MATT BLAZE [1]

TESTIMONY BEFORE THE
US HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION

HEARING ON DEFENDING AGAINST ELECTION INTERFERENCE

NOVEMBER 19, 2019

[1] Professor and McDevitt Chair of Computer Science and Law, Georgetown University, 600 New Jersey Ave NW, Washington, DC 20001. *mab497@georgetown.edu.* Affiliation for identification only.

INTRODUCTION

Thank you for the opportunity to offer testimony on the important questions raised by the security of the technology used for elections in the United States.

For more than 25 years, my research and scholarship has focused on security and privacy in computing and communications systems, especially as we rely on insecure platforms such as the Internet for increasingly critical applications. My work has focused particularly on the intersection of this technology with public policy issues. For example, in 2007, I led several of the teams that evaluated the security of computerized election systems from several vendors on behalf of the states of California and Ohio.

I am currently the McDevitt Chair of Computer Science and Law at Georgetown University. From 2004 to 2018, I was a professor of Computer and Information Science at the University of Pennsylvania. From 1992 to 2004, I was a research scientist at AT&T Bell Laboratories. I hold a PhD in computer science from Princeton University, an MS in computer science from Columbia University, and a BS from the City University of New York. This testimony is not offered on behalf of any organization or agency.

In this testimony, I will give an overview of the security risks facing elections in the United States today, with emphasis on vulnerabilities inherent in electronic voting machines, as well as the exposure of our election infrastructure to disruption by national security adversaries. I have attempted, to the extent possible, to represent the current consensus of experts in the field, but space and time constraints limit my ability to be comprehensive or complete. An especially valuable resource, with comprehensive discussion and recommendations. is the recent National Academies "Securing the Vote" consensus study report.[2]

I offer three specific recommendations:

- Paperless ("DRE") voting machines should be phased out from US elections immediately, and urgently replaced with precinct-counted optical scan ballots that leave a direct artifact of voters' choices.
- Statistically rigorous "risk limiting audits" should be routinely conducted after *every* election, in *every* jurisdiction, to detect and correct software failures and attacks.
- State and local voting officials should receive access to significant additional resources, infrastructure, and training to help them protect their election management IT systems against increasingly sophisticated adversaries.

I. ELECTIONS AND SOFTWARE SECURITY

A consequence of our federalist system is that US elections are in practice highly decentralized, with each state responsible for setting its own standards and procedures for registering voters, casting ballots, and counting votes. The federal government has set only broad

[2] https://www.nap.edu/catalog/25120/securing-the-vote-protecting-american-democracy

standards for such issues as accessibility, but has historically been largely uninvolved in day-to-day election operations. In most states, the majority of election management functions are delegated to local county and town governments, which are responsible for registering voters, procuring voting equipment, creating ballots, setting up and managing local polling places, counting votes, and reporting the results of each contest. Consequently, thousands of individual local election offices shoulder the burden of managing and securing the voting process for most of the American electorate.

Elections in the US are among the most operationally and logistically complex in the world. Many jurisdictions have large numbers of geographically dispersed voters, and most elections involve multiple ballot contests and referenda. Baseline election security must account for sophisticated adversaries, ballot secrecy, fair access to the polls, and accurate reporting of results, making secure election management one of the most formidable – and potentially fragile – information technology problems in government

Computers and software play central roles in almost every aspect of our election process: managing voter registration records, defining ballots, provisioning voting machines, tallying and reporting results, and controlling electronic voting machines used at polling places.[3] The integrity and security of our elections are thus inexorably tied to the integrity and security of the computers and software that we rely on for these many functions.

The passage of the Help America Vote Act (HAVA) in 2002 accelerated the computerization of voting systems, particularly with respect to the ways in which voters cast their ballots at local polling stations. HAVA provided funds for states to replace precinct voting equipment with "accessible" technology. As implemented, however, some of this new technology has had the unfortunate unintended consequence of increasing, rather than decreasing, the risk of our elections being compromised by malicious actors.

A. Election Software and Hardware

A typical[4] county election office today depends on computerized systems and software for virtually every aspect of registering voters and conducting elections. Generally, an election office workflow will include at least the following pre- and post- election functions:

Voter registration – The ongoing maintenance of an authoritative database of registered voters in the jurisdiction, including the precinct-by-precinct "poll books" of voters (which might be on paper or in electronic form) that are used to check in voters at precinct polling stations.

Ballot definition – The pre-election process of creating data files that list the various contests, candidates, and rules (e.g., number of permitted choices per race) that will appear on the ballot. The ballot definition is used to print paper ballots, to define what is

[3] A typical election administration office is much like any modern enterprise, with local computer networks tying together desktop computers, printers, servers, and Internet access. This increasing connectivity served as a critical avenue in 2016 for what US intelligence agencies have identified as attacks by Russian military intelligence..

[4] The precise nature of the systems used and how they interact with one another will vary somewhat depending on the vendors from which the systems were purchased and the practices of the local jurisdiction.

displayed on touchscreen voting terminals, and to control the vote tallying and reporting software. Local races (such as school boards) may sometimes require that different ballot definitions be created for different precincts within a county in any given election.

Voting machine provisioning – The pre-election process of configuring the individual precinct voting machines for an election. This typically includes resetting internal memory and loading the appropriate ballot definition for each precinct. Depending on the model of voting machine, provisioning typically involves using a computer to write removable memory cards that are installed in each machine.

Absentee and early voting ballot processing – The process of reading and tabulating ballots received by mail and from early voting polling places. Mail votes are typically processed in bulk by high-volume optical scan ballot reading equipment.

Tallying and reporting – The post-election process of tabulating the results for each race received from each precinct and reporting the overall election outcomes. This process typically involves using a computer to read memory card media retrieved from precinct voting machines.

Each of the above "back end" functions employs specialized election management software running on computers. Depending on the size and practices of the county, the same computers may be used for more than one function (e.g., the ballot definition computer might also serve as the tallying and reporting computer). These computers are typically off-the-shelf desktop machines running a standard operating system (such as Microsoft Windows), often equipped with electronic mail and web browser software along with the specialized voting software. Election office computers are typically connected to one another via a wired or wireless local area network, which may have a direct or indirect connection (sometimes via a firewall) to the Internet.

In some jurisdictions, some of these election management functions (most often those concerned with voter registration databases and ballot definition), may be outsourced by a county or state to an election services contractor. These contractors provide jurisdictions with specialized assistance with such tasks as creating ballots in the correct format, managing voter registration databases, creating precinct poll books, and maintaining voting machines. The degree to which jurisdictions rely on outside contractors varies widely across the nation.

Much of the voting equipment used at precincts is computerized as well, although it is generally packaged in specialized hardware. This equipment includes:

Direct Recording Electronic (DRE) Voting Machines – DRE machines are special-purpose computers that display ballot choices to the voter (based on the ballot definition) and record voter choices. Both the ballot definition configuration and the vote count are typically stored on removable memory media.[5]

Optical Scan Ballot Readers – Optical scan ballot readers are specialized computers that read

[5] Some models of DRE can be equipped with a *Voter Verified Paper Audit Trail (VVPAT)* option in which the voters' selections are printed on a paper tape roll that is visible to the voter. VVPATs can assist with determining the voter's intent during a recount, but their efficacy depends on each voter's diligence in confirming that their choices are correctly recorded on the paper tape before they leave the voting booth. Research consistently suggests that, in practice, very few voters successfully perform this confirmation step.

voter-marked paper ballots. The ballot is read according to the ballot definition configuration (typically on removable memory media), and a tally is maintained in memory (also typically on removable media). The machine also captures the scanned ballots and stores them in a mechanically secured ballot box.

Ballot Marking Devices (BMDs) – Ballot marking devices are an assistive technology used in optical scan systems to allow visually or mobility impaired voters to create ballots for subsequent scanning. BMDs are similar in appearance to DRE machines in that they display (or read aloud) the ballot electronically, based on a ballot definition configuration, and accept voter choices for each race. However, instead of recording those choices in computer memory as DREs do, BMDs print a marked paper ballot that can then be submitted through an optical scan ballot reader.

Electronic Poll Books – These devices are typically tablet-style computers that contain an authoritative copy of the database of registered voters at each precinct. Electronic poll books are not used directly by voters, but rather by precinct poll workers as voters are checked in at their polling place. They are not used in all jurisdictions.

B. Software and Election Security

Securing complex software systems is notoriously difficult, and those that perform the various functions described above are no exception.[6] There are several avenues of vulnerability in such systems. Common software "bugs" often introduce vulnerabilities that can be exploited by an adversary to silently compromise the integrity of data or make unauthorized (and difficult to detect) changes to the behavior of systems. Configuration and system management errors (such as the use of vulnerable out-of-date platforms and weak passwords) can further compromise security. Computer networks (which are not generally used by precinct voting machines themselves but are commonly connected to back end systems in election offices) compound these risks by introducing the possibility of remote attack over the Internet.

The integrity of the vote today thus increasingly depends on the integrity of the software systems – running on voting machines and on county election office networks – over which elections are conducted. Any security weakness in any component of any of these systems can serve as a "weak link" that can allow a malicious actor to disrupt election operations, alter tally results, or disenfranchise voters.

In many electronic voting systems used today, a successful attack that exploits a software flaw might leave behind little or no forensic evidence. This can make it effectively impossible to determine the true outcome of an election or even that a compromise has occurred.

Unfortunately, these risks are not merely hypothetical or speculative. Many of the software and hardware technologies that support US elections today have been shown to suffer from serious and easily exploitable security vulnerabilities that could be used by an adversary to alter vote tallies or cast doubt on the integrity of election results.

[6] The fact that software systems can be, and often are, vulnerable to attack is not unique to election systems, of course. Serious data breaches are literally daily events across the public and private sectors, and cybersecurity is widely recognized to be a serious law enforcement and national security problem. To the extent that elections depend on software or are administered by networked computing systems, they are subject to all the same risks.

II. CURRENT ELECTRONIC VOTING SYSTEMS HAVE PROVEN VULNERABLE TO A RANGE OF KNOWN, EXPLOITABLE SECURITY FLAWS

A. Risks in Various Election Components

Security concerns about computerized voting systems have been raised from almost the moment such systems were first proposed. Most of these concerns have focused on electronic voting equipment used at polling stations, although the "back end" election management software used to manage voter registration, provision voting machines, and tally are at least equally critical to the integrity of the vote.

To be clear, all electronic voting technology can and does suffer from security vulnerabilities. The consequences of these vulnerabilities being successfully exploited, however, depends on the particular class of device and whether the technology permits effective post-election auditing to validate or recover correct election results.

1. Election Management IT Systems

As noted above, local jurisdictions rely on computers for almost every aspect of election administration. Official information for voters is distributed on public-facing websites. Voter registration records, used on election day to determine who is permitted to vote, are maintained in computerized databases. Ballots forms are created and edited on computers. Absentee ballot mailings are managed by computer. Preliminary and official election results are maintained and disseminated by computer. Specialized "Election Management" software (generally provided by the vendor of the voting equipment) is used to configure ballots and read results from precienct voting machines.

In most cases, the computers used for election administration employ the same hardware, operating systems, and networking platforms employed by other enterprises, and are connected, directly or indirectly, to the Internet. Election management systems are exposed to the same risks of compromise by malicious actors that cause the commonplace "data breaches" in other private and public sector domains that have become regular fixtures of online life.

Many jurisdictions outsource some of their election management tasks to outside vendors or contractors. This further amplifies the exposure of local election systems to external tampering.

Disruption or compromise of any local election administration functions can have grave and often non-recoverable consequences for the integrity of elections. Compromise of voter registration databases can be exploited by adversaries to cause long lines at polling places (forcing large numbers of voters to cast provisional ballots) and can selectively disenfranchise voters to favor particular candidates. Provisioning of voting machines with incorrect ballot definitions can prevent correct ballots from being cast. Errors in in unofficial or final tallies can cast doubt on the legitimacy of entire elections. In some cases, successful attacks may not be discovered until long after polls have closed, or may never be discovered at all.

The IT and security administration of election management computers varies widely from

jurisdiction to jurisdiction. In the best cases, there may be a full-time staff devoted to securing and managing election computers and networks. In a more typical case, computer security is relegated to the general county IT staff, which may have only limited resources relative to the threat. In all cases, however, even the best defensive cybersecurity resources of a local county are of only limited value against a foreign state adversary.

Local election management computers and networks are especially attractive targets for foreign tampering and interference. They can often be attacked remotely, without the need for physical presence in the targeted jurisdiction, and successful attacks may be rewarded with partial or complete control over a county's voter registration databases, voting machine configuration, and results reporting infrastructure.

2. Electronic Poll Books

Electronic poll books, which are not used in every jurisdiction, perform the initial voter "check in" function at polling places on election day. They must, by nature of their function, have reliable access to an authoritative list of the voters registered to vote at each polling places. This may be accomplished either with an internal copy of the voter registration database or by online remote access to a central computer. In either configuration, electronic poll books perform an essential election function and must be reliably secured against tampering. If poll books are unavailable or if their databases are corrupted, voters will not be able to cast ballots (except by provisional ballot, to the extent that is a viable option).

Electronic poll books have received much less scrutiny than other precinct voting equipment, but are subject to all the same risks and attack vectors as other electronic devices. In many jurisdictions, they are largely unregulated and require little or no outside certification or audit.

3. Optical Scan Ballot Readers

Optical scan ballot readers are specialized computers that scan and retain printed ballots and record on electronic storage media the tally of votes cast in each race. They depend on the integrity of their software and hardware for their ability to correctly interpret ballots and to correctly record votes. They are exposed to physical access by poll workers, and, in many cases, individual voters.

Ballot scanners can be compromised in a number of practical ways, any one of which can compromise the recorded vote tally. However, because they retain the physical paper ballots marked by voters, it is possible to recover from such a compromise if it is detected. A technique called "risk-limiting audits" can reliably detect and recover from defective or compromised ballot scanners and is discussed in the sections that follow.

4. Ballot Marking Devices

Originally, Ballot Marking Devices (BMDs) were conceived of narrowly, as an assistive technology for use by voters with disabilities to assist them in marking optical scan paper ballots, (bringing such systems into compliance with Help America Vote Act (HAVA) requirements for

accessible voting). However, certain recent voting products greatly expand the use of BMD technology by integrating a BMD into the voting process for all voters, whether they require assistive technology or not.

BMD-based voting systems are controversial, since, by virtue of their design, the correctness of their behavior cannot be effectively audited except by every individual voter carefully verifying his or her printed ballot before it is cast. A maliciously compromised BMD could subtly mismark candidate selections on ballots in a way that might not be noticed by most voters. If BMDs fail or must be rebooted at a polling place, there may be no way for voters to create marked ballots, making BMDs a potential bottleneck or single point of failure on election day.

As a relatively new technology, BMD-based systems have not yet been widely examined by independent researchers and have been largely absent from practical election security research studies. However, even with relatively little scrutiny, exploitable weaknesses and usability flaws have been found in these systems, This underscores the need for more comprehensive studies and for caution before these systems are purchased by local jurisdictions or widely deployed.

5. Direct Recording Electronic (DRE) Voting Machines

From a security perspective, by far the most problematic and risky class of electronic voting systems are those that employ *Direct Recording-Electronic (DRE)* machines. DRE machines are special purpose computers programmed to present the ballot to the voter and record the voter's choices on an internal digital medium such as a memory card. At the end of the election day, the memory card containing the vote tallies for each race is generally removed or electronically read from the machine and delivered to the county election office, where the tallies from each precinct are recorded by the county tallying software. DRE machines are sometimes informally called "touchscreen" voting machines, although not all DRE models use actual touchscreen displays (nor are all election devices that employ touchscreens DREs).

The design of DREs makes them inherently difficult to secure and yet also makes it especially imperative that they *be* secure. This is because the accuracy and integrity of the recorded vote tally depends completely on the correctness and security of the machine's hardware, software, and data. Every aspect of a DRE's behavior, from the ballot displayed to the voter to the recording and reporting of votes, is under control of the DRE hardware and software. Any security vulnerability in this hardware or software, or any ability for an attacker to alter (or re-load new and maliciously behaving) software running on the machine, not only has the potential to alter the vote tally, but can make it impossible to conduct a meaningful recount (or even to detect that an attack has occurred) after the fact. If a DRE is compromised at any time before or during an election, any votes cast on it are irreparably compromised as well.

DRE-based systems introduce several avenues for attack that are generally not present (or are not as security-critical) in other voting technologies:

- Alteration or deletion of vote tallies stored in internal memory or removable media
- Alteration or deletion of ballot definition parameters displayed to voters [7]

[7] An incorrect (or maliciously altered) DRE ballot definition can make it impossible to determine the true

- Alteration or deletion of electronic log files used for post-election audits and detecting unauthorized tampering

Attacks might be carried out in any of several ways, each of which must be reliably defended against by the DRE hardware and software:

- Direct tampering with data files stored on memory cards or accessible through external interface ports
- Surreptitious replacement of the certified software running on the device with a maliciously altered version
- Exploitation of a pre-existing vulnerability in the certified software

Successfully exploiting just *one* of these avenues of attack can be sufficient to undetectably compromise an election. The design of DREs makes it necessary not only that their hardware be highly secure against unauthorized tampering, but that the software running on them not suffer from *any* vulnerabilities that could be exploited by a malicious actor. This makes the security requirements for DREs more stringent – and also more easily defeated – than for any other currently deployed election technology.

Unfortunately, the DRE-based systems purchased by and used in various states under HAVA have repeatedly been found to suffer from exactly these kinds of exploitable hardware and software vulnerabilities.

B. The 2007 California and Ohio Studies

To date, the most extensive independent studies of the security of electronic voting systems were commissioned ten years ago by the Secretaries of State of California and Ohio. Expert review teams were given access to the voting machine hardware and software source code of every system certified for use in those states. The systems used in California and Ohio were also certified for use in most of the rest of the country, so these studies effectively covered a large fraction of available electronic voting equipment and software. I led the teams that reviewed the Sequoia products (for the state of California) and the ES&S products (for the state of Ohio); other teams in these studies reviewed the Diebold/Premier and Hart InterCivic products.[8]

In both studies, every team found and reported serious exploitable vulnerabilities in *almost every component* examined. In most cases, these vulnerabilities could be exploited by a

---

election results even without any malicious software exploitation. For example, in York County, PA, a DRE ballot definition programming error in the 2017 general election appears to have allowed candidates in some local races to be voted for twice, with the possible consequence that the election will have to be invalidated and redone. See http://www.ydr.com/story/news/2017/11/08/voting-machine-problems-what-york-countys-options/843423001/ . Paper-based systems, in contrast, are more robust against such errors. For example, the 2000 general election in Bernalillo County, NM had a similar error in their punch card counting software, but was later able to correct the error without a new election; see https://www.wsj.com/articles/SB976838091124686673

[8] The various final reports of the California "Top-To-Bottom Review" studies can be found at http://www.sos.ca.gov/elections/voting-systems/oversight/top-bottom-review/ . The final report of the Ohio "Project EVEREST" study can be found at https://www.eac.gov/assets/1/28/EVEREST.pdf

single individual, who would need no more access than an ordinary poll worker or voter. Such an attacker would be able to alter vote tallies, load malicious software, or erase audit logs. Some of the vulnerabilities found were the consequence of software bugs, while others were caused by fundamental architectural properties of the system architecture and design. In some cases, compromise of a single system component (such as a precinct voting machine) was sufficient to compromise not just the vote tally on that machine, but to compromise the entire county back end system.

In response, California and Ohio ordered some equipment decertified and some election-day procedures modified. However, all the vulnerable equipment and software remained certified for use in at least some other states.

Some equipment vendors and local voting officials claimed at the time that the findings of the California and Ohio studies were irrelevant or overstated, that any problems identified could be easily fixed, and that it would be difficult or impossible for anyone but an expert with extensive experience and access to privileged information (such as source code) to exploit vulnerabilities in practice. However, as exercises such as the DEFCON Voting Village (described below) have demonstrated, not only do these systems remain vulnerable, but they can be readily exploited by people with no more than ordinary computer science experience and expertise and without access to any secret or proprietary information.

C. The DEFCON Voting Village Exercise

The DEFCON conference is one of the world's largest and best-known computer security "hacker" conferences. This year's DEFCON was held August 8-10, 2019, in Las Vegas, NV, and drew more than 25,000 participants from around the world. DEFCON participants have broad interest in technology, and include security researchers from industry, government, and academia, as well as individual hobbyists.

For the last three years, DEFCON has featured a *Voting Machine Hacking Village* ("Voting Village") to give participants an opportunity to examine and get hands-on experience with the security technology used in US elections, including voting machines, voter registration databases, and election office networks. I am one of the organizers of the Voting Village.[9]

The voting machines available in the Voting Village included a variety of DRE, optical scan readers, ballot marking devices and electronic poll books from a range of commercial vendors. We acquired (from the surplus market) and made available to participants a sampling of different pieces of election hardware, including both DRE and optical scan voting machines as well as "poll book" devices used by used by precinct workers to verify and check in voters at polling places. Every model machine currently at the Voting Village is still certified for use in U.S. elections in at least one jurisdiction today.

The DEFCON Voting Village is not intended to be a formal security assessment or test, but rather an opportunity for a general audience of technologists to examine election equipment

[9] Organizers of the DEFCON Voting Village include the author as well as Harri Hursti, Margaret MacAlpine, and Jeff Moss.

and systems. However, participants are encouraged to critically examine and probe the equipment and software for vulnerabilities, and to seek practical ways to compromise security mechanisms. No proprietary information or computer source code is made available.

The results of the Voting Village are summarized each year in detail in a report.[10] It is notable that participants, who overwhelmingly do not have any previous special expertise in voting machines or access to any proprietary information about them, have been very quickly able to find ways to compromise *every* piece of equipment in the Village by the end of the weekend. Depending on the individual model of machine, participants have found ways to load malicious software, gain access to administrator passwords, compromise recorded votes and audit logs, or cause equipment to fail. In most cases, these attacks could be carried out from the ordinary interfaces that are exposed to voters and precinct poll workers.

The ease with which participants compromise equipment in the Voting Village should be regarded as at once alarming and yet also unsurprising. It is alarming because the very same equipment is in use in polling places around the United States, relied on for the integrity of real elections. But it is also ultimately unsurprising. Versions of many of the machines at DEFCON had been examined in the 2007 studies and found to suffer from basic, exploitable security vulnerabilities. It should not come as any surprise that, given access and motivation, people of ordinary skill in computer security would be able to replicate and expand on these results. It is, in fact, precisely what the previous studies of these devices warned would happen.

In summary, the DEFCON Voting Village demonstrates that much of the voting technology used in the US is vulnerable not just to hypothetical expert attack in a laboratory environment, but also to practical analysis, manipulation and exploitation by non-specialists with only very modest resources.

III. US Election Systems Are Not Engineered to Resist National Adversaries

The traditional "threat model" against which electronic voting systems have been evaluated has been largely focused on resisting traditional election *fraud*, in which domestic conspirators, perhaps assisted by corrupt poll workers or election officials, attempt to "rig" an election to favor a preferred candidate in a local, state, or national contest. Fraud might be accomplished by altering votes, adding favorable votes, deleting unfavorable votes, or otherwise compromising the security mechanisms that protect the ballot and tally.

While virtually every study of electronic voting technology has raised questions about the ability of current systems to resist serious efforts at fraud, traditional election fraud is not the only kind of threat, or even the most serious threat, that a voting systems must resist today.

Electronic voting systems must resist not only fraud from corrupt candidates and supporters, but also election *disruption* from hostile nation-state adversaries. This is a much more formidable threat, and one that current systems are far less equipped to resist.

[10] The current Voting Village final report is available at: https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf

The most obvious difference between traditional election fraud by corrupt domestic actors and disruption by hostile state actors is the expected resources and capabilities available to each. The intelligence services of even small nations can marshal far greater financial, technical, and operational resources than would be available to even highly sophisticated criminal conspiracies. For example, intelligence services can feasibly conduct advance operations against the voting system *supply chain*. In such operations, the aim might be to obtain confidential source code or to secure surreptitious access to equipment before it is even shipped to local election officials. Hostile intelligence services can exploit information and other assets developed broadly over extended periods of time, often starting well before any specific operation or attack has been planned.

But their greater resources are not the most important way that hostile state actors can be a more formidable threat than corrupt candidates or poll workers. They also enjoy easier goals. The aim of traditional "retail" election fraud is to tilt the outcome in favor of a particular candidate. That is, to succeed, the attacker must generally alter the reported vote count or add, change, or delete votes. But a hostile state actor – via an intelligence service such as Russia's GRU – might be satisfied with merely *disrupting* an election or calling into question the *legitimacy* of the official outcome. With election systems so heavily dependent on demonstrably insecure software and voting equipment, this kind of disruption could be comparatively simple to accomplish, even at a national scale.

A hostile state actor who can compromise even a handful of county networks might not need to alter any actual votes to create widespread uncertainty about an election outcome's legitimacy. It may be sufficient to simply plant suspicious (and detectable) malicious software on a few voting machines or election management computers, create some suspicious audit logs, delete registered voters from the rolls, or add some obviously spurious names to the voter rolls. If the preferred candidate wins, they can simply do nothing (or, ideally, use their previously arranged access to restore the compromised networks to their original states, erasing any evidence of compromise). If the "wrong" candidate wins, however, they could covertly reveal evidence that county election systems had been compromised, creating public doubt about whether the election had been "rigged". This could easily impair the ability of the true winner to effectively govern, at least for a period of time.

Electronic voting machines and vote tallies are not the only potential targets for such attacks. Of particular concern are the back end systems that manage voter registration, ballot definition, and other election management tasks. Compromising any of these systems (which are often connected, directly or indirectly, to the Internet and therefore potentially remotely accessible) can be sufficient to disrupt an election while the polls are open or cast doubt on the legitimacy of the reported result. The decentralization of election operations, managed by thousands of individual local offices throughout the nation (with widely varying resources) is sometimes cited as a strength of our electoral process. However, this decentralization can be turned to the adversary's advantage. An attacker can choose arbitrarily from among whatever counties have the weakest systems – those with the least secure software or most poorly defended networks and procedures – to target.

It is beyond the scope of my testimony to speculate on specific intrusions that occurred against state and local election management systems in the 2016 US general election, much of which remains classified or under investigation. It has been reported that voter registration management systems in at least several states were targeted for exploitation and access. It is unclear whether voting machines or tallying systems were also targeted. However, targeting and exploiting such systems would have been well within the capability of any major rival intelligence service.[11]

In summary, the architecture of many current electronic voting systems, especially those that employ DRE voting machines, makes disruption attacks an especially attractive option for our foreign adversaries – and especially difficult one to effectively defend against. These systems can give hostile actors interested in disruption an even *easier* task than that facing corrupt candidates seeking to steal even a small local office. And the consequences of election disruption strike at the very heart of our national democracy.

IV. RECOMMENDATIONS: ALL US ELECTIONS SHOULD EMPLOY PAPER BALLOTS AND RISK-LIMITING AUDITS

It is perhaps tempting to conclude pessimistically that election technology in the US is fatally flawed, leaving our nation irreparably vulnerable to election fraud and foreign meddling. But while it is true that the current situation exposes us to significant risk, it is by no means hopeless or beyond repair. Relatively simple, and available, technologies can be deployed that render our elections significantly more robust against attack.

While electronic voting machines do indeed suffer demonstrably fundamental weaknesses, some electronic voting technologies are significantly more resilient in the face of compromise than others. The most important feature required is that there be a reliable record of each voter's true ballot selections that can be used as the basis for a post-election audit to detect and recover from failure or compromise of the software or hardware.

Among currently available, HAVA-compliant voting products, the only systems that meet this requirement are those that employ *optical scan paper ballot* technology. In such systems, the voter fills out a machine-readable paper ballot form (possibly with the aid of an assistive ballot marking device for language-, visually- and mobility-impaired voters), that is then deposited into a ballot scanning device that reads the ballot choices, maintains an electronic tally, and retains and secures the marked paper ballots for subsequent audit. After the polls close, the electronic tally records are read from each ballot scanner and preliminary results calculated.

The paper records of votes that precinct-counted optical-scan systems provide are a necessary, but not by themselves sufficient, safeguard against software. As noted above, even non-DRE systems can suffer from flaws and exploitable vulnerabilities in the voting machine and back end software. The second essential safeguard is a systematic and reliable process for

[11] For a comprehensive discussion of technical attacks against our election infrastructure in 2016, see the Report of the Select Committee on Intelligence, US Senate on Russian Active Measures in the 2016 US Election, Vol 1. https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume1.pdf

detecting whether the software has reported incorrect results, and to recover the true results if so.

The most reliable and well-understood method to achieve this is through an approach called *risk-limiting audits*.[12] In a risk limiting audit, a statistically significant randomized sample of ballots are manually checked by hand and the results compared with the electronic tally. (This must be done for *every* contest, not just those with close results that might otherwise call for a traditional "recount".) If discrepancies are discovered between the manual and electronic tallies, additional manual counts are conducted. The effect of risk-limiting audits is not to eliminate software vulnerabilities, but to ensure that the integrity of the election outcome does not depend on the herculean task of securing every software component in the system. This important property is called *strong software independence*.[13]

Optical scan paper ballots and risk-limiting audits comprise a critical, and readily deployable, safeguard against both traditional election fraud and nation-state disruption. Taken together, they permit us to more safely enjoy the benefits of computerized election management, without introducing significant new costs or requiring the development of speculative new technology. The technology required for this is available *today*, from multiple vendors, and is already in use in many states.

As important as paper ballots and risk-limiting audits are, however, they are not panaceas that solve every threat to our elections. It is also critical that the state and county backend computer networks and systems used for election management and voter registration be vigilantly protected against compromise. As we saw in 2016, hostile adversaries might attempt to breach not just voting machines, but also back end election management systems and voter registration database systems, which are often connected, directly or indirectly, to the Internet.

It is no exaggeration to observe that state and local election officials serve on the front lines of our national cybersecurity defense. They must be given sufficient resources, infrastructure, and training to help them effectively defend their systems against an increasingly sophisticated – and increasingly aggressive – threat environment. It is notable that the budgets for election administration often must compete for resources with essential local services such as fire protection and road maintenance. Election management represents only a miniscule fraction of the total national spending on political campaigns. Additional investment here will pay significant dividends for our security.

By analogy, we do not make the county sheriff responsible for defending against ground invasions by foreign military forces. Yet that is precisely the role into which we have placed our local county IT administrations in defending our election infrastructure against electronic attacks. Just by doing so, we have set them up for failure.

Simply put, much of our election infrastructure remains vulnerable to practical attack, with threats that range from traditional election tampering in local races to large-scale disruption

[12] A good introduction to the theory and practice of risk limiting audits in elections can be found at https://www.stat.berkeley.edu/~stark/Preprints/RLAwhitepaper12.pdf .

[13] See Ron Rivest. "On the notion of 'software independence' in voting systems". *Phil. Trans Royal Society A*. Volume 366 Issue 1881. October 28, 2008. http://rsta.royalsocietypublishing.org/content/366/1881/3759 .

by national adversaries. We should take no comfort if such attacks have not yet been widely detected. At best, it is only because, for whatever reason, serious attempts have not yet been made. Given the potential rewards to our adversaries, it is only a matter of time before they will.

National-level investment in safeguards such as those described above serve our democracy in critically important ways. They can provide a significant improvement to election security, both in our ability to resist attack and in our ability to recover from attacks when they occur. Perhaps most importantly, they provide meaningful assurance to voters that their ballots truly count and that their elected officials are governing truly legitimately. Our republic cannot long survive without the confidence that comes from that assurance.