."

In a summation of the EVEREST findings, U-Penn team-leader Blaze (along with team-leaders from Penn State and WebWise Security) concluded, "There was a pervasive lack of quality in the implementation (coding and manufacturing) of these systems. Failures were present in almost every device and software module we investigated."

Professor Dan Wallach, manager of Rice University's Computer Security Lab, was part of the California TTBR, which he said "found all the same things as Ohio's EVEREST… Every paperless electronic voting system has unacceptable security vulnerabilities. None would be robust against sophisticated attackers." In one bemused but representative remark, a member of the TTBR's team reviewing the proprietary source code said of Sequoia systems, "We could not find a single instance of correctly used cryptography that successfully accomplished the security purposes for which it was apparently intended."

CREDIT: Diana Ofosu

The combined results of the TTBR and EVEREST reveal that in 2007, virtually every door and window in America's e-voting machines had been left open to entry-level hackers, to say nothing of their vulnerability to sophisticated attackers like nation-states. Indeed, it appeared as though the companies manufacturing machines critical to the functioning of American democracy had not bothered to hire expert information-security professionals, a problem exacerbated by their vehement refusal to submit their proprietary code to review by outside testers.

Immediately following the release of the TTBT and EVEREST reports, vendors recalled the named machines and patched them, though the summation by the EVEREST team foresaw those patches and essentially discounted them in advance, noting, "While some of the technical weaknesses we identified can be mitigated with improved procedural safeguards, others are more systemic. These structural flaws are more difficult to correct, and reliably correcting them will require re-engineering and redesign of the equipment and software itself."

Bernhard's reservations about the patches are striking. "Given the competency shown by these companies in the past," he said, "my intuition is that whatever patching they may have done is vastly insufficient. I have essentially no confidence in the vendors that they have actually fixed issues. And if they have, I have no confidence that

they've mitigated enough threats that we can consider the machines safe."

Voting technology provides a false sense of security—and opens up new vulnerabilities

As a result of the work of investigators affiliated with the TTBR and EVEREST, as well as more recent investigations by researchers like Haldeman at the University of Michigan (who installed Pac-Man on a Sequoia DRE in 2010) or Edward Felton and Andrew Appel at Princeton, paperless DRE machines have become less popular. In 2016, their use had declined more than 15 percent since the last presidential election.

But in many ways, the remaining uneasily patched DREs have been cast as the bogeyman of voting machines—while the other systems' remarkable vulnerabilities have been ignored.

Cybersecurity professional Mark Graff, former CISO of NASDAQ, has briefed Congress and Pentagon on voting cybersecurity. He says preying on DREs is "possible, but not particularly attractive from an attacker's point of view… A much more attractive approach would be to attack those machines that are aggregating the votes… If you attack at the lowest part of the food chain, where networked machines are being used to gather vote totals from the precincts, before cross-checking has taken place, that's a fairly sensitive moment… where the individual totals have been accumulated, but before there's a cross-check."

> *"I have no confidence that they've mitigated enough threats that we can consider the machines safe."*

Aggregation systems, he notes, handle significantly larger numbers of votes than precinct machines, and are likelier to be connected to the internet.

Relying on the security of the air gap is a mistake, Wallach explained in his address to the House Committee on Space, Science & Technology. An "air gap" is a physical and communication disconnect between one machine and the next created by a lack of internet, WiFi, or other networking connection. "The Stuxnet malware, for example,

was engineered specifically to damage nuclear centrifuges in Iran, even though those centrifuges were never connected to the internet," Wallach noted. "We don't know exactly how the Stuxnet malware got in, but it did nonetheless."

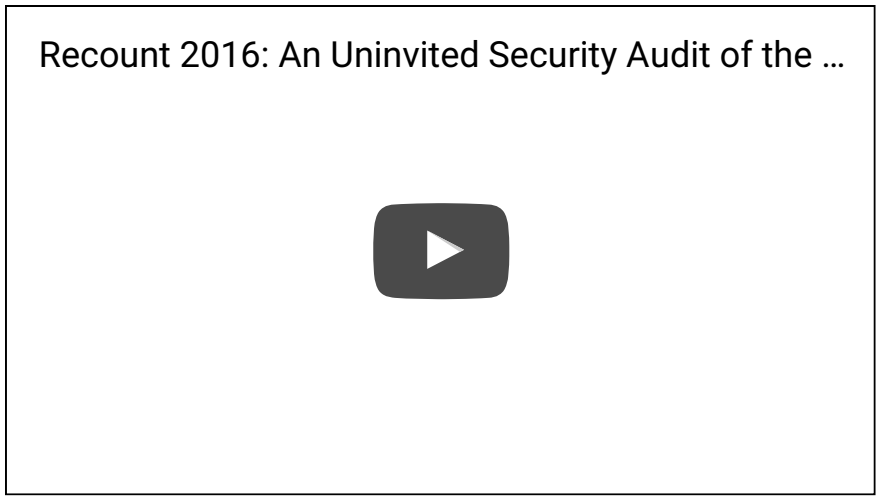
Unfortunately, Wallach says that the security of supposedly air-gapped systems is a great deal flimsier than it's sold as being. "When you dig down, [many vendors] often have election management systems connected to the Internet, albeit behind firewalls, VPNs, or other such devices. It's incorrect to call such systems 'never connected.'" Wallach also noted that certification requirements are such that all elections management systems run on unpatched, obsolete operating systems (usually Windows 2000 or XP), which are subject to a variety of vulnerabilities that have been well-known for years.

But because air-gapped voting machines run on ballot and tabulation software centrally programmed elsewhere, the air gap is a moot point.

"These are small businesses with little to no operational security oversight on the part of the government," Bernhard explained. "So any breach would be hard to detect. Moreover, it's likely that ballots are programmed by computers that are in some way connected to the Internet."

In a presentation to the hacking convention Chaos Communication Congress (CCC) in December 2016, Bernhard and Halderman argued that in order to overcome the U.S.'s diverse, decentralized voting technologies, an attacker would need only determine (with help from pre-election assessments like Nate Silver's) which states are likely to result in close votes, select two, then preordain an Electoral College victory by shifting those states' votes by less than 1 percent of the total (which would dispel suspicion).

Watch:



To underline the lack of security at the ballot-programming level, Bernhard and Halderman displayed a screenshot of the "Who We Are" section of the webpage for Governmental Business Systems (GBS), an Illinois-based company that programs ballots for the state of Michigan. (They noted that GBS's website didn't even have basic Transport Layer Security encryption enabled.) This website offered names of all of GBS's employees, along with their email addresses. From this, they pointed to the administrative assistant as a possible target.

But with the email addresses for every person in the company on display, it would be easy enough to find one person likely to be convinced enough by a professional-looking email purporting to come from Gmail, Facebook, LinkedIn, or Twitter to click on a link or attachment. A more sophisticated social engineering attack would rely on some research: running the names of the firm's employees through search engines to discover their hobbies and interests, finding out who has an Etsy store, who's a supporter of one cause or another, and who's part of a public fantasy football league, then sending convincing hobby-related emails asking the target to click on an infected PDF that would open attackers' access to GBS's systems. From there, a sophisticated hacker could introduce malware into the central programming of the ballots. Each vote would run through malware, ensuring a preferred candidate always wins.

The most effective attack is the one that goes undetected

What casts well-deserved doubt on paperless DREs is their lack of physical evidence of tampering. In theory, this should make optical-scan voting safer, since even if attackers are able to change digital results of scanning, the paper record would still tell the truth.

However, as Bernhard and Halderman have pointed out, a paper trail only matters if it's actually examined as part of the regular election process. In the U.S., it almost never has been. The 2016 election cycle endured multiple instances of hacking from attackers based in a hostile nation-state, and it resulted in a surprising outcome in which a candidate who polled as significantly less likely to win nonetheless became president—yet few if any states looked at any paper ballots created by computers to determine if there was evidence of attempts to breach their systems.

"Most states never look at the paper," Bernhard said in their CCC presentation. "You have a great way to defend against an attack, but you never use it."

"If even in 2016 we're not going to look at any of the paper," Halderman added, "Well, it might as well not be there."

Following up with ThinkProgress, Bernhard noted that attackers attempting to change the outcome of an election would try to remain undetected, making changes just large enough to accomplish their goals.

"If they didn't care about the outcome and just wanted to destroy confidence, they could try to be detected," he said. "Hilariously, based on how messy our election system is, even if someone tried to carry out an easily detected attack, we still might not notice it."

Politicizing election security: Make it a "states' rights" argument

However, in the wake of the fraught 2016 election—during which voter registries and John Podesta's personal emails were hacked, and the Democratic National Committee endured a series of attacks that began in 2015 and continued for months—the first response from the Republican-dominated House has been to vote to close the commission responsible for helping states secure their elections. [Disclosure: Podesta founded the Center For American Progress Action Fund, which is the parent organization of ThinkProgress.]

On February 7, the Committee on House Administration approved H.R. 634, the Election Assistance Commission Termination Act.

Committee chairman Rep. Gregg Harper (R-MS) released a statement calling the Election Assistance Commission (EAC) "an agency that has outlived its usefulness, mismanaged its resources, and cost taxpayers millions. […] Bottom line, the agency does not administer elections and the time to eliminate the EAC has come."

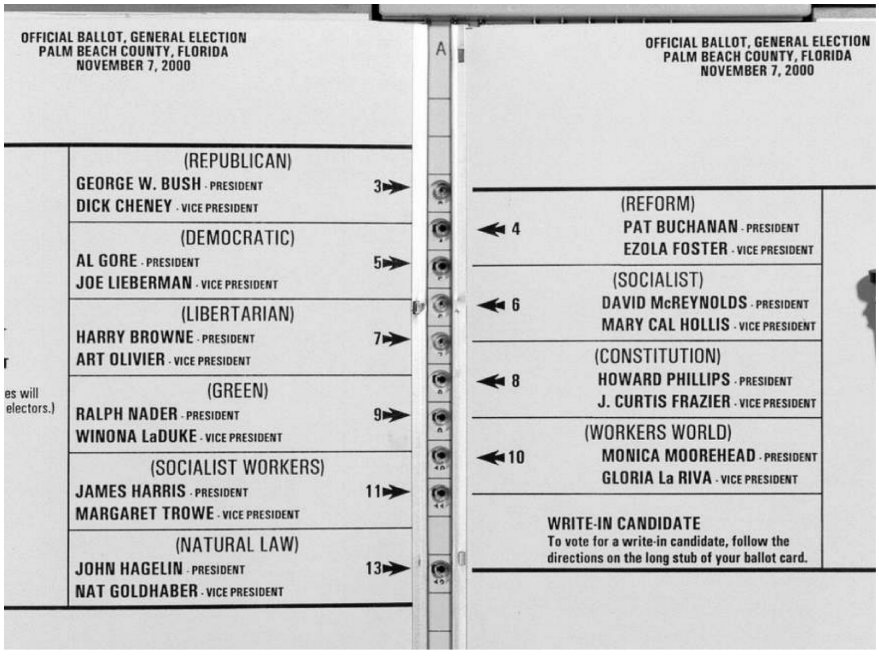
The EAC has been the target of Republicans for years. Legitimate complaints against the nominally nonpartisan organization certainly exist: it was found in 2009 to have discriminated in hiring for its General Counsel position, rejecting an attorney on the basis that he was a Republican. In 2010 it lost its quorum of Commissioners (until 2014). At that point the Republicans, led by Harper, began their

attempts to eliminate it, arguing that its comparatively tiny budget of roughly $11 million (around 0.0004 percent of the federal budget) was a waste of money.

"It has less to do with elections and more to do with the parties' views about the federal government," explained Doug Chapin, director of the program for excellence in election administration at the University of Minnesota's Humphrey School of Public Affairs. "My sense is that opponents of the EAC see an opportunity to demonstrate that they can shrink the federal government by eliminating the agency."

In 2015, the National Association of Secretaries of State renewed its decade-old call for the dissolution of the EAC, noting its initial 2005 motion to defund the EAC was intended to "prevent the EAC from eventually evolving into a regulatory body."

The EAC was a byproduct of the controversial Help America Vote Act (HAVA) in 2002, and its earliest role was to distribute $830 million in federal HAVA funds to states for upgrading voting systems.



Palm Beach Chad Ballot from the 2000 Election; CREDIT:

"The EAC sets federal guidelines for certification of voting systems," said Lawrence Norden, deputy director of the Brennan Center's Democracy Program. "A critical part of those certification guidelines

has to do with security. Forty-seven states rely on the federal certification program in some way."

"The fact is that all of these machines are aging out."

The EAC's quality-monitoring program requires vendors of election systems to notify the EAC if any anomalies are discovered within their systems. The EAC can also strip certification, which vendors need to sell voting equipment. Testing and certification of voting systems used to be done by a consortium of state election directors, explained Pamela Smith, president of the Verified Voting Foundation, a non-profit NGO dedicated to "safeguarding elections in the digital age." But the EAC "really professionalized it. They made it much more stringent and rigorous. There's a lot of transparency there."

What's startling about the new resolution calling for termination of the EAC is that it makes no attempt to transfer the certification program to another agency. Testing and certification simply seem to disappear.

Are voting machines part of the country's critical infrastructure?

One potential stand-in for the EAC is the Department of Homeland Security (DHS), which offers an array of cybersecurity information, tools, and services. Last summer, when news broke that Arizona and Illinois voter-registration data had been breached by Russian hackers, the DHS underlined the array of services (such as vulnerability scanning) it offered at no cost to states.

"At first there was a trickle of interest, maybe three states. Then it was eleven, then twenty, then by election day almost all the states had interacted with the DHS in some way or other," Smith said. This sudden burst of demand has a capacity to overwhelm DHS cybersecurity staff and resources. To allow for that, the Obama Administration's DHS designated elections systems—polling places, election machines, voter databases, and other information technology—part of America's "critical infrastructure" (along with things like water systems, dams, and the power grid) in early January.

"This designation does not mean a federal takeover, regulation, oversight or intrusion concerning elections in this country," said Jeh Johnson, outgoing Secretary of Homeland Security.

> *"[T]he only real way to secure them is to destroy them and start over."*

Nonetheless, the move prompted immediate outcry. On February 18, the National Association of Secretaries of State (NASS) adopted a resolution opposing the designation. Connecticut Secretary of State Denise Merrill, a Democrat who is also president of NASS, called on the Trump administration to rescind the critical infrastructure label.

The same week, Dan Wallach at Rice University published a Wired op-ed titled "Want Secure Elections? Then Maybe Don't Cut Security Funding." He argued the move to cut the EAC was "evidence of a radical disconnect between a handful of influential House Republicans and nearly everyone else—including the scientific community, leading cybersecurity experts, and even the White House—who contend that voting vulnerabilities are a serious problem."

Electronic voting systems, Norden underlines, age a great deal faster than mechanical ones—which means that vulnerabilities reveal themselves at a much greater frequency than before.

"We don't just keep the same equipment for 40 years anymore," he said in an interview. In the next few years, dozens of states and hundreds if not thousands of counties will be updating equipment purchased through HAVA. The bipartisan Presidential Commission on Election Administration called that coming shift "an impending crisis."

"The fact is that all of these machines are aging out," says Norden. "If you suddenly get rid of the Federal certification program, you're severely limiting the choices of the next generation of systems that jurisdictions can buy, and you're left with older systems that are likely to be less secure. They are not likely to have passed through more rigorous certification standards."

While voting systems remain frozen in the Bush-administration era, attackers in the present are expanding their approaches.

"Our adversaries might have a variety of goals," Wallach told the House Committee on Space, Science & Technology at a hearing in September. "If they simply want to disrupt our elections, and if they're unconcerned with [whether they're noticed], then even very modest or crude attacks will raise doubts and damage voter confidence in the election outcome. Trust in our election systems is fragile and is potentially easily shaken by our adversaries."

Making future elections secure—and accessible

The challenge of safeguarding elections is multifaceted, but very few security experts seem inclined to agree with the House Republicans in leading by dismantling the EAC.

"[Deciding] the role of the federal government in writing standards for these voting machines [is] a very tricky thing," said Mark Graff, the former former CISO of NASDAQ.

He cautions against any kind of centralized system of election tallies —like that in use during the 2014 Ukraine election. Instead, he likens the variety of voting systems to planting a variety of grain, rather than a monoculture that one blight can wipe out. "One of the protections

for our electoral system is the disparate nature of all these systems… We've got a crazy-quilt system in voting security, and I think that offers some hardiness and strength… Any uniform system would just invite focused attack on its weakest point."

However, Graff acknowledged that the security of federal elections is a matter of national security. To balance the interests, he suggested the government offer guidelines (rather than imposing standards) for federal elections and provide states with assistance in encrypting voting data and databases, securing voting aggregation systems with at least two-factor authentication, and physically quarantining the machines prior to each election. At present, NIST offers basic recommendations on protecting general computer systems, and he hopes to see NIST produce a similar set of recommendations specifically for voting systems.

> *"[E]ven if someone tried to carry out an easily detected attack, we still might not notice it."*

In order to build security in, the machines themselves would likely need to be re-engineered, an argument the EVEREST testers first made a decade ago. At the same time, the EVEREST project's testers called for elections to run on open-source software that would constantly be tested by hackers—rather than feeble proprietary software shielded jealously from testing or criticism by vendors. Several vendors have emerged to offer open-source elections software, but Norden says it is not in use anywhere in the U.S. at present.

A few jurisdictions—including Los Angeles, San Francisco City/County, and Travis County, Texas—are in the process of developing their own voting systems. Everyone else will continue to vote with whatever the vendors offer, whether it's new technology purchased in the near future, or aging, problematic technology.

"We should be hardening our voting technology to make it more resistant to attacks, to buffer-overflows, to basic security vulnerabilities," Halderman told the CCC in December. "But even this, it's not sufficient. This raises the bar to an attack, but we need to make sure we're getting a physical safeguard […] by having a paper record in place for every vote. We have to go from 70 percent [of

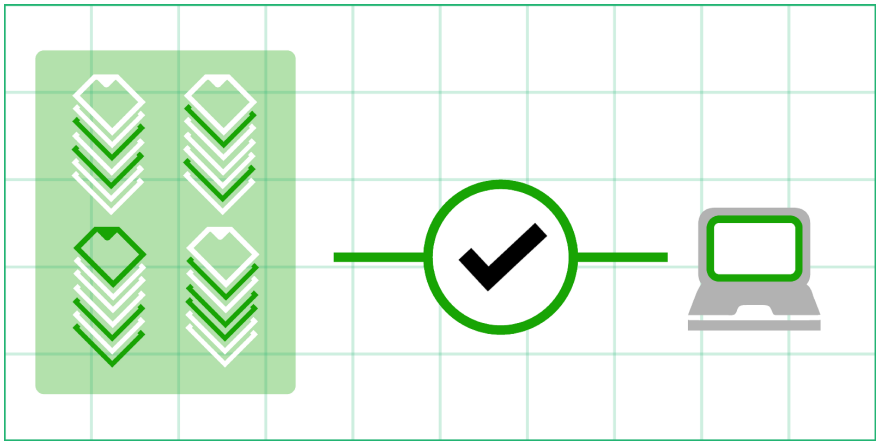
polls] to 100 percent, and there are still a number of states that need to take action to do so. But most importantly, we need to make sure every state actually makes use of that evidence. We need […] a cheap and easy-to-use mechanism that states can use to make sure the electronic totals are right, by looking at enough of the paper [to guard against tampering]."

Graff agrees. While he acknowledges that accessibility issues for people with disabilities and the ease of voting for stationed military and others outside the country are important reasons for the continued use of electronic voting technology, he also said, "paper really is the gold standard… Paper ballots are a marvelous thing to have. We ought to be going back and auditing to see if there has been any tampering."

There's never been a forensic-level audit of federal election technology, Graff said, so we have little idea what kinds of intrusion —if any—have been attempted or successful.

"Nation-state actors and players at that level are very good at covering their tracks: the fact that you didn't find anything wouldn't be determinative. But we certainly should take a look and see."

Pamela Smith of the Verified Voting Foundation said that while the EAC has been effective in offering testing and certification, they have not yet advised any kind of post-election auditing, or required systems to be auditable.



Ideally, paper records would be actively checked against electronic vote counts; CREDIT: Diana Ofosu

"Audits should be everywhere," she said. "About three quarters of the states have auditable systems, some more easily auditable than others… Just over half use some kind of post-election audit. Most of those are not extremely robust… but even the ones that are pretty weak have in fact found outcome-changing errors."

Presuming that simply having a recount measure in place is all a state needs to appease uncertainties about an election's outcome is an artifact of a simpler era in elections technology.

At the moment, the after-the-fact security of elections is often predicated on the capability of candidates to demand (and pay for) recounts, presuming they're undaunted by the accusation of being called sore losers. But recount legislation can be an obstacle of its own. Halderman and Bernhard discovered that in Pennsylvania, where 70 percent of votes are on DREs with no paper trail, three citizens from every *precinct* to be recounted need to post a bond, swearing they believe fraud has taken place. With more than 9,000 precincts across Pennsylvania, a statewide recount would require 277,000 people to swear they believed the vote was fraudulent. As Halderman points out, this is cart-before-horse thinking: the point of a recount is to look for evidence, so requiring evidence to merit searching for evidence is problematic.

At the moment, some states have a provision for an automatic partial recount in a close election, selecting around 5 percent of ballots to consider.

"The challenge there is that, in many cases," Smith says, "especially in a close margin, you actually have to count more in order to be sure that the count was correct.

What Halderman and Bernhard specifically called for in their CCC presentation was "statistical risk-limiting audits." Risk-limiting audits aren't complete audits of the entire election, but rather audits of a cross-section of enough ballots to establish with confidence that a complete audit would achieve the same result as the official tally.

Risk-limiting audits are cheaper than complete audits, but any mandatory audits would cost money, Smith acknowledges. However, she argues that they would pay dividend in election security.

> "We spend a lot on campaigns," she said, "but we don't spend a lot on election administration…. We can invest in [things like auditing] in order to have reliable confidence in the outcome of elections."

Compared to what the federal government could be investing in election security, Norden said, the EAC's roughly $10 million budget "is nothing."

> "The cost to do really well is probably going to be a lot more than $10,000,000 a year."

The cost of not doing "really well," on the other hand, could prove incalculable.