U.S. Senate Select Committee on Intelligence

Russian Interference in the 2016 U.S. Elections

Expert Testimony by
J. Alex Halderman
Professor of Computer Science, University of Michigan

June 21, 2017

Chairman Burr, Vice Chairman Warner, and members of the Committee, thank you for inviting me to speak today about the security of U.S. elections. I'm here to tell you not just what I think, but about concerns shared by hundreds of experts from across cybersecurity research and industry. Such expertise is relevant because elections—the bedrock of our democracy—are now on the front lines of cybersecurity, and they face increasingly serious threats. Our interest in this matter is decidedly non-partisan; our focus is on the integrity of the democratic process, and the ability of the voting system to record, tabulate, and report the results of elections accurately.

My research in computer science and cybersecurity tackles a broad range of security challenges.[1] I study attacks and defenses for the Internet protocols we all rely on every day to keep our personal and financial information safe. I also study the capabilities and limitations of the world's most powerful attackers, including sophisticated criminal gangs and hostile nation states. A large part of my work over the last ten years has been studying the computer technology that our election system relies on.[2] In this work, I often lead the "red team," playing the role of a potential attacker to find where systems and practices are vulnerable and learn how to make them stronger.

I know firsthand how easy it can be to manipulate computerized voting machines. As part of security testing, I've performed attacks on widely used voting machines, and I've had students successfully attack machines under my supervision.

[1] My curriculum vitae and research publications are available online at https://jhalderm.com.
[2] For an accessible introduction to the security risks and future potential of computer voting technologies, see my online course, *Securing Digital Democracy*, which is available for free on Coursera: https://www. coursera.org/learn/digital-democracy.

U.S. Voting Machines Are Vulnerable

As you know, states choose their own voting technology.[3] Today, the vast majority of votes are cast using one of two computerized methods. Most states and most voters use the first type, called optical scan ballots, in which the voter fills out a paper ballot that is then scanned and counted by a computer. The other widely used approach has voters interact directly with a computer, rather than marking a choice on paper. It's called DRE, or direct-recording electronic, voting. With DRE voting machines, the primary records of the vote are stored in computer memory.[4]

Both optical scanners and DRE voting machines are computers. Under the hood, they're not so different from your laptop or smartphone, although they tend to use much older technology—sometimes decades out of date.[5] Fundamentally, they suffer from security weaknesses similar to those of other computer devices. I know because I've developed ways to attack many of them myself as part of my research into election security threats.

Ten years ago, I was part of the first academic team to conduct a comprehensive security analysis of a DRE voting machine. We examined what was at that time the most widely used touch-screen DRE in the country,[6] and spent several months probing it for vulnerabilities. What we found was disturbing: we could reprogram the machine to invisibly cause any candidate to win. We also created malicious software—vote-stealing

---

[3] In many states, the technology in use even differs from county to county. Verified Voting maintains an online database of the equipment in use in each locality: https://www.verifiedvoting.org/verifier/.

[4] Some DREs also produce a printed record of the vote and show it briefly to the voter, using a mechanism called a voter-verifiable paper audit trail, or VVPAT. While VVPAT records provide a physical record of the vote that is a valuable safeguard against cyberattacks, research has shown that VVPAT records are difficult to accurately audit and that voters often fail to notice if the printed record doesn't match their votes. For these reasons, most election security experts favor optical scan paper ballots. See: S. Goggin and M. Byrne, "An Examination of the Auditability of Voter Verified Paper Audit Trail (VVPAT) Ballots." In *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop*, August 2007. Available at: http://www.accurate-voting.org/wp-content/uploads/2007/08/evt07-goggin.pdf. See also: B. Campbell and M. Byrne, "Now Do Voters Notice Review Screen Anomalies?" In *Proceedings of the 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop*, August 2009. Available at: http://chil.rice.edu/research/pdf/CampbellByrne_EVT_(2009).pdf.

[5] In 2016, 43 states used computer voting machines that were at least 10 years old—close to the end of their design lifespans. Older hardware and software generally lacks defenses that guard against more modern attack techniques. See: L. Norden and C. Famighetti, "America's Voting Machines at Risk," Brennan Center, 2015. https://www.brennancenter.org/publication/americas-voting-machines-risk. See also: S. Checkoway, A. Feldman, B. Kantor, J. A. Halderman, E. W. Felten, and H. Shacham, "Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage." In *Proceedings of the 2009 USENIX/ACCURATE/IAVoSS Electronic Voting Technology Workshop*, August 2009. Available at: https://jhalderm.com/pub/papers/avc-evt09.pdf.

[6] The machine was the Diebold AccuVote TS, which is still used statewide in Georgia in 2017.

code—that could spread from machine-to-machine like a computer virus, and silently change the election outcome.[7]

Vulnerabilities like these are endemic throughout our election system. Cybersecurity experts have studied a wide range of U.S. voting machines—including both DREs and optical scanners—and in *every single case,* they've found severe vulnerabilities that would allow attackers to sabotage machines and to alter votes.[8] That's why there is overwhelming consensus in the cybersecurity and election integrity research communities that our elections are at risk.

Cyberattacks Could Compromise Elections

Of course, interfering in a state or national election is a bigger job than just attacking a single machine. Some say the decentralized nature of the U.S. voting system and the fact that voting machines aren't directly connected to the Internet make changing a state or national election outcome impossible. Unfortunately, that is not true.[9]

Some election functions are actually quite centralized. A small number of election technology vendors and support contractors service the systems used by many local governments. Attackers could target one or a few of these companies and spread malicious code to election equipment that serves millions of voters.

Furthermore, in close elections, decentralization can actually work against us. An attacker can probe different areas of the most important "swing states" for vulnerabilities, find the areas that have the weakest protection, and strike there.[10] In a close election, changing a few votes may be enough to tip the result, and an attacker can choose where—and on which equipment—to steal those votes. State and local elections are also at risk.

---

[7] A. J. Feldman, J. A. Halderman, and E. W. Felten, "Security Analysis of the Diebold AccuVote-TS Voting Machine." In *Proceedings of the 2007 USENIX/ACCURATE Electronic Voting Technology Workshop* (EVT), August 2007. The research paper and an explanatory video are available at: https://citp.princeton.edu/research/voting/.

[8] For a partial bibliography of voting machine attack research, see: J. A Halderman, "Practical Attacks on Real-world E-voting." In F. Hao and P. Y. A. Ryan (eds.), *Real-World Electronic Voting: Design, Analysis and Deployment*, CRC Press, December 2016. Available at: https://jhalderm.com/pub/papers/ch7-evoting-attacks-2016.pdf.

[9] I explained how attackers can bypass these obstacles in a recent congressional briefing: *Strengthening Election Cybersecurity*, May 15, 2017. The video is available at https://www.electiondefense.org/congressional-briefings-cyber-security/.

[10] For a more detailed description of how adversaries might select targets, see J. A. Halderman, "Want to Know if the Election was Hacked? Look at the Ballots," November 2016, available at: medium.com/@jhalderm/want-to-know-if-the-election-was-hacked-look-at-the-ballots-c61a6113b0ba.

Our election infrastructure is not as distant from the Internet as it may seem.[11] Before every election, voting machines need to be programmed with the design of the ballot, the races, and candidates. This programming is created on a desktop computer called an election management system, or EMS, and then transferred to voting machines using USB sticks or memory cards. These systems are generally run by county IT personnel or by private contractors.[12] Unfortunately, election management systems are not adequately protected, and they are not always properly isolated from the Internet. Attackers who compromise an election management system can spread vote-stealing malware to large numbers of machines.[13]

Russian Attack Attempts: The Threats Are Real

The key lesson from 2016 is that hacking threats are real.

This month, we've seen reports detailing Russian efforts to target voter registration systems in up to 39 states[14] and to develop a capability to spread an attack from an election technology vendor to local election offices.[15] Attacking the IT systems of

---

[11] Fortunately, the U.S. has resisted widespread use of Internet voting—a development that would paint a fresh bull's eye on our democratic system. I myself have demonstrated attacks against Internet voting systems in Washington, D.C., Estonia, and Australia. See:
S. Wolchok, E. Wustrow, D. Isabel, and J. A. Halderman, "Attacking the Washington, D.C. Internet Voting System." In *Proceedings of the 16th Intl. Conference on Financial Cryptography and Data Security*, February 2012. Available at: https://jhalderm.com/pub/papers/dcvoting-fc12.pdf.
D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman, "Security Analysis of the Estonian Internet Voting System." In *Proceedings of the 21st ACM Conference on Computer and Communications Security* (CCS), November 2014. Available at: https://jhalderm.com/pub/papers/ivoting-ccs14.pdf.
J. A. Halderman and V. Teague, "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election." In *Proceedings of the 5th International Conference on E-voting and Identity*, September 2015. Available at: https://arxiv.org/pdf/1504.05646v2.pdf.
For a broader discussion of why secure Internet voting systems are likely decades away, see:
R. Cunningham, M. Bernhard, and J. A. Halderman, "The Security Challenges of Online Voting Have Not Gone Away." IEEE Spectrum, November 3, 2016. http://spectrum.ieee.org/tech-talk/telecom/security/the-security-challenges-of-online-voting-have-not-gone-away.

[12] In my own state, Michigan, about 75% of counties outsource pre-election programming to a pair of independent service providers. These are small companies with 10–20 employees that are primarily in the business of selling election supplies, including ballot boxes and "I Voted" stickers.

[13] See, for example, J. Calandrino, et al., "Source Code Review of the Diebold Voting System," part of the California Secretary of State's "Top-to-Bottom" Voting Systems Review, July 2007. Available at: https://jhalderm.com/pub/papers/diebold-ttbr07.pdf.

[14] M. Riley and J. Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known." *Bloomberg*, June 13, 2017. https://www.bloomberg.com/politics/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections.

[15] M. Cole, R. Esposito, S. Biddle, and R. Grim, "Top-secret NSA Report Details Russian Hacking Efforts Days Before 2016 Election." *The Intercept*, June 5, 2017. https://theintercept.com/2017/06/05/top-secret-nsa-report-details-russian-hacking-effort-days-before-2016-election/.

vendors and municipalities could put the Russians in a position to sabotage equipment on election day, causing voting machines or electronic poll books to fail, resulting in long lines or other disruptions. The Russians could even have engineered this chaos to have a partisan effect, by targeting localities that lean heavily towards one candidate or another.

Successful infiltration of election IT systems also could have put the Russians in a position to spread an attack to the voting machines and potentially steal votes. Although the registration systems involved were generally maintained at the state level, and most pre-election programming is performed by counties or outside vendors, counties tend to be even less well defended than state governments. They typically have few IT support staff and little, if any, cybersecurity expertise.

Another approach that the Russians might have been planning is to tamper with the voting system in an obvious, easily discovered way, such as causing reporting systems to send the news media incorrect initial results on election night. Even if the problem was corrected and no actual votes were changed, this would cause uncertainty in the results and widespread distrust of the system, which would injure our democratic processes. If voters cannot trust that their votes are counted honestly, they will have reason to doubt the validity of elections.[16]

I don't know how far the Russians got in their effort to penetrate our election infrastructure, nor whether they interfered with equipment on election day. (As far as the public knows, no voting equipment has been forensically examined to check whether it was successfully attacked.) But there is no doubt that Russia has the technical ability to commit widescale attacks against our voting system, as do other hostile nations. As James Comey testified here two weeks ago, we know "They're coming after America," and "They'll be back."[17]

Practical Steps to Defend Election Infrastructure

We must start preparing now to better defend our election infrastructure and protect it from cyberattacks before the elections in 2018 and 2020. The good news is, we know how to accomplish this. Paper ballots, audits, and other straightforward steps can make elections much harder to attack.

---

[16] See, as one example, E. H. Spafford, "Voter Assurance." NAE *The Bridge*, December 2008. https://www.nae.edu/19582/Bridge/VotingTechnologies/VoterAssurance.aspx.

[17] Testimony of former FBI Director James B. Comey before the Senate Select Committee on Intelligence, June 8, 2017.

I have entered into the record a letter from over 100 computer scientists, security experts, and election officials. This letter recommends three essential measures that can safeguard U.S. elections:

- First, we need to replace obsolete and vulnerable voting machines, such as paperless systems, with optical scanners and paper ballots—a technology that 36 states already use. Paper provides a resilient physical record of the vote[18] that simply can't be compromised by a cyberattack. President Trump made this point well shortly before the election in an interview with Fox News. "There's something really nice about the old paper-ballot system," he said. "You don't worry about hacking. You don't worry about all the problems that you're seeing."[19]

- Second, we need to consistently and routinely check that our election results are accurate, by inspecting enough of the paper ballots to tell whether the computer results are right.[20] This can be done with what's known as risk-limiting audits.[21] Such audits are a common-sense quality control.[22] By manually checking a relatively small random sample of the ballots, officials can quickly and affordably provide high assurance that the election outcome was correct.

Optical scan ballots paired with risk-limiting audits provide a practical way to detect and correct vote-changing cyberattacks. They may seem low-tech, but they are a reliable, cost-effective defense.[23]

---

[18] Of course, paper ballots can be tampered with too, by people handling them. Optical scan tabulation has the advantage that it produces both paper and electronic records. As long as officials check that both sets of records agree, it would be very difficult for criminals to alter the election outcome without being detected, whether by a cyberattack or by old-fashioned ballot manipulation.

[19] See: http://www.businessinsider.com/donald-trump- election-day-fox-news-2016-11.

[20] At least 29 states already require some form of post-election audit. However, since the procedures in most states are not designed as a cyber defense, the number of ballots that are audited may be much too low or geographically localized to reliably detect an attack. Some states also allow auditing by rescanning paper ballots through the same potentially compromised machines. Results from paperless DRE voting machines cannot be strongly audited, since there is no physical record to check. For state-by-state details, see National Conference of State Legislatures, "Post-election Audits," June 2017. Available at: http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx.

[21] For a detailed explanation of risk-limiting audits, see J. Bretschneider et al., "Risk-Limiting Post-Election Audits: Why and How." Available at: https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf. New Mexico already requires something similar to a risk-limiting audit, and Colorado is implementing risk-limiting audits starting in 2017. Risk-limiting audits have been tested in real elections in California, Colorado, and Ohio.

[22] One of the reasons why post-election audits are essential is that pre-election "logic and accuracy" testing can be defeated by malicious software running on voting machines. Vote-stealing code can be designed to detect when it's being tested and refuse to cheat while under test. Volkswagen's emission-control software did something similar to hide the fact that it was cheating during EPA tests.

[23] Former CIA director James Woolsey and Lt. Col. Tony Shaffer call for paper ballots and auditing in a May 12, 2017 op-ed in Fox News: "Ultimately, we believe the solution to election insecurity lies in

- Lastly, we need to raise the bar for attacks of all sorts—including both vote tampering and sabotage—by conducting comprehensive threat assessments and by applying cybersecurity best practices to the design of voting equipment[24] and the management of elections.

These fixes aren't expensive. Replacing insecure paperless systems nationwide would cost between $130 million and $400 million.[25] Running risk-limiting audits nationally for federal elections would cost less than $20 million a year.[26] These amounts are vanishingly small compared to the national security improvement the investment buys. Yet such measures could address a prime cyber challenge, boost voter confidence, and significantly strengthen a crucial element of our national security. They would also send a firm response to any adversaries contemplating interfering with our election system.

Election officials have an extremely difficult job, even without having to worry about cyberattacks by hostile governments. The federal government can make prudent and cost-effective investments to help them defend our election infrastructure and uphold voters' confidence. With leadership from across the aisle, and action in partnership with the states, our elections can be well protected in time for 2018 and 2020.

Thank you for the opportunity to testify. I look forward to answering any questions.

President Reagan's famous old adage: 'trust but verify'." http://www.foxnews.com/opinion/2017/05/12/america-s-voting-systems-need-security-upgrades-it-s-time-to-beef-up-cybersecurity.html.

[24] One notable effort to develop secure voting equipment is STAR-Vote, a collaboration between security researchers and the Travis County, Texas elections office. STAR-Vote integrates a range of modern defenses, including end-to-end cryptography and risk limiting audits. See S. Bell et al., "STAR-Vote: A Secure, Transparent, Auditable, and Reliable Voting System." USENIX Journal of Election Technology and Systems (JETS) 1(1), August 2013. https://www.usenix.org/system/files/conference/evtwote13/jets-0101-bell.pdf.

[25] Brennan Center, "Estimate for the Cost of Replacing Paperless, Computerized Voting Machines," June 2017. https://www.brennancenter.org/sites/default/files/analysis/New_Machines_Cost_Across_Paperless_Jurisdictions%20%282%29.pdf. This cost might be significantly reduced by developing voting equipment based on open-source software and commercial off-the-shelf (COTS) hardware.

[26] This estimate assumes that auditing a federal race will have an average cost similar to manually recounting 10% of precincts. In a risk-limiting audit, the actual number of ballots that must be checked varies with, among other factors, the margin of victory.