BRENNAN
CENTER
FOR JUSTICE
TWENTY
YEARS

SECURING ELECTIONS FROM FOREIGN INTERFERENCE

Lawrence Norden and Ian Vandewalker

Foreword by Amb. R. James Woolsey, Director of Central Intelligence 1993-95

Brennan Center for Justice *at New York University School of Law*

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. We work to hold our political institutions and laws accountable to the twin American ideals of democracy and equal justice for all. The Center's work ranges from voting rights to campaign finance reform, from ending mass incarceration to preserving Constitutional protection in the fight against terrorism. Part think tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, the courts, and in the court of public opinion.

ABOUT THE BRENNAN CENTER'S DEMOCRACY PROGRAM

The Brennan Center's Democracy Program works to repair the broken systems of American democracy. We encourage broad citizen participation by promoting voting and campaign finance reform. We work to secure fair courts and to advance a First Amendment jurisprudence that puts the rights of citizens — not special interests — at the center of our democracy. We collaborate with grassroots groups, advocacy organizations, and government officials to eliminate the obstacles to an effective democracy.

ABOUT THE BRENNAN CENTER'S PUBLICATIONS

Red cover | Research reports offer in-depth empirical findings.
Blue cover | Policy proposals offer innovative, concrete reform solutions.
White cover | White papers offer a compelling analysis of a pressing legal or policy issue.

ABOUT THE AUTHORS

Lawrence Norden is Deputy Director of the Brennan Center's Democracy Program. He has authored several nationally recognized reports and articles related to voting rights and voting technology, including *America's Voting Machines at Risk* (September 2015), *How to Fix Long Lines* (February 2013), *Better Design, Better Elections* (July 2012), and *Voting Law Changes in 2012* (October 2011). His work has been featured in media outlets across the country, including *The New York Times*, *The Wall Street Journal*, Fox News, CNN, MSNBC, and NPR. He has testified before Congress and several state legislatures on numerous occasions. He received his J.D. from New York University School of Law.

Ian Vandewalker serves as Senior Counsel for the Brennan Center's Democracy Program, where he works on voting rights and campaign finance reform. His work includes *Stronger Parties, Stronger Democracy: Rethinking Reform* (September 2015), a recurring series analyzing spending in U.S. Senate elections, and academic articles in the fields of election law and civil liberties. Press outlets across the nation have featured his work, including *The New York Times*, *The Washington Post*, and NPR. He earned his J.D. cum laude in 2008 from New York University School of Law and holds a master's degree in philosophy from Indiana University and a bachelor's degree from New College of Florida.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the many colleagues that collaborated in preparing this report. Brennan Center President Michael Waldman and Director of the Brennan Center's Democracy Program Wendy Weiser supplied an indispensable source of leadership and vision at all stages of this project. Brennan Center Vice Presidents Vivien Watts and John Kowal provided instrumental guidance and direction. Christopher Famighetti contributed crucial research and editorial support to this project. Raffe Jefferson and Rebecca Autrey of the Brennan Center's Communications Team lent valuable review and editing assistance. Brennan Center Senior Editor Jim Lyons provided helpful revisions. The authors are grateful to Ava Mehta for her important research. Research and Program Associate Phoenix Rice-Johnson and Democracy Program Intern Peter Dunphy merit special thanks for their sustained assistance in researching, fact-checking, and editing.

We are also immensely grateful to the many experts and officials whose knowledge and views helped shape this report. We sincerely thank the following individuals for generously sharing their expertise and information through multiple interviews: Matt Masterson, Commissioner, U.S. Election Assistance Commission; Merle King, Executive Director, Center for Election Systems at Kennesaw State University; David Becker, Director, Election Initiatives, Pew Charitable Trusts; Rebecca Wright, Professor of Computer Science at Rutgers University and Director of the Center for Discrete Mathematics and Theoretical Computer Science; Edgardo Cortes, Commissioner, Virginia Department of Elections; Matt Damschroder, Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio; Douglas Kellner, Co-Chair, State Board of Elections, New York; Jeremy Epstein, Deputy Division Director, Computer & Network Systems Division, National Science Foundation; Marian Schneider, Special Advisor to the Governor on Election Policy, Pennsylvania; Alex Halderman, Director, Center for Computer Security and Society, University of Michigan; Stuart Holmes, Voting Information System Manager, Secretary of State, Washington; Marc Burris, IT Director and CIO, State Board of Elections, North Carolina; Maggie Toulouse Oliver, Secretary of State of New Mexico; and Neil Jenkins, Chief of Policy and Planning, Department of Homeland Security, National Protection and Programs Directorate, Office of Cybersecurity & Communications.

This report also benefitted from the many willing to share their valuable experience and provide insight in the review process. Alongside many of the aforementioned experts, we gratefully acknowledge the following individuals for their helpful feedback: Pamela Smith, President, Verified Voting; Amb. R. James Woolsey; Justin Talbot-Zorn, Policy and Legislative Outreach Director, National Election Defense Coalition; and Ronald L. Rivest, Vannevar Bush Professor of Electrical Engineering and Computer Science, Massachusetts Institute of Technology.

The Brennan Center gratefully acknowledges Arkay Foundation, Bohemian Foundation, Carnegie Corporation of New York, Change Happens, Democracy Alliance Partners, Ford Foundation, Lisa and Douglas Goldman Fund, The Charles Evans Hughes Memorial Foundation, Audrey and Sydney Irmas Charitable Foundation, The JPB Foundation, Kohlberg Foundation, Inc., The Leon Levy Foundation, John D. and Catherine T. MacArthur Foundation, The Mertz Gilmore Foundation, Open Society Foundations, The Overbrook Foundation, PARC Foundation, Rockefeller Brothers Fund, The Schooner Foundation, Vital Projects Fund, Wallace Global Fund, and The WhyNot Initiative for their generous support of our money in politics and elections work.

TABLE OF CONTENTS

FOREWORD

By Amb. R. James Woolsey, Director of Central Intelligence 1993-95

In the last few months, we have learned extraordinary details about a Russian assault on our election infrastructure. While there is no evidence that this assault altered the vote count, that fact should be cold comfort as we look to protect ourselves against future attacks.

One doesn't have to be an expert on cybersecurity or election technology to understand how dangerous this is. Based on my experience, as a former Director of Central Intelligence, and in service to this country under both Democratic and Republican Presidents, I am confident the Russians will be back, and that they will take what they have learned last year to attempt to inflict even more damage in future elections. In particular, their history of interfering in other nations' politics, their antipathy to the United States and Western democracies generally, and their proven ability to multiply the impact of their actions through cyberattacks should put us on the highest alert, and spur us to take all necessary actions to protect ourselves from further attack.

Of course, Moscow is not the only adversary that we have to worry about. North Korea has been implicated in the ransomware attack that locked up the computers of government agencies and businesses worldwide this May, while Al Qaeda and ISIS have a history of executing cyberattacks on foreign government websites. They too might be emboldened by Russia's actions against us last year.

This report offers important guidance on how to protect ourselves. In particular, it looks at the two most critical parts of America's election infrastructure: voting machines, which could be hacked to cast doubt on the integrity of vote tallies, or change them; and voter registration databases, which could be manipulated to block voters and cause disorder when citizens attempt to vote.

As the authors explain, much has been done to secure these systems in the last few years. But hackers have grown increasingly sophisticated in this time as well. And the state and local elections officials who are custodians of our election infrastructure often operate with highly constrained resources.

What more must be done? The key security measures detailed in this report are the right place to start: replace paperless electronic machines, upgrade the hardware and software that supports voter registration, and conduct post-election audits to confirm the results.

These are common-sense solutions that will increase security and public confidence in the integrity of our system. Importantly, they will do so without interfering with the right of any eligible citizen to participate in the choice of who will govern the nation.

Sadly, as polarization has increased in this country, even discussions of topics like how to safeguard our voting systems have broken down into partisan fighting, with each side looking for an advantage in the debate, and failing to take the steps necessary to secure our infrastructure from attack. We can no longer afford such indulgence. As has happened at key moments in our history, we face a test from outsiders who would like to harm us. We are forced to answer whether we can, once again, lay aside our differences to work together to protect the common interests of our nation.

The history of national defense shows that threats are constantly evolving. When the United States was attacked at Pearl Harbor, we took action to protect our fleet. When we were attacked on 9/11, we took action to upgrade transportation security and protect our ports and other vulnerable targets. We were attacked in 2016. The target was not ships or airplanes or buildings, but the machinery of our democracy. We will be attacked again. We must act again — or leave our democracy at risk.

INTRODUCTION

In the spring of 2017, Americans began to learn startling details of Russia's unprecedented attack on our election infrastructure. While it is important to emphasize that there is no evidence these actions changed the vote count, the attack makes clear that our country is not immune from foreign interference in our elections merely because it is the world's dominant superpower.

To a greater degree than many realize, America's election systems remain vulnerable. This is a product of old technology, inadequate systems, and a patchwork election administration model with widely varying levels of resources and skill at protecting against new-era threats. A twentieth century election system is no match for twenty-first century threats.

But we are far from helpless. This report outlines urgent steps we can take now to protect the security of the most critical elements of the U.S. election infrastructure:

- voting machines, which could be hacked to cast doubt on the integrity of vote tallies, or to even change them; and

- voter registration databases, which could be manipulated in an attempt to block voters, cause disruption, and undermine confidence when citizens vote.

The Brennan Center has studied these systems for more than a decade. Following the 2016 election, we surveyed cyber-attacks against election systems in the United States and around the world. And we conducted interviews with more than a dozen of the country's leading election officials and security experts, including officials from the Department of Homeland Security and the United States Election Assistance Commission.

This report examines the greatest vulnerabilities to the integrity of our election infrastructure, and the important steps that election officials and others have taken to protect these vulnerabilities. Above all else, we set out the measures that must be put in place as soon as possible to protect the integrity of American democracy as we prepare for elections in 2018, 2020, and beyond.

Much of the focus on Russia's attack on our election system turns on Putin and foreign policy matters. In response, sanctions and other steps may be warranted. But we can do much more to harden our election infrastructure so it is not susceptible to manipulation — by Moscow, by any other foreign power or terrorist group, or by domestic interests.

Understanding the Threat

On January 6, 2017, the Director of National Intelligence (DNI) published an extraordinary document that described a brazen attack on American sovereignty. Over the course of 14 information-packed pages, the DNI report condensed the best thinking from the FBI, CIA, and NSA about how Russia interfered in the 2016 election, in part by targeting the systems we use to run our elections.

Portions of the report read like a throwback to the Cold War, noting "Moscow's longstanding desire to undermine the US-led liberal democratic order." But what was different in 2016 is that Russia's effort "demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations."[1]

Among other actions, the report describes the hacking of private information from political targets, including both major parties; the leaking of stolen information; and the use of media reaching U.S. audiences to spread propaganda. The report also found that "Russian intelligence obtained and maintained access to elements of multiple … state or local electoral boards, though the Department of Homeland Security assesses that the types of systems Russian actors targeted or compromised were not involved in vote tallying."

The report does not mince words about who directed this operation or its purpose:

> Russian President Vladimir Putin ordered an influence campaign in 2016 aimed at the US presidential election. Russia's goals were to undermine public faith in the US democratic process, denigrate Secretary Clinton, and harm her electability and potential presidency.[2]

In the last several weeks we have learned that Russian attacks on the country's election infrastructure may have gone even further than was indicated in the DNI report. In particular, *The Intercept* reported on a leaked National Security Agency document that revealed a "months-long Russian intelligence cyber effort against" the voter registration process, "including a private sector manufacturer of devices that maintain and verify the voter rolls," as well as spear-phishing attacks against "local government organizations," and government officials "involved in the management of voter registration systems."[3] A subsequent article in *Bloomberg* stated that in Illinois "investigators found evidence that cyber intruders tried to delete or alter voter data," on the state's voter registration database and that "[i]n all, Russian hackers hit systems in a total of 39 states."[4]

Not surprisingly, American intelligence agencies have concluded that Russia will use what it learned in 2016 to meddle in future elections.[5] *Bloomberg* cited one former senior U.S. official as expressing concern "that the Russians now have three years to build on their knowledge of U.S. voting systems before the next presidential election, and there is every reason to believe they will use what they have learned in future attacks."[6] Former FBI Director James Comey has been particularly blunt, stating that "They're coming after America,"[7] and "I expect to see them back in 2018, especially in 2020."[8]

Sowing Doubt About American Democracy

Russia may have preferred Donald Trump to Hillary Clinton. But its "number one mission," as Comey told the House Intelligence Committee in March, "is to undermine the credibility of our entire democracy enterprise of this nation."[9] Russia's primary goal is to sow chaos, not necessarily to support a particular candidate.

While there is no evidence that these cyberattacks altered the vote count in 2016, all signs point to the fact that sooner or later some interest — or collection of interests — will try. As former intelligence officer Lieutenant Colonel Tony Shaffer (retired) put it in a briefing to Congress Members and staff, "anything that can be done to penetrate this system … will be done. It is just a matter of time."[10]

Moreover, as he noted in that same briefing, we should not assume we must only worry about Russia.[11] Other nations could try to attack our electoral system, whether it's an ascendant China, Iran, or North Korea, which has been linked to the ransomware attack that held hostage the computers of government agencies and businesses across the world in May of 2017.[12] The threat is not limited to nations, of course; well-organized terrorist groups such as al Qaeda or ISIS have a history of executing cyberattacks on foreign government websites and could expand their efforts.[13]

Immediate Steps Needed to Protect Our Election Infrastructure

For the past ten years, in the face of evolving cyberattacks and warnings from security experts about protecting our elections from hacking, Congress has remained strangely silent. Now, as Congressional leaders investigate Russia's interference in the 2016 election, they can take immediate, common sense actions to protect our elections from attacks in 2018 and 2020. While states and counties run our elections, the federal government and Congress have a critical role to play through funding and setting standards. All levels of government must be involved in securing our elections.

Among the most important security recommendations detailed in this report are the following:

- **Replace Antiquated Voting Machines with New, Auditable Systems.** Our election infrastructure is aging. It is time for Congress, states, and local governments to assist election officials in replacing antiquated equipment that is costly and difficult to maintain, has an increased risk of failure and crashes, and remains a significant security risk. Perhaps most importantly, Congress should act to help states and counties replace the old, paperless Direct Recording Electronic machines that are still used in 14 states, with more secure, accessible systems.

- **Conduct Audits of Paper Ballots or the Voter Verified Paper Record.** Paper records of votes have limited value against a cyberattack if they are never used to check that the software-generated total has not been hacked. Today, only 26 states require that election officials conduct post-election audits of paper records. Even in states where they are conducted, they are often insufficiently robust to ensure an election-changing software error would be found.

- **Complete a Full Assessment of Threats to Our Voter Registration Systems.** State and local governments must fully identify potential avenues for attacking voter registration systems, mapping out all of the entities that interact with that system, and implementing mitigation strategies where weaknesses are identified. The consensus among experts interviewed by the Brennan Center is that this should be done on a regular basis, but that many states are unlikely to have completed this kind of comprehensive risk assessment in the last few years, despite the fact that both registration systems and cyber threats have evolved enormously over that time.

- **Upgrade and Replace IT Infrastructure, Including Databases.** The Brennan Center estimates that 42 states are using voter registration databases that were initially created at least a decade ago. Experts interviewed by the Brennan Center agreed that many states will require upgrades to their databases and election infrastructure in the near future, and that the need is particularly great at the local level, where systems often run on discontinued software like Windows XP[14] or Windows 2000 that is more vulnerable to cyberattack because it is no longer vendor supported.

Further recommendations are discussed in more detail in the body of this report.

Critically, members of Congress and state legislatures should be talking with election officials and security experts about local needs, as they will vary by county and state. The best legislative solutions may mimic already existing bipartisan bills to address cybersecurity issues, such as the State Cyber Resiliency Act, a bill introduced in March in the Senate by Senators Warner (D) and Gardner (R) and in the House by Representatives Kilmer (D) and Comstock (R).[15] That bill requires the Federal Emergency Management Agency and DHS to work with state and local governments in administering and awarding State Cyber Resiliency Grants to protect critical infrastructure, based on the needs in those states. That is a good start. Our election infrastructure could benefit from an even more narrowly tailored program of grants that aims to provide money for the kinds of measures discussed in this report.

• • •

In May, former Director of National Intelligence James Clapper warned the Senate Judiciary Committee "If there has ever been a clarion call for vigilance and action against a threat to the very foundation of our democratic political system, this episode is it."[16] We would add that if anything can be deemed vital to our political system, it is election integrity. Indeed, election integrity is the prerequisite for democracy itself.

The Russian attacks are a powerful illustration of how the integrity of elections has become a matter of national security. Vulnerabilities in election systems can be exploited by foreign powers for their own benefit, with the potential for lasting damage to American democracy.

The threats against each system we discuss below are very real. Fortunately, they can be neutralized. In this report, we explain how.

VOTING MACHINES

Although no evidence has emerged of foreign tampering with American voting machines, the press has devoted many breathless words to the question of whether machines can be hacked.[17] The emphasis is understandable: to the average person, voting machines *are* elections. Manipulating voting machines is a concrete, easy-to-understand method for tampering with elections.

But is there an actual danger of such attacks succeeding in the United States? Based on recent experiences in other countries, the evolution of cyber-attacks over the last decade, and current vulnerabilities in our system, the answer is yes.

In fact, cyberattacks against voting systems are not just the stuff of binge-watched TV shows or movies.[18] We have seen at least two known cyberattacks on *non*-American voting systems in the last couple of decades. In 2014, Ukraine's presidential vote was targeted by cyber attackers, who deleted enough files to make the country's voting system inoperable days before the election.[19] Officials were able to restore the system from backups and the election went forward. But shortly before the results were to be announced, experts examining computers at the Ukrainian Central Election Commission discovered a virus designed to falsely declare an ultra-nationalist party as the victor with 37 percent of the vote.

A pro-Russian hacker group, CyberBerkut, claimed responsibility for the Ukrainian attacks. Experts debate whether the group is sponsored by the Kremlin.[20] One possible indication of state support, or perhaps tacit assent, is how quickly the group's exploits appeared in the Russian press. Intriguingly, the same day the virus attempting to falsify the Ukrainian vote was discovered, the Russian state-controlled Channel One incorrectly reported that the ultra-nationalist party had won with the exact same vote totals as those programmed into the virus.[21]

Russia has also been implicated in a hack against Bulgaria's Central Election Commission during a referendum and local elections in 2015.[22] While that attack did not impact the systems used to total votes, it did hit the commission's website, "which provided updates on voter turnout."[23]

Looking farther back, a hacker in South Africa attempted to steal that country's historic first democratic election in 1994 from Nelson Mandela by changing vote totals.[24] The hacker was able to access a computer remotely and add votes to the tallies of three right-wing parties, eating into the lead of Mandela's ANC party.[25] The hack was discovered, and there was a delay as the counting method was switched from electronic to manual.

It is thus not surprising that throughout the world, we have seen greater concern about how to protect voting systems from cyberattack. Most recently, the Netherlands opted to count all votes by hand in their March 2017 general election out of fear that the software used to total regional and national vote tallies was "vulnerable" to hacking.[26]

Built-in Protections Against Cyberattacks on American Voting Machines

Fortunately, the U.S. has some built-in protections against widespread attack.[27] First, the decentralization of American election administration offers perhaps the most important measure of protection. There are more than 8,000 election jurisdictions, and voters cast their ballots at about 100,000 polling places.[28] Each state or locality buys its own machines, sets its own rules for designing and counting ballots, and devises its own security measures. This means that a federal election is in many ways, thousands of separate elections, with different voting machines, ballots, rules and security measures. While there can be security downsides to such decentralization (discussed below), one clear benefit is that it is practically impossible to attack all of the nation's voting machines at a single point, as might be possible with a statewide voter registration database or campaign e-mail server.[29] Similarly, because the vast majority of voting is done on machines that are not connected to the internet, attacking them remotely is extremely difficult, in a way that might not be true for a voter registration database or a campaign's e-mail server. What this means is that the impact of any particular attack will likely be limited in geographic scope. At worst, it might impact an entire county or state, depending on how uniform the equipment, programming and processes in a particular state.

Second, particularly in the last decade, counties, states and the federal government have done much to make voting more secure. In recent years, states have taken out of service voting machines that had their own remotely-accessible wireless networks, making remote attacks much more difficult.[30]

Just as importantly, since the Help America Vote Act was passed in 2002, the Election Assistance Commission (EAC) developed standards for federal certification of voting systems, which were issued in 2005 and updated in 2015.[31] Today, 47 of 50 states rely on the EAC's federal certification program in some way.[32] This program includes much more rigorous security testing than previously existed.[33] Of course, this protection is only useful *prospectively,* for states that acquire new machines. For the many counties and states that purchased machines before the new federal standards were in place, their existence is of no benefit.

Finally, in the last few years, many jurisdictions have replaced their paperless computerized voting machines with systems that scan paper ballots filled out by voters or produce a paper trail that can be reviewed by the voter. The Brennan Center estimates that in November 2016, at least 80 percent of registered voters made selections on a paper ballot, or voted on an electronic machine that produced a paper trail.[34] This extra "software independent" record provides another important security redundancy that should act as a deterrent to attack, and should provide voters with more confidence that their votes have been counted accurately in the event there is an attack that successfully casts doubt on the integrity of the results. A public post-election audit of the voting machines can be used to confirm that the electronic record reported by the machine is correct; if systems were tampered with, a good post-election audit would let us know. This protection only applies for the 80 percent of votes cast on machines for which there is a voter verified paper record, and where good post-election audits are conducted. Unfortunately, more often than not, jurisdictions are not conducting robust post-election audits comparing paper records to software totals, so their value is frequently theoretical.

Remaining Concerns About Attacks on Voting Equipment

> *"If I were a bad guy from another country who wanted to disrupt the American system … I think I'd concentrate on messing up the touch screen (voting) systems."*
> – Ambassador James Woolsey, former Director of the Central Intelligence Agency.[35]

Despite the security advances of the last few years, dozens of independent experts have repeatedly identified serious vulnerabilities in America's electronic voting machines.[36] One 2006 report found that commonly used machines "did not have any security mechanisms beyond what you'd find on a typical home PC."[37] Experts at the Argonne National Laboratory demonstrated in 2011 that someone with a high school education and $26 worth of parts could manipulate a voting machine that was used by more than 26 million voters in the following year's election.[38] A targeted scheme could still do significant damage to American's faith in election outcomes, and even derail the integrity of local or even national elections.

Part of the problem is that most electronic voting systems used in the United States are quite old. Forty-two states currently use voting machines that were purchased more than a decade ago.[39] This is perilously close to the end of most machines' projected lifespan, particularly machines designed and engineered in the late 1990s and early 2000s. Using aging voting equipment increases the risk of failures, vote "flipping," and crashes. Such occurrences can lead to long lines and lost votes of course, but also — in an environment where adversaries are attempting to cast doubt on the integrity of American elections — can seriously undermine voters' faith in the reliability and accuracy of our voting equipment.

Moreover, aging systems also frequently rely on unsupported software, like Windows XP or Windows 2000, which does not receive regular security patches and is more vulnerable to the latest methods of cyberattack.[40] As Jeremy Epstein of the National Science Foundation has put it, "from a security perspective, old software is riskier, because new methods of attack are constantly being developed, and older software is [more] likely to be vulnerable."[41] The ransomware attack on computer systems around the world in May 2017 illustrates the danger of using old operating systems. Hackers sponsored by North Korea's spy agency released a computer worm that locked data on victims' computers and demanded a ransom to restore access.[42] The British National Health Service was hit especially hard because it relies heavily on machines running Windows XP, which Microsoft stopped supporting in 2014.[43] In response to the crisis, security experts recommended updates with the newest security patches, but at the time there were no new patches for Windows XP.

The fact that voting machines themselves are not connected to the internet does not, by itself, fully protect us from such cyberattacks. Starting with the most limited kind of attack, experts have shown that with brief physical access to many voting machines or their removable memory cards — which contain ballot data and vote counts — a knowledgeable actor could flip the result of a local election, where the tally on a single voting machine could be extremely important.[44] Or attackers could manipulate the system to do any number of things that might shake the confidence of voters, including causing machines to crash or completely erasing vote totals. They could even change the vote tally in such an obvious way that the public would doubt all voting machines' results by, for instance, having all the votes on the machine tallied for Republican candidates in a highly Democratic polling station. In the current hyper-partisan environment, evidence of this kind of hack could lead to accusations by each side that the other is rigging the election.

Unfortunately, this kind of attack is probably easier than most people would imagine. This April, electronic poll books were stolen from the pickup truck of a poll worker during a "grocery run" shortly before a Congressional special election.[45] Physically accessing voting machines themselves is also certainly possible. Before he served in the White House Office of Science and Technology Policy, Princeton Computer Engineering Professor Ed Felten made an annual tradition of taking photos of unguarded voting machines left in polling stations in the days before Election Day.[46]

More troubling than attacks that require physical access to machines is the threat of remote attacks in which a small group of attackers could manipulate a large number of machines. While voting machines themselves are not connected to the internet, this does not make the spread of malware across machines (particularly ones used in the same city or county) impossible.[47] Just as computer viruses existed before the internet and could be spread through infected floppy disks, malware could be distributed by infected memory cards. These infected memory cards could cause the same kinds of problems discussed above, including misreporting totals and crashing machines, but on a larger scale.

A single computer can be responsible for programming hundreds of memory cards for one or more counties in a state.[48] As Professor J. Alex Halderman, Director of the University of Michigan's Center for Computer Security and Society, has noted, in several states, "many counties outsource their pre-election [memory card] programming to independent companies. In Michigan 75% of counties use just two 20 -person companies to do that programming."[49] There are no nationally mandated security requirements (for either hiring or physical protection of systems connected to ballot programming) for these vendors.[50] While some jurisdictions like New York State ban these computers from ever being connected to the internet, not all do so.[51]

Finally, state level central tabulators and election night reporting systems present another target that could seriously damage American's faith in election outcomes.[52] These central tabulators are frequently connected to the internet (just as county tabulators totaling counts from precincts may be).[53] Hacking these tabulators would probably not result in changing the official outcome of an election, as candidates and election officials would likely notice that the central tabulator outputs did not match the inputted vote totals provided by localities. Nevertheless, such hacking could seriously undermine voter confidence, if for example early reporting shows one candidate with a commanding lead that later disappears.

Solutions

While the attack scenarios discussed above paint a troubling picture, we are far from helpless against them. As discussed in greater detail below, independent security experts who have studied voting machine vulnerabilities are nearly unanimous in arguing that two of the most important things we can do to increase the security of these machines is to replace old, paperless Direct Recording Electronic ("DREs") voting machines with systems that include a "software-independent" record such as a voter verified paper ballot, and to conduct regular post-election audits that compare that record to the software totals generated by the voting machine.[54]

More generally, continuing to use antiquated voting machines perilously close to the end of their projected lifespan is a security risk. Election officials in the majority of states have told the Brennan Center that they would like to replace this equipment soon, but most do not have the money to do so.[55] Finding the money is crucial, as is adequately funding the EAC to guide the development of the next generation of voting machines, continue publishing information about problems with existing machines, and help local election officials with their plans to purchase new equipment.

Finally, ensuring that election officials around the country have adequate resources to implement general security best practices is always of utmost importance.

Replace Antiquated Voting Machines with New, Auditable Systems

It is time for Congress, states, and local governments to assist election officials in replacing antiquated equipment that is costly and difficult to maintain, has an increased risk of failure and crashes, and that presents a significant security risk. Perhaps most importantly Congress should act to help states and counties replace the old, paperless DREs that are still used in 14 states around the country. Jurisdictions that do so must comply with the Help America Vote Act, and ensure that new voting systems do not discriminate against disabled voters, allowing them to cast votes privately and independently.[56]

At a recent public meeting of the Technical Guidelines Development Committee (TGDC) — a federal advisory committee charged with, among other things, developing federal testing guidelines for voting system security — Professor David Wagner of the committee's Working Group stated, "the number one most important thing we can do for cybersecurity would be to ensure that the voting systems are auditable." That means that "an undetected error or fault in the voting system's software," should not be "capable of causing an undetectable change in the election results," and that the voting system should "support efficient audits."[57]

For all practical purposes, given the current state of voting technology, this means that a voting system should provide a paper record that the voter has reviewed or filled out before casting her ballot on the electronic machine. The Brennan Center estimates that in 2016, at least 80 percent of registered voters made selections on a paper ballot or voted on an electronic machine that produced a paper trail.[58] This "software independent" record provides an important security redundancy that should act as a deterrent to cyberattacks and should provide voters with more confidence that their votes have been counted accurately.[59]

The Brennan Center estimates that replacing paperless machines in every jurisdiction that still uses them should cost between $130 million and $400 million. This estimate is specific to the cost of the machine itself, and does not include other items that may be included in a new voting machine contract. Many of those items (maintenance, programming, software licensing, replacement parts) will be things a jurisdiction must pay for in some amount, regardless of whether it replaces its paperless system or not; some of the items could represent new costs (e.g., training poll workers, voter education, ballot printing.) All of these costs will vary dramatically by jurisdiction.[60]

Many state and local election officials are eager to replace their antiquated systems, but have failed to convince legislatures of the urgency of doing so.[61] A time limited offer from Congress to cover even a fraction of the costs to replace these systems is likely to go a long way toward pushing states with paperless voting machines to finally replace them with equipment that makes auditing possible and relatively easy.

Conduct Audits of Paper Ballots or the Voter Verified Paper Record

Of course, paper records of votes have limited value against a cyberattack if they are never used to check that the software-generated vote total has not been hacked. Today, only 26 states require that election officials conduct post-election audits of paper records.[62] In general, these states require officials to compare a random sample of paper ballots with voting machine totals to confirm that machines are accurately counting votes. Unfortunately, as several experts have noted, even in states where they are conducted, audits are often insufficiently robust to ensure that an election-changing software error would be found.[63] Requiring post-election audits in every state, and ensuring they sample a sufficient number of ballots, is critical to catching and preventing a hack or software error from changing the results of an election. Putting post-election auditing in place requires establishing processes and allocating funding. Unless audits are mandated for federal contests, it may also require changes to state law.[64]

These post-election audits are critical not only for catching election-changing hacks, but also reassuring the public in the integrity of final vote totals. No matter what kind of attack, real or imagined, post-election audits can assure voters they can have confidence in the final results. They are an essential tool for restoring trust in the system.

Support the Election Assistance Commission

Since 2005, the EAC has performed critical functions that help increase the reliability of our voting machines. Among other things, it sets standards and provides guidance for electoral systems on criteria like performance and security. It certifies testing laboratories that ensure that equipment actually meets those standards, and manages a quality monitoring program to track, collect and share information about reported system problems. Forty-seven states have laws or rules that require them to rely on the EAC's standards, testing or certification programs when purchasing equipment.[65] In 2016, the FBI and Department of Homeland Security worked with the EAC to share information on hacking threats; former FBI Director Comey told the Senate Judiciary Committee, "That's one of the most important things we can do is equip them with the information to make their systems tighter."[66]

Despite the agency's crucial role in ensuring the integrity of elections, some members of Congress have repeatedly and recently introduced legislation to abolish the EAC.[67] But the drive to eliminate the agency is difficult to understand in the context of the size of the federal budget. With a budget of between eight and ten million dollars a year, the EAC's costs comprise a tiny sliver of federal spending. Yet eliminating the EAC's testing, certification, and monitoring programs would create an unnecessary national security risk. Rather than abolish the agency, Congress should ensure that it has adequate resources to pursue its vital mission. The EAC can guide the development of the next generation of voting machines, continue publishing information about problems with existing machines, and help local election officials with their plans to purchase new equipment.[68]

Adopt General Security Best Practices

Many of the security problems facing election systems are similar to those facing other large distributed systems, for which there are already well established security protocols. The most important of these are discussed in a document prepared by members of the Election Verification Network in response to an invitation from the Chairman of the Election Assistance Commission in the summer of 2016.[69] While the vast majority of election officials should be aware of these best practices, more resources would help ensure that they are fully implemented.

Congressional Role in Safeguarding Elections

Under the American system, states and counties are in charge of running elections. But Congress has an important supporting role to play to ensure that federal contests are fair, accessible, and secure. It can do so by providing resources and setting standards and guidelines for federal elections.

Here are three key steps Congress should take immediately to safeguard federal elections:

1. Provide grants to replace antiquated and insecure voting machines (especially paperless DREs)*;
2. Mandate robust post-election audits for federal contests, or at the very least charge a federal agency with establishing guidelines for such audits;
3. Create a grant program to fund:
    a. Threat analyses and security improvements for state and local voter registration database systems, and other essential election systems;

    b. Upgrades and replacement of critical IT infrastructure, including voter databases;

    c. Contingency, response and resiliency planning; and

    d. Ongoing cybersecurity programs, including for maintenance and updates.

*All replacement systems should satisfy HAVA's requirement to allow voters with disabilities to vote privately and independently.

VOTER REGISTRATION DATABASES

In every state except North Dakota, eligible citizens must be registered in order to vote. Under the Help America Vote Act (HAVA), passed by Congress in 2002, states are required to create and maintain statewide databases to serve as the central source of voter registration information. Despite the federal directive, state databases are subject to differing rules and use differing technologies.[70]

These databases have nothing to do with vote tallying. Rather, they tell election officials who may vote, listing the names of registered voters along with identifying information and other characteristics such as party affiliation. This means that an attack on a database will not alter voting machine counts or election night reporting systems, but it could disrupt the orderly staging of elections and target particular groups of voters for mischief.

As with cyber threats against voting machines, the decentralization and diversity of databases can have security benefits: it makes it far less likely that database problems — whether caused intentionally or inadvertently — will impact the entire nation. The other side of the coin, though, is that the security of databases can vary greatly from one locale to the next. Some local systems may be especially vulnerable.

In securing voter registration databases, we do not need to move backwards, reversing the technology advances of the last 15 years. Rather, we need to upgrade, modernize and be smarter about how we protect this technology.

Built-in Protections Against Cyberattacks On Registration Systems

The public nature of registration lists is itself a critical security protection. Voting machines present a security challenge because of the importance our country places on the secret ballot. Because an individual has the right to keep her vote secret, it becomes more difficult to know if her vote was changed absent a "software independent" record such as a paper ballot that can be used to double check the software total. By contrast, voter registration lists are public. The parties, candidates, election officials and even voters themselves can review the voter registration lists to ensure there have been no illegitimate changes.[71]

A massive and improper manipulation of the lists is likely to be caught before, and certainly during or after an election. While the discovery of such a breach could no doubt undermine confidence in the system and potentially cause serious administrative challenges at the polls if not corrected by Election Day, there are also steps that could be taken on and after Election Day to ensure that legitimate voters can cast a ballot that will be counted. Most importantly, anyone who attempts to vote in an election must be given, at the very least, a "provisional ballot," even if the registration database indicates there is some reason they are not entitled to vote. That provisional ballot can and should be counted if the reason for the problem was manipulation of the database. In a worst case scenario, where there is evidence that a manipulation of the voter rolls might have impacted an election outcome, an election could be re-run.

Of course, ideally, there will be no breach of the database. Several election officials have informed the Brennan Center that their states have been able to use state IT security experts to harden their systems against attack in the last decade, and some have also consulted with their state National Guard services and the FBI.[72] More recently, in 2016, the Department of Homeland Security offered assistance to local elections officials to address cyber intrusions during the run-up to the 2016 elections, including a "computer hygiene" screening that scanned election agency computers and networks for malware and vulnerabilities.[73] At least 33 states and 36 counties took advantage of the agency's offer of assistance and services.[74] And in January, 2017, DHS designated electoral systems, including voter registration databases, as "critical infrastructure," paving the way for more information sharing on vulnerabilities and DHS prioritization of election officials' requests for help.[75] In addition, DHS and the FBI have shared knowledge about the tactics hackers use against databases to inform their efforts to "make their systems tighter."[76]

Finally and importantly, in the event of a breach of a voter registration system that results in some sort of manipulation of the list, there are several redundancies within every state that should allow election officials to quickly recreate their lists, or use back up lists, so that no legitimate voter will be prevented from casting a ballot, or having their votes counted. Critically, within each state, there are both state and county lists that can be used to buttress each other in the event of a breach. At the same time, virtually every state makes a nightly, offline copy of the statewide registration database that can be used to recreate lists in the event of a breach.[77] EAC Commissioner Matt Masterson and Dr. Neil Jenkins of DHS both noted in interviews with the Brennan Center that, even before the breaches of 2016, state contingency plans for database breaches or failures were already robust.[78]

Reasons for Concern About Foreign Attacks on Registration Databases

The full extent of Russia's attempts to infiltrate state voter registration systems is not yet known. A series of news reports this year have revealed progressively more information showing the attacks to be far more pervasive than was known before the election.[79] As of the writing of this report, *Bloomberg* has reported the most far-ranging account of the attacks: that Russian agents accessed election systems in 39 states, though that number has been disputed.[80] Despite direct and repeated warnings from the Obama White House to the Kremlin about the attacks, hackers affiliated with Russia's military intelligence continued attempting to access the computers of 122 election officials until shortly before Election Day.[81]

In at least one state, Illinois, the cyber intruders tried to alter or delete records in the statewide voter registration database; they failed, but it may have been a practice run for a more aggressive attack down the line.[82] Hackers were able to access publicly-available voter files in Illinois for nearly three weeks before being detected, and the system was shut down for 10 days to address the problem.[83] Their attempts to change or delete files were blocked. And in Arizona, malware was installed on the computer of a county election official who opened an e-mail attachment.[84] That malware gave hackers access to the official's username and password, which could have been used to access a county version of the voting registration system.[85]

The Russians also attacked private vendors working for election agencies in the hopes of stealing credentials that would help them access election systems themselves. In June of 2017, *The Intercept* detailed the findings of an NSA report, which recounted a cyber-attack by Russian military intelligence against a voter registration software company and election offices just days before the 2016 election. According to the NSA report, Russian government hackers appear to have used "data obtained from that operation to … launch a voter registration-themed spear-phishing campaign targeting U.S. local government organizations."[86]

Not every instance of a hacker accessing a database constitutes an attempt to disrupt an election. American officials say that hackers are constantly probing state systems — both elections systems and others — sometimes hoping to steal information about individuals on government lists. "The fact someone passes by, or runs a quick test on the database and doesn't get through, that happens every day with every major database," noted Colorado Secretary of State Wayne Williams.[87]

While this is certainly true, it is also true that if a determined state actor or terrorist group was able to gain access and control of a statewide voter registration database, it would have several ways of threatening the integrity of an election in that state. As is often noted in cybersecurity circles, "a defender has to get it right every time, while an attacker only has to succeed once."[88]

Perhaps the biggest hacking threat against voter registration systems is one where hackers manipulate the databases themselves, as the Russians attempted to in Illinois last year.[89] Attackers could try to interfere with the ability of voters to cast ballots by deleting them from lists of registered voters, marking them as felons prohibited from voting, or changing party affiliation to keep them from voting in their party's primary. These obstacles could be targeted to likely voters for one side or the other through data on demographics, address, and party affiliation. If there are no back up lists, these methods could cause problems on Election Day, forcing scores of voters to cast provisional ballots, leading to long lines, undermining faith in the fairness of an election, and creating a major administrative headache to accurately count votes after the polls closed.

Another concern is related to changing addresses for existing names on the databases, or adding entirely new (and fictitious) names and addresses to cast fraudulent votes by mail. Both attacks would necessarily be limited in nature if they were to avoid detection, but they could still do significant damage to confidence in the system. In the first instance, hackers could steal votes by changing the address on file for a large number of voters and ordering absentee ballots to vote as they choose.[90] It might remain undiscovered until those voters tried to cast their ballots on Election Day and found that votes were already recorded for them. In 2012, hackers submitted computer requests for thousands of absentee ballots in Florida, but the activity was discovered.[91] Election officials would have a way of addressing this kind of attack retroactively. They could reject absentee ballots associated with forged addresses, and make sure to count provisional ballots cast by people who had their addresses improperly changed.

In the second instance, attackers could add entirely new names and addresses and request absentee ballots for those addresses. Here, merely having the "eyes" of legitimate voters on their own registration information is not enough to catch the problem. For this reason, regular and random sampling of the database to check that registered voters and addresses are real is important.

Given intelligence officials' conclusion that Russian interference is designed to weaken the public's faith in the integrity of the election process, it may be even more likely that hackers simply try to keep databases from working.[92] They could delete whole databases[93] or use “denial of service” attacks to make systems crash on or slightly before Election Day, hampering poll workers’ ability to sign voters in. This could drastically increase long lines and make voting substantially more difficult. The resulting irregularities could lead to a widespread sense that the election was rigged or otherwise illegitimate.

This is not far-fetched. There are accusations that foreign hackers targeted the British government’s voter registration site with a denial of service attack on June 7, 2016, the last day citizens could register before the June 23 “Brexit” referendum. It is unclear what caused the website to become temporarily inaccessible, but a report issued by the House of Commons Public Accounts Select Committee included the possibility that the crash “may have been caused by a DDOS [distributed denial of service] attack using botnets.”[94]

In addition to attacks on the integrity of voter registration systems, some have argued that foreign interests may want personal information from voter databases as part of a broader campaign of election influence that includes stealing and strategically leaking information to harm a candidate or party, as the Russians did with the hack of the Democratic National Committee.[95] Damaging information can be included in ads that are custom designed for a specific demographic, and stolen personal information would allow those ads to be micro-targeted to that demographic through emails or social media. And even without any further election-related use of voter registration information, the violation of voters’ privacy can be used to harm them in other ways and can in and of itself undermine confidence in the election system.

Solutions

Given the centrality of the voter registration system to elections in nearly every state, it is surprising that there has been “very little research ... on the security and integrity of state voter registration databases … certainly nowhere near the amount of research that has focused on the security of other components of the American election infrastructure.”[96] Going forward, election professionals and independent researchers in the election field would do well to devote more resources to studying the security of state voter registries.

In the meantime, based on a review of existing literature as well as interviews with election officials in several states, the Brennan Center is able to make several observations about immediate steps that should be taken to increase the security of voter registration systems around the country. Most importantly, to the extent they have not already done so, every state should complete a thorough audit and threat analysis of their registration system, hardening the system against attack, making it more difficult for breaches to succeed, and easier to catch breaches if and when they happen. In many states, hardening the system against attack will involve upgrading and replacing antiquated IT infrastructure, including database software and operating systems.

Of course, no system can be made completely secure. If there are determined actors there will eventually be breaches against the system. States should be reviewing and updating contingency plans in the event of a successful breach that interferes with the integrity of the system, correct data is available and recoverable when needed, and eligible citizens will not be prevented from registering or voting.

The solutions offered below are quite specific, but not all states and localities will share exactly the same needs. There is no comprehensive study of voter registration systems, making it nearly impossible to pinpoint which states and localities could benefit most from a particular security measure. Congress has an important role to play in securing the nation's voter registration. It may want to follow the example of the bipartisan State Cyber Resiliency Act, a bill introduced in March in the Senate by Senators Warner (D) and Gardner (R) and in the House by Representatives Kilmer (D) and Comstock (R).[97] That bill requires the Federal Emergency Management Agency and DHS to work with state and local governments in administering and awarding State Cyber Resiliency Grants to protect critical infrastructure. Grants can support projects that will enhance "preparation, response and resiliency of computer networks," "implementing a process of continuous cyber security vulnerability assessments," adopting cybersecurity best practices, and mitigating talent gaps in the government workforce. States and localities could benefit from a more narrowly tailored program of grants that aims to provide money for the same sort of measures, more focused on securing the voter registration system.

Voter registration systems differ significantly from state to state. This provides both advantages and disadvantages from a security perspective. Because each one is different (and in most cases not built from a common software base), an attacker must develop many different methods of manipulating different kinds of databases. On the other hand, because there is so much diversity, it is far more difficult to obtain cost advantages and economies of scale by building common defenses.

Harden Systems by Updating Threat Awareness

Experts we spoke to agreed that the first step that state and local governments should take in securing voter registration systems is to regularly and fully identify the potential avenues for attack, mapping out all of the systems and entities that interact with a particular voter registration system, and developing and implementing mitigation strategies where weaknesses are identified.[98]

This may be more difficult than it sounds. A statewide registration database is constantly changing, as new information (related to registration status, voting history, and the like) comes in from voters (on line and through paper applications inputted into the system), and from a host of government actors including county election officials who keep their own lists (and may be using insecure work stations to access and update information), Departments of Motor Vehicles, social service agencies, and other states (for purposes of cross-checking duplicate registrations), among many others. As Merle King, executive director for the Center for Election Systems at Kennesaw State University in Georgia put it, "Each interface or vector ... carries inherent risk…there may be hundreds of interfaces between the [voter registration] system and county election offices and thousands of interfaces between the [voter registration] system and poll books at polling locations. Knowing the nature of these interfaces, the function they serve, the quantity and the roles and responsibilities for defining and using these interfaces is key to understanding the threat(s)."[99] In addition to understanding what must be protected, those working on security must also understand where the vulnerabilities to cyberattack are. What are the potential threats for each kind of interaction with the system? What the implications might be if a breach happened at any particular point? What can be done to identify successful intrusions and mitigate against them? And how to best prevent breach and manipulation in the first place?

There was a consensus among the experts interviewed that many states are unlikely to have completed this kind of risk assessment and audit in the last few years, despite the fact that both registration systems and cyber threats have evolved enormously over that time.[100] The cost of completing a threat assessment is likely to be manageable. The State of Ohio recently completed a full security scan of its registration system for approximately $25,000.[101] The State of Virginia also recently finished a partial threat assessment of its registration system that it considered to be the "most critical" at a cost of $40,000. Edgardo Cortes, Commissioner of the Virigina Department of Elections, estimates his department would need $80,000 annually to conduct a comprehensive" threat assessment or audit, though he notes that "[t]his is just the actual audits — costs for mitigating any identified issues would be separate."[102]

The data from Ohio and Virginia suggest that the national cost of performing such audits could come in between $1 million and $5 million annually (with the important caveat that if weaknesses were identified, there could be additional costs for increased security).[103]

The Department of Homeland Security may be able to help state and local jurisdictions carry out threat assessments and implement needed mitigation, but ultimately such a project must be led by the election offices that know and use the registration system. While states and local governments will bear the majority of the cost for such assessments, Congress has a role to play too. Targeted grants through DHS to support threat analyses and audits would encourage these urgently needed projects in all 50 states.

Upgrade and Replace IT Infrastructure, Including Databases

For many jurisdictions the single most important step in hardening may be a wholesale upgrade of the databases and the software and hardware supporting them. Based on individual state HAVA reports, annual reports from secretaries of state, and subsequent contracts for new systems, the Brennan Center estimates that 42 states are using voter registration databases that were initially created at least a decade ago.[104]

In that time, cyber threats have advanced enormously. "These systems weren't designed with [current cyber threats] in mind," according to Edgardo Cortes, Commissioner for the Virginia Department of Elections. If anything, the use of outdated databases and operating systems present even more challenges than those associated with using old voting machines. As Marc Burris, Chief Information officer of the North Carolina State Board of Elections put it, at least the oldest voting machines in the United States were actually "designed for a longer shelf life. That's not true of many of the database systems we are using today."

At least five states have recently put out requests for information, quotation or proposal to replace or upgrade their systems, while the State of Virginia is already in the process of making major upgrades on its own.[105]

Experts interviewed by the Brennan Center believed that many more states would likely require such upgrades in the near future.[106] At the same time, regular security maintenance — for things like security patches, software upgrades and licensing fees — may become more costly, as most states have exhausted the federal HAVA funds that helped them create the federally mandated databases in the first place.[107] Congress mandated the creation of these computerized statewide voter registration databases, noted Matt Damschroder, Assistant Secretary of State and Chief of Staff to the Ohio Secretary of State. While he views the creation of those systems as ultimately beneficial to elections, he noted that the failure to pay for ongoing upkeep of these systems has left election officials in a bind. "Election administration always plays second fiddle to other things that [state and local] funders need to fund."

The need for updates or replacement of IT infrastructure and software may be even greater at the local level, where systems often run on discontinued software like Windows XP or Windows 2000 that is more vulnerable to cyberattack because it is no longer vendor supported. This is particularly troubling because smaller jurisdictions frequently have little or no IT support of their own.[108] "At the state level, you are generally going to have more resources and higher levels of sophistication," noted Damschroder. Local election official are likely to have "far fewer resources," to protect against attacks.[109]

Adopt General Security Best Practices and Employ Contingency Plans

As with voting machines, employing general best practices for protecting against cyberattack will be useful in defending voter registration databases. This includes limiting employees' access to registration database as much as possible, securing work stations used by employees to access databases, and programming databases to run frequent, automated scans of registration activity to monitor for and alert election officials to potentially fraudulent or abnormal activity, such as a high volume of traffic or oddly timed traffic. A more complete list of such practices can be found in the Brennan Center's white paper, *Voting System Security and Reliability Risks*.[110] It also includes conducting regular random audits of the registration lists themselves, to ensure that registered voters are real people and that mailing address for voters are legitimate.

But of course, no system can be made completely secure. For this reason, it is also essential to ensure that election officials can recover records quickly, and that citizens can continue to effectively register and vote, in the event of a successful breach.

The basics of such contingency planning should be well known to most election officials. Among other things, staff should be trained on cyber-security best practices and a written contingency plan. Contingency plans should clearly inform employees of the steps they must take in various defined scenarios, like the loss of registration data, detection of the addition of unauthorized data, or the detection of a hacker's probe. Training should include practice drills or "war games." To protect against data being manipulated or deleted, backups should be made regularly, on removable media isolated from internet connections as well as on paper.[111] Contingency plans should cover when and how to restore databases from backups, and staff should practice executing data recovery. Neil Jenkins of DHS noted that when it came to contingency planning, election officials had the kind of mentality he had seen in the military and homeland security, describing election officials as "robust planners… [they know] they have one day to do it and do it right."[112]

DHS and the EAC may be able to help state and local jurisdictions refine their security protocols and contingency plans by sharing best practices from around the country. But having good plans is only the first step. As many election officials noted, ensuring that good security plans are actually executed can often be the most expensive part of the plan. "People have considerably underestimated the amount of resources needed to keep these databases secure," explains Edgardo Cortes. Douglas Kellner, Co-Chair of the New York State Board of elections adds that even with the best security protocol, getting resources for "enforcing and maintaining [them] is [often] the biggest challenge."[113]

Ensure Election Day Failsafe

Perhaps the most important thing to know about the security of voter registration databases and election integrity is that as long as states and local jurisdictions keep backups, including paper copies of their registration lists, no manipulation of state computer registration databases should ever prevent legitimate voters from casting a ballot, or having their votes counted.

In a worst case scenario, election officials may not realize there are problems with the voter registration list until Election Day. But even then, voters whose names are not on the list should be provided with provisional ballots that can be counted later, when the compromised registration list is reconstructed with the backups.

Officials should run tests to ensure that they are able to revert to the database as stored in an offline electronic backup in case of an attack. In jurisdictions where electronic poll books are used, the system should include paper backups of poll books, as well.

Electronic Poll Books

Electronic pollbooks (also known as e-pollbooks) are electronic versions of the voter rolls that can be used to process voters at the polls instead of using paper-based lists. Use of e-pollbooks has spread dramatically over the last decade. While only a handful of jurisdictions used them in 2006, today, 34 states and the District of Columbia use e-pollbooks for at least some portion of voting.[114]

The Presidential Commission on Election Administration recommended the use of e-pollbooks "for greater accuracy and efficiency."[115] Among the many benefits of e-pollbooks is that they can make it much easier to set up "vote centers" during early voting or on Election Day. Vote centers are "an alternative to traditional, neighborhood-based precincts." Anyone in a particular jurisdiction can vote there, regardless of where in the jurisdiction they live.[116] If a county uses multiple vote centers, the e-pollbooks can automatically sync up during the day to ensure that once someone has voted in a particular location, they can't vote in another on the same day.

While e-pollbooks have many election administration advantages, they also pose additional security challenges. As with registration databases, someone who gained control over these pollbooks could delete names from the pollbooks, mark individuals as felons prohibited from voting or as eligible citizens who already voted, or change peoples' party affiliation to keep them from voting in a party primary. While anyone impacted by such changes would have the right to ask for a provisional ballot, which could be counted after a hack or manipulation was discovered, such an attack could greatly undercut confidence in the election system, and figuring out which provisional ballots to count would be a logistical headache for election officials and poll workers.

Unlike voting machines, there are currently no national security standards for electronic poll books. Of the 34 states using electronic pollbooks, only 13 have statewide procedures or certification requirements, or certify systems statewide, according to NCSL.[117] That leaves close to two dozen states that do not have statewide procedures or certification requirements for these systems.

While there was no unanimity from election officials we spoke to on whether it was a good idea, states might benefit from the creation of voluntary federal guidelines for the security (and usability and accessibility) of e-pollbooks. Publication of such guidelines by the Election Assistance Commission is clearly permitted (if not required) under Section 222 of the Help America Vote Act.[118]

Whether the EAC does so or not, we recommend that states and localities considering the purchase of e-pollbooks work with the EAC as they develop their own test reports and standards before buying such systems. Several states, including Ohio, Virginia, California, and Indiana have collaborated with the EAC on such efforts in recent months.[119]

E-pollbooks make it simpler for election officials to run flexible, efficient elections that make voting easier. The Brennan Center encourages their use, but also urges all states using them to have paper backups of poll books ready for use in the event of their malfunction, whether due to glitches, poll worker error, or a denial of service attack.

A Note About Federal, State and Local Cost Sharing

The steps we recommend in this paper cost relatively little, certainly in comparison to the potentially damaging consequences the nation could suffer if we fail to take them. Even the most expensive step, replacing the most insecure and antiquated voting machines, is an additional expense in the tens of millions of dollars, not the hundreds of millions or billions the country routinely spends for other aspects of national security.

Unfortunately, at the moment, legislators do not appear to feel nearly enough urgency about taking these needed precautions. Part of the problem, as always in American elections, is that control is divided among federal, state and local governments. Too often, state and local governments have been slow to invest in election infrastructure, even in the face of warnings from election officials and security experts that the consequences of failing to act could be dire.[120]

Meanwhile, issues of election administration generally receive almost no attention from Congress, except when it adds new mandates in the form of laws like the Help America Vote Act. Many of these mandates address important and necessary matters, like replacing failed voting equipment or making it easier for military and overseas voters to cast a ballot that will be counted.[121] But they come with additional long term costs for which states and localities have not budgeted.

Of course, states and localities want to run elections where all eligible voters cast ballots that will be counted. And Congress has an obligation to ensure that federal contests are run with security and integrity. It is for these reasons that many of the recommendations in this report follow a formula: Congress should provide the states and localities with a time-limited offer of a partial grant in exchange for a commitment to complete the needed security step (replacing voting equipment, conducting meaningful post-election audits of federal elections, completing new threat analyses and audits for voter registration systems). We believe that this formula will provide states and localities with the urgency and resources needed to finally take these overdue measures.

CONCLUSION

The intelligence community's assessment is that Russia will continue to escalate its interference in our democracy, and other foreign powers or terrorist groups may become even bolder in the years to come. Complacency is not an option. There are weak points in our election system's armor that need to be shored up immediately. Voting machines and voter registration databases, in particular, represent two of the most critical systems to protect from attack.

Unfortunately, election law and policy has become intensely polarized, like so many contemporary issues. Both parties are too often guilty of using debates around election systems and their integrity to seek electoral advantage or whip up their base. Indeed, it is almost impossible to imagine today's Congress mustering bipartisan support for reform legislation like that seen for the Federal Election Campaign Act of 1974 or the Help America Vote Act of 2002.

But this is a national security issue too. So we should heed the wise words of Senate Foreign Relations Chairman Arthur Vandenberg who, in leading bipartisan efforts to craft defenses against the threat posed by the post-war Soviet Union, declared we must stop "partisan politics at the water's edge."[122] National security is no place for partisan squabbling. We all share the goal of protecting American democracy against foreign interference, and we must come together to safeguard the integrity of our elections.

The reforms we propose will make our elections safer and protect public confidence in their legitimacy. And time is of the essence. Implementing reforms does not happen quickly; the process must get started in order to be complete in time for the next federal elections.

We must recognize that we live in a world where foreign interests are vying for power on the world stage by trying to shape American politics, or even attempting to create doubts that democracy really works. Against that backdrop, it is clear that strengthening election security is essential to protecting our national security.

ENDNOTES

[1] *Assessing Russian Activities and Intentions in Recent U.S. Elections*, ICA 2017-01D, Office of the Director of National Intelligence, 2017, ii.

[2] Ibid.

[3] Matthew Cole et al., "Top-Secret NSA Report Details Russian Hacking Effort 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/.

[4] Michael Riley and Jordan 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.

[5] *Assessing Russian Activities and Intentions in Recent U.S. Elections*, Office of the Director of National Intelligence, iii.

[6] Riley and Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known.

[7] *Open Hearing of the Senate Intelligence Committee*, 115th Cong. (2017) (statement of James Comey, Former Director of the Federal Bureau of Investigation).

[8] *Oversight of the Federal Bureau of Investigation, Before the Senate Committee on the Judiciary*, 115th Cong. (2017) (statement of James Comey, Director of the Federal Bureau of Investigation). Comey made similar remarks in House testimony, saying, "they'll be [back] in 2020, they may be back in 2018 and one of the lessons they may draw from this is that they were successful because they introduced chaos and division and discord and sewed doubt about the nature of this amazing country of ours and our democratic process." *Open Hearing on Russian Active Measures Investigation, Before the House Intelligence Committee*, 115th Cong. (2017) (statement of James Comey, Director of the Federal Bureau of Investigation).

[9] *Open Hearing on Russian Active Measures Investigation, Before the House Intelligence Committee* (statement of James Comey, Director of the Federal Bureau of Investigation).

[10] Lt. Col. Tony Shaffer, Senior Fellow at the London Center for Policy Research and former intelligence officer, "Congressional Briefing: Strengthening Election Cybersecurity," Moderated by Karen Greenberg, May 15, 2015, https://youtu.be/Mlqv952Rb4w.

[11] Ibid.

[12] Ellen Nakashima, "The NSA has linked the WannaCry computer worm to North Korea," *Washington Post*, June 14, 2017, https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.91dec512312b.

[13] Kim Sengupta, "Isis-linked hackers attack NHS websites to show gruesome Syrian civil war images," *The Independent*, February 7, 2017, http://www.independent.co.uk/news/uk/crime/isis-islamist-hackers-nhs-websites-cyber-attack-syrian-civil-war-images-islamic-state-a7567236.html; Vasudevan Sridharan, "Al-Qaeda hacks Indian railways website urging Muslims to take up jihad," *International Business Times*,

March 2, 2016, http://www.ibtimes.co.uk/al-qaeda-hacks-indian-railways-website-urging-muslims-take-jihad-1547051; Joseph Marks, "ISIL aims to launch cyberattacks on U.S.," *Politico*, December 29, 2015, http://www.politico.com/story/2015/12/isil-terrorism-cyber-attacks-217179.

14 Microsoft recently announced that it is "releasing a new patch for Windows XP, a product it no longer formally supports, out of concern for state-sponsored cyberattacks." Ali Breland, "Microsoft releases new update citing concern over state-sponsored attacks," *The Hill*, June 13, 2017, http://thehill.com/policy/technology/337646-microsoft-releases-unusual-update-out-of-nation-state-concerns.

15 "S.516 - State Cyber Resiliency Act," accessed June 7, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/516/related-bills; "H.R.1344 - State Cyber Resiliency Act," accessed June 7, 2017, https://www.congress.gov/bill/115th-congress/house-bill/1344?r=2.

16 Washington Post Staff, "Full Transcript: Sally Yates and James Clapper Testify on Russian Election Interference," *Washington Post*, May 8, 2017, https://www.washingtonpost.com/news/post-politics/wp/2017/05/08/full-transcript-sally-yates-and-james-clapper-testify-on-russian-election-interference/?utm_term=.897cd34f213f.

17 See NPR Staff, "After DNC Hack, Cybersecurity Experts Worry About Old Machines, Vote Tampering," *NPR*, August 20, 2016, http://www.npr.org/sections/alltechconsidered/2016/08/20/490544887/after-dnc-hack-cybersecurity-experts-worry-about-old-machines-vote-tampering; Laurie Segall, "Just how secure are electronic voting machines?," *CNN*, August 9, 2016, http://money.cnn.com/2016/08/09/technology/voting-machine-hack-election/; Brian Barrett, "America's Electronic Voting Machines Are Scarily Easy Targets," *Wired*, August 2, 2016, https://www.wired.com/2016/08/americas-voting-machines-arent-ready-election/.

18 *House of Cards*, "Season 5," Directed by Daniel Minahan, et al., Netflix, May 30, 2017; *Scandal*, "Defiance," Directed by Tom Verica, Written by Shonda Rhimes and Peter Noah, ABC, November 29, 2012.

19 Mark Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers," *Christian Science Monitor*, June 17, 2014, http://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers-video.

20 Jeff Stone, "Meet CyberBerkut, The Pro-Russian Hackers Waging Anonymous-Style Cyberwarfare Against Ukraine," *International Business Times*, December 17, 2015, http://www.ibtimes.com/meet-cyberberkut-pro-russian-hackers-waging-anonymous-style-cyberwarfare-against-2228902.

21 Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers."

22 Oren Dorell, "Russia Engineered Election Hacks and Meddling in Europe," *USA Today*, January 9, 2017, https://www.usatoday.com/story/news/world/2017/01/09/russia-engineered-election-hacks-europe/96216556/.

23 "Huge Attack on Bulgaria Election Authorities 'Not to Affect Vote Count'," *Novinite.com (Sofia News Agency)*, October 27, 2015, http://www.novinite.com/articles/171533/Huge+Hack+Attack+on+Bulgaria+Election+Authorities+%27Not+to+Affect+Vote+Count%27.

24 John Leyden, "Hacker almost derailed Mandela election in South Africa," *The Register*, October 27, 2010, https://www.theregister.co.uk/2010/10/27/sa_election_hack/.

25 Martin Plaut, "Book says hacker tried to stop Mandela coming to power," *BBC*, October 26, 2010, http://www.bbc.com/news/world-africa-11630092.

26 “Dutch will count all election ballots by hand to thwart hacking,” *The Guardian*, February 1, 2017, https://www.theguardian.com/world/2017/feb/02/dutch-will-count-all-election-ballots-by-hand-to-thwart-cyber-hacking.

27 FBI Director Comey said, voting is “very, very hard to hack into because it is so clunky and dispersed.” See Elizabeth Weise, “Could the U.S. election be hacked?,” *USA Today*, October 10, 2016, https://www.usatoday.com/story/tech/news/2016/10/10/could-us-election-hacked/91866334/.

28 *The 2014 EAC Election Administration and Voting Survey Comprehensive Report*, U.S. Election Assistance Commission, 2015, 259-260, https://www.eac.gov/assets/1/1/2014_EAC_EAVS_Comprehensive_Report_508_Compliant.pdf.

29 See *Protecting the 2016 Elections from Cyber and Voting Machine Attacks, Hearing 4, Before the House Committee on Space, Science & Technology*, 114th Cong. (2016) (statement of Dr. Dan S. Wallach, Professor of Computer Science at Rice University), https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-114-SY-WState-DWallach-20160913.pdf; Sanger and Savage, “Sowing Doubt Is Seen as Prime Danger in Hacking Voting System.”

30 Jenna Portnoy, “Va. Board of Elections votes to decertify some voting machines,” *The Washington Post*, April 14, 2015, https://www.washingtonpost.com/local/virginia-politics/va-board-of-elections-votes-to-decertify-some-voting-machines/2015/04/14/46bce444-e2a6-11e4-81ea-0649268f729e_story.html.

31 *U.S. Election Assistance Commission*, “EAC Updates Federal Voting System Guidelines,” news release, March 31, 2015, https://www.eac.gov/assets/1/28/EAC%20Updates%20Federal%20Voting%20System%20Guidelines-News-Release-FINAL-3-31-15-website.pdf.

32 See *Protecting the 2016 Elections from Cyber and Voting Machine Attacks, Before the House Committee on Space, Science & Technology*, 114th Cong. (2016) (statement of Dr. Charles H. Romine, Director of the Information Technology Laboratory at the Department of Commerce’s National Institute of Standards and Technology), http://democrats.science.house.gov/sites/democrats.science.house.gov/files/documents/Romine%20Testimony.pdf; Brian Hancock, Merle S. King, and Matthew Masterson, *Infrastructure Requirements for the Testing and Certification of Election Systems*, Bowen Center for Public Affairs, 2015, http://bowencenterforpublicaffairs.org/wp-content/uploads/2015/05/Infrastructure-Requirements-for-the-Testing-and-Certification-of-Election-Systems_FINAL.5.13.15.pdf.

33 *Protecting the 2016 Elections from Cyber and Voting Machine Attacks, Before the House Committee on Space, Science & Technology* (statement of Dr. Charles H. Romine, Director of the Information Technology Laboratory at the Department of Commerce’s National Institute of Standards and Technology), https://science.house.gov/sites/republicans.science.house.gov/files/documents/HHRG-114-SY-WState-CRomine-20160913.pdf.

34 *Cybersecurity: Ensuring the Integrity of the Ballot Box, Before the Committee on House Oversight and Government Reform, Subcommittee on Information Technology*, 114th Cong. (2016) (statement of Lawrence D. Norden, Deputy Director, Democracy Program, Brennan Center for Justice at NYU School of Law), https://oversight.house.gov/wp-content/uploads/2016/09/2016-09-28-Norden-NYU-Testimony.pdf.

35 “Why a Fmr. CIA Director is Worried about Voting Machines,” *Fox Business* video, 1:16. November 7, 2016, http://video.foxbusiness.com/v/5199936869001/?#sp=show-clips.

36 Ben Wofford, “How to Hack an Election in 7 Minutes,” *Politico*, August 5, 2016, http://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144.

37 Ibid; Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, Princeton University, 2006, https://css.csail.mit.edu/6.858/2012/readings/accuvote-ts.pdf.

38 Victoria Collier, "How to Rig an Election," *Harper's*, November 2012, http://harpers.org/archive/2012/11/how-to-rig-an-election/?single=1.

39 Lawrence Norden and Christopher Famighetti, *America's Voting Machines at Risk*, Brennan Center for Justice, 2015, 9, https://www.brennancenter.org/publication/americas-voting-machines-risk. Note that since the publication of this report, Rhode Island has purchased new voting machines. "Rhode Island buys 590 new voting machines," *The Associated Press*, July 21, 2016, https://apnews.com/25d780c61bbb44f78d7ed55c76a3b189.

40 Merle King (Executive Director, Center for Election Systems, Kennesaw State University), in phone discussion with Lawrence Norden, February 5, 2015; Joe Rozell (Director of Elections, Oakland County, Michigan), in phone discussion with Lawrence Norden, February 24, 2015; Neal Kelley (Registrar of Voting, Orange County, California), in phone discussion with Lawrence Norden, February 2, 2015; Ryan Macias (Voting Systems Analyst, Office of the Secretary of State, California), in phone discussion with Lawrence Norden, March 13, 2015; Joseph Mansky (Elections Manager, Ramsey County, Minnesota), in phone discussion with Lawrence Norden, April 30, 2015; Sherry Poland (Director of Elections, Hamilton County, Ohio), in phone discussion with Lawrence Norden, February 18, 2015; Garth Fell (Elections and Recording Manager, Snohomish County, Washington), in phone discussion with Lawrence Norden, April 30, 2015; Jeremy Epstein (Deputy Division Director, National Science Foundation), email message to Lawrence Norden, May 30, 2015.

41 Jeremy Epstein (Deputy Division Director, National Science Foundation), email message to Lawrence Norden.

42 Ellen Nakashima, "The NSA has linked the WannaCry computer worm to North Korea."

43 Brian Barrett, "If You Still Use Windows XP, Prepare For the Worst," *Wired*, May 14, 2017, https://www.wired.com/2017/05/still-use-windows-xp-prepare-worst/.

44 *Security Assessment of WinVote Voting Equipment for Department of Elections*, Virginia Information Technologies Agency Commonwealth Security and Risk Management, April 14, 2015, http://www.elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf.

45 Christopher Wallace, "New details emerge in theft of Ga. voting machines," *Fox News*, April 18, 2017, http://www.foxnews.com/politics/2017/04/18/new-details-emerge-in-theft-ga-voting-machines.html.

46 Ed Felten, "E-Voting Links for Election Day," *Freedom to Tinker*, November 2, 2010, https://freedom-to-tinker.com/2010/11/02/e-voting-links-election-day/.

47 See *Protecting the 2016 Elections from Cyber and Voting Machine Attacks, Hearing 4, Before the House Committee on Space, Science & Technology,* (statement of Dr. Dan S. Wallach, Professor of Computer Science at Rice University) (explaining that malware can be spread to machines not connected to the internet, as the Stuxnet malware was when introduced into nuclear facilities in Iran.).

48 See Jesse B. Staniforth, "How Easy Would It Be to Rig the Next Election?," *ThinkProgress*, May 1, 2017, https://thinkprogress.org/how-easy-would-it-be-to-rig-the-next-election-819326cbbbd (quoting computer science expert Matt Bernhard saying, "These are small businesses with little to no operational security oversight on the part of the government … So any breach would be hard to detect").

49 Matt Bernhard and J. Alex Halderman, "Recount 2016: An Uninvited Security Audit of the U.S. Presidential Election," (presentation, University of Michigan, December 28, 2016), https://media.ccc.de/v/33c3-8074-recount_2016_an_uninvited_security_audit_of_the_u_s_presidential_election#video&t=19.

50 Jeremy Epstein notes that the use of outside vendors to program memory cards could introduce another vulnerability, depending on the security protocol in place. It is possible "that the localities email the ballot information to the outsourced company, which sets up the configuration and emails the files back for loading onto the voting machines. If [this happens], then those files could be manipulated in transit to change their behavior. Additionally, this [would imply] that although the voting machines themselves may be offline, they're getting removable media from a machine that's connected to the internet." Jeremy Epstein (Deputy Division Director, National Science Foundation), email message to Lawrence Norden.

51 N.Y. Comp. Codes R. & Regs. tit. 9, § 6210.5(b).

52 Staniforth, "How Easy Would It Be to Rig the Next Election?." (quoting Mark Graff, former chief information security officer for NASDAQ, saying that "a much more attractive approach would be to attack those machines that are aggregating the votes…").

53 Ibid, ("aggregation systems, [Graff] notes, handle significantly larger numbers of votes than precinct machines, and are likelier to be connected to the internet."); Douglas Kellner (Co-Chair, State Board of Elections, New York), email message to Lawrence Norden, May 11, 2017; Karen Hobart Flynn and Pamela Smith, "Why voting systems must be as secure as the U.S. power grid," *Reuters*, August 17, 2016, http://www.reuters.com/article/us-security-internet-voting-commentary-idUSKCN10S08G.

54 Feldman, Halderman, and Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine*, 14; Tadayoshi Kohno et al., *Analysis of an Electronic Voting System,* IEEE, 2004, 21, http://avirubin.com/vote.pdf.

55 Norden and Famighetti, *America's Voting Machines at Risk*, 5.

56 Help America Vote Act, 52 U.S.C.A. § 21081 (2015).

57 "U.S. Election Assistance Commission Technical Guidelines Development Committee, Meeting February 13-14, 2017: Day 1, Part 3," *National Institute of Standards and Technology* video, 2:06, February 13, 2017, https://www.nist.gov/news-events/events/2017/02/tgdc-meeting-february-13-14-2017.

58 See "Voting System Security and Reliability Risks", *Brennan Center for Justice*, 2016, https://www.brennancenter.org/sites/default/files/analysis/Fact_Sheet_Voting_System_Security.pdf.

59 *Cybersecurity: Ensuring the Integrity of the Ballot Box, Before the Committee on House Oversight and Government Reform, Subcommittee on Information Technology, United States House of Representatives*, (statement of Lawrence D. Norden, Deputy Director, Democracy Program, Brennan Center for Justice at NYU School of Law).

60 For more details see Lawrence Norden and Christopher Famighetti, *Estimate for the Cost of Replacing Paperless, Computerized Voting Machines*, Brennan Center for Justice, 2017, https://www.brennancenter.org/sites/default/files/analysis/New_Machines_Cost_Across_Paperless_Jurisdictions%20%282%29.pdf.

61 Lawrence Norden and Christopher Famighetti, "Now Is the Time to Replace Our Decrepit Voting Machines," *Slate*, November 17, 2016, http://www.slate.com/articles/technology/future_tense/2016/11/now_is_the_time_to_fix_our_old_voting_machines.html; Michael R. Wickline, "Bill to buy poll gear falls short," *Arkansas Online*, March 23, 2017, http://www.arkansasonline.com/news/2017/mar/23/bill-to-buy-poll-gear-falls-short-20170-1/?f=news-arkansas; David Saleh

Rauf, "States Scramble for Funding to Upgrade Aging Voting Machines," *US News*, March 12, 2017, https://www.usnews.com/news/best-states/texas/articles/2017-03-12/states-scramble-for-funding-to-upgrade-aging-voting-machines.

[62] *Cybersecurity: Ensuring the Integrity of the Ballot Box, Before the Committee on House Oversight and Government Reform, Subcommittee on Information Technology, United States House of Representatives*, (statement of Lawrence D. Norden, Deputy Director, Democracy Program, Brennan Center for Justice at NYU School of Law).

[63] Philip B. Stark, "Risk-limiting Postelection Audits: Conservative P-values from Common Probability Inequalities," IEEE Transactions on Information Forensics and Security 4.4, (2009), 1013, http://ai2-s2-pdfs.s3.amazonaws.com/c6f0/4c884e5382d0ecbea9239b83224982dc6411.pdf.; *Cybersecurity: Ensuring the Integrity of the Ballot Box, Before the Committee on House Oversight and Government Reform, Subcommittee on Information Technology, United States House of Representatives*, (statement of Lawrence D. Norden, Deputy Director, Democracy Program, Brennan Center for Justice at NYU School of Law); Ronald L. Rivest and John P. Wack, "On the notion of "software independence" in voting systems," Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences 366, (2008), 3, https://pdfs.semanticscholar.org/37a3/9c83f6c77bdafb3012a3b70aab8070298a25.pdf.

[64] For instance, in Virginia, the state law on audits includes the following requirement "No audit conducted pursuant to this section shall commence until after the election has been certified and the period to initiate a recount has expired… [a]n audit shall have no effect on the election results." 2017 Va. Acts Ch. 367.

[65] See *Protecting the 2016 Elections from Cyber and Voting Machine Attacks, Committee on Science, Space and Technology, United States House of Representatives,* (statement of Charles H. Romine, Ph.D., Director, Information Technology Laboratory, National Institute of Standards and Technology, United States Department of Commerce); Hancock, King, and Masterson, *Infrastructure Requirements for the Testing and Certification of Election Systems.*

[66] *Oversight of the Federal Bureau of Investigation, Before the Senate Committee on the Judiciary*, (statement of James Comey, Director of the Federal Bureau of Investigation).

[67] Russell Berman, "The Federal Voting Agency Republicans Want to Kill," *The Atlantic*, February 13, 2017, https://www.theatlantic.com/politics/archive/2017/02/election-assistance-commission-republicans-congress/516462/.

[68] Norden and Famighetti, *America's Voting Machines at Risk*, 7.

[69] U.S. Election Assistance Commission, *Election Verification Network 2016 Short-Term Recommendations*, January 28, 2016, https://www.eac.gov/assets/1/28/EVN%20Top%20Ten%20v7.pdf.

[70] *Assorted Rolls: Statewide Voter Registration Databases Under HAVA*, electionline.org, 2005, http://www.pewtrusts.org/~/media/legacy/uploadedfiles/wwwpewtrustsorg/news/press_releases/election_reform/electionline0605pdf.pdf.

[71] 47 states allow voters to check their registration online. The Brennan Center verified this number by checking each state's registration lookup website. Voters are unable to check their voter registration status in Maine, Mississippi, and Wyoming. "Check Your Registration! 50 State Guide. Don't let dirty tricks block your vote.," *DailyKos*, September 19, 2016, https://www.dailykos.com/story/2016/9/19/1572027/-Check-Your-Registration-50-State-Guide-Don-t-let-dirty-tricks-block-your-vote

72 Douglas Kellner, "Elections as Critical Infrastructure," (presentation, New York Board of Elections, March 17, 2017), http://electionverification.org/wp-content/uploads/2017/01/Kellner-cybersecurity-20170317.pptx; Douglas Kellner (Co-Chair, State Board of Elections, New York), email message to Lawrence Norden; Marian Schneider (Deputy Secretary for Elections and Administration, Department of State, Pennsylvania), in phone discussion with Lawrence Norden, May 5, 2017; Edgardo Cortes (Commissioner, Department of Elections, Virginia), in phone discussion with Lawrence Norden, May 24, 2017; Matthew Masterson (Commissioner, U.S. Election Assistance Commission), in phone discussion with Lawrence Norden, June 2, 2017; Matt Damschroder (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden May 25, 2017.

73 David E. Sanger and Charlie Savage, "Sowing Doubt Is Seen as Prime Danger in Hacking Voting System," *New York Times*, September 14, 2016, https://www.nytimes.com/2016/09/15/us/politics/sowing-doubt-is-seen-as-prime-danger-in-hacking-voting-system.html.

74 "NASS Reports on State Officials Findings RE: 2016 U.S. Elections," *National Association of Secretaries of State,* March 21, 2017, http://www.essvote.com/blog/98.

75 Chase Gunter, "DHS vague on rules for election aid, say states," *FCW*, February 14, 2017, https://fcw.com/articles/2017/02/14/what-does-dhs-mean-by-critical.aspx; The Department of Homeland Security, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," news release, January 6, 2017, https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical.

76 *Oversight of the Federal Bureau of Investigation, Before the Senate Committee on the Judiciary*, (statement of James Comey, Director of the Federal Bureau of Investigation).

77 Matthew Masterson (Commissioner, U.S. Election Assistance Commission), in phone discussion with Lawrence Norden; Neil Jenkins (Chief of Policy and Planning, Department of Homeland Security, National Protection and Programs Directorate, Office of Cybersecurity & Communications), in phone discussion with Lawrence Norden, June 13, 2017.

78 Ibid.

79 Ibid.

80 Riley and Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known." However, on June 21, 2017, during a hearing of cybersecurity officials before the Senate Intelligence Committee, a Department of Homeland Security official said that only 21 states "were potentially targeted by Russian government-linked cyber actors." Tal Kopan, "DHS officials: 21 states potentially targeted by Russia hackers pre-election," *CNN,* June 21, 2017, http://www.cnn.com/2017/06/21/politics/russia-hacking-hearing-states-targeted/index.html.

81 Ibid.

82 Ibid.

83 Ibid; "Illinois Elections Board Offers More Information on Hacking Incident," *Illinois Public Radio*, May 4, 2017, http://news.wsiu.org/post/illinois-elections-board-offers-more-information-hacking-incident.

84 Jeff Pegues, "After hack, Arizona working to keep its elections database secure," *CBS News,* October 13, 2016, http://www.cbsnews.com/news/after-hack-arizona-working-to-keep-its-elections-database-secure/.

85 Wesley Bruer and Evan Perez, "Officials: Hackers breach election systems in Illinois, Arizona," *CNN*, August 30, 2016, http://www.cnn.com/2016/08/29/politics/hackers-breach-illinois-arizona-election-systems/.

86 Cole et al., "Top-Secret NSA Report Details Russian Hacking Effort Days Before 2016 Election."

87 Eric Geller and Daniel Samuelsohn, "More than 20 states have faced major election hacking attempts, DHS says," *Politico*, September 30, 2016, http://www.politico.com/story/2016/09/states-major-election-hacking-228978.

88 Kevin Poulsen, "Surprise! America Already Has a Manhattan Project for Developing Cyber Attacks," *Wired*, February 18, 2015, https://www.wired.com/2015/02/americas-cyber-espionage-project-isnt-defense-waging-war/.

89 Riley and Robertson, "Russian Cyber Hacks on U.S. Electoral System Far Wider Than Previously Known." "If you can steal the data, you can change it," said Art Gilliland, a cyber security executive. Eric Chemi and Mark Fahey, "Assessing the threat of Russia hacking the US election," *CNBC*, October 11, 2016, http://www.cnbc.com/2016/10/11/russian-hackers-may-try-to-disrupt-us-elections.html.

90 "If you can impersonate a person, you can request a ballot," according to voting security expert Pamela Smith of Verified Voting. Cory Bennett, "Election fraud feared as hackers target voter records," *The Hill*, May 2, 2016, http://thehill.com/policy/cybersecurity/278231-election-fraud-feared-as-hackers-target-voter-records; Mark Potter, "Cyberattack on Florida election is first known case in US, experts say," *NBC News*, March 18, 2013, http://investigations.nbcnews.com/_news/2013/03/18/17314818-cyberattack-on-florida-election-is-first-known-case-in-us-experts-say.

91 Potter, "Cyberattack on Florida election is first known case in US, experts say." The scheme turned out to have been executed by a congressional staffer seeking an advantage in voter outreach. Patricia Mazzei, "Ex-aide to Miami Rep. Joe Garcia to head to jail in absentee-ballot case," *Miami Herald*, October 20, 2013, http://www.miamiherald.com/news/local/community/miami-dade/article1956526.html.

92 Sanger and Savage, "Sowing Doubt Is Seen as Prime Danger in Hacking Voting System."

93 The master copy of the registration database should never be online. But even deletion of a working copy that interfaced with other portals on a particular day would be extremely disruptive.

94 Josh Lowe, "Foreign Powers May Have Hacked Brexit Voter Registration Site, British MPs Say," *Newsweek*, April 12, 2017, http://www.newsweek.com/brexit-voter-registration-site-hack-russia-germany-macron-france-582697.

95 Kate Brannen, "Connecting the Dots: Political Microtargeting and the Russia Investigation," *Just Security*, May 19, 2017, https://www.justsecurity.org/41199/connecting-dots-political-microtargeting-russia-investigation-cambridge-analytica/.

96 Michael Alvarez, "How secure are state voter registration databases?," *Election Updates,* October 12, 2016, http://electionupdates.caltech.edu/2016/10/12/how-secure-are-state-voter-registration-databases/.

97 State Cyber Resiliency Act - S.516; State Cyber Resiliency Act - H.R. 1344.

98 Merle King (Executive Director, Center for Election Systems, Kennesaw State University), in phone discussion with Lawrence Norden; Marc Burris (IT Director and CIO, State Board of Elections, North Carolina), in phone discussion with Lawrence Norden, May 22, 2017; Edgardo Cortes (Commissioner, Department of Elections, Virginia), in phone discussion with Lawrence Norden; Stuart Holmes (Voting

Information System Manager, Washington Secretary of State), in phone discussion with Lawrence Norden, June 8, 2017.

99 Merle King (Executive Director, Center for Election Systems, Kennesaw State University), in phone discussion with Lawrence Norden.

100 Merle King (Executive Director, Center for Election Systems, Kennesaw State University), in phone discussion with Lawrence Norden; Marc Burris (IT Director and CIO, State Board of Elections, North Carolina), in phone discussion with Lawrence Norden; Matt Damschroder (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden; Edgardo Cortes (Commissioner, Department of Elections, Virginia), in phone discussion with Lawrence Norden; Stuart Holmes (Voting Information System Manager, Washington Secretary of State), in phone discussion with Lawrence Norden, June 8, 2017.

101 Matt Damschroder, (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden.

102 Edgardo Cortes (Commissioner, Department of Elections, Virginia), email message to Lawrence Norden, June 20, 2017.

103 Ohio and Virginia are the seventh and twelfth largest states respectively. If we assume that Ohio and Virginia's costs for conducting a full assessment represent the low and high end for conducting such assessments (in fact for much smaller states the cost would likely be less) the cost for all 50 states would range somewhere between. "List of U.S. states and territories by population," *Wikipedia*, https://en.wikipedia.org/wiki/List_of_U.S._states_and_territories_by_population.

104 The Brennan Center arrived at this figure by examining information made available by the U.S. Election Assistance Commission and by individual states. That information principally included HAVA grant reports, HAVA extension requests, state HAVA reports, state contracts for new systems, and Secretaries of State annual reports. Based on a review conducted on May 23, 2017, we estimate that 42 states implemented their voter registration database by the end of 2006. Those 42 states are: Alaska, Arizona, Arkansas, Connecticut, Delaware, District of Columbia, Florida, Georgia, Hawaii, Idaho, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Mississippi, Missouri, Montana, Nebraska, Nevada, New Hampshire, New Jersey, New Mexico, North Carolina, Minnesota, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island, South Carolina, South Dakota, Tennessee, Utah, Vermont, Washington, West Virginia, and Wisconsin.

105 Texas Secretary of State, *Purchase Order*, (Austin, Texas, 2014), http://www.sos.state.tx.us/about/procurement/2017-invoices/307-4-00455.pdf; State of New Jersey Department of the Treasury, *T-2840 Hosting, Maintenance, Support for the NJ Statewide Voter Registration System*, (Trenton, NJ, 2012), http://www.state.nj.us/treasury/purchase/noa/contracts/t2840_13-x-22355.shtml; Arizona Department of State, Office of the Secretary of State, *Bid Solicitation: ADSPO17-00007130*, (Phoenix, Arizona, 2017), https://procure.az.gov/bso/external/bidDetail.sdo?bidId=ADSPO17-00007130&parentUrl=activeBids; Washington State Office of the Secretary of State, *ITPS Work Request*, (Olympia, WA, 2017), https://www.sos.wa.gov/_assets/office/RFQQ%2017-08%20Work_Request.pdf; S.B. 2170, 100th Gen. Assemb., Reg. Sess. (Ill. 2017).

106 Edgardo Cortes (Commissioner, Virginia Department of Elections), in phone discussion with Lawrence Norden; Merle King (Executive Director, Center for Election Systems, Kennesaw State University), in phone discussion with Lawrence Norden; Matt Damschroder, (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden; Marc Burris,

(Chief Information Officer, State Board of Elections, North Carolina), in phone discussion with Lawrence Norden; Stuart Holmes (Voting Information System Manager, Washington Secretary of State), in phone discussion with Lawrence Norden, June 8, 2017.

107 The U.S. Election Assistance Commission, *Annual Grant Expenditure Report Fiscal Year 2015*, 2016, 2, https://www.eac.gov/assets/1/28/Final%20FY%202015%20Grants%20Report.pdf.

108 Norden and Famighetti, *America's Voting Machines at Risk*, 39; Merle King (Executive Director, Center for Election Systems, Kennesaw State University), in phone discussion with Lawrence Norden; Edgardo Cortes (Commissioner, Department of Elections, Virginia), in phone discussion with Lawrence Norden; Matt Damschroder (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden.

109 Matt Damschroder, (Assistant Secretary of State and Chief of Staff, Office of the Secretary of State, Ohio), in phone discussion with Lawrence Norden.

110 "Voting System Security and Reliability Risks," Brennan Center for Justice.

111 Ibid, 3-4.

112 Neil Jenkins (Chief of Policy and Planning, Department of Homeland Security, National Protection and Programs Directorate, Office of Cybersecurity & Communications), in phone discussion with Lawrence Norden.

113 Douglas Kellner (Co-Chair, State Board of Elections, New York), email message to Lawrence Norden.

114 "VRM in the States: Electronic Poll-books," last modified February 6, 2017, Brennan Center for Justice, http://www.brennancenter.org/analysis/vrm-states-electronic-poll-books.

115 Presidential Commission on Election Administration, "Presidential Commission on Election Administration Presents Recommendations to President Obama," news release, January 22, 2014, http://web.mit.edu/supportthevoter/www/2014/01/22/presidential-commission-on-election-administration-presents-recommendations-to-president-obama/.

116 "Vote Centers," National Conference of State Legislatures, http://www.ncsl.org/research/elections-and-campaigns/vote-centers.aspx.

117 "VRM in the States: Electronic Poll-books," Brennan Center for Justice.

118 52 U.S.C.A. § 20962.

119 Matthew Masterson (Commissioner, U.S. Election Assistance Commission), email message to Lawrence Norden, June 12, 2017.

120 Norden and Famighetti, *America's Voting Machines at Risk*, 8–20.

121 52 U.S.C.A. § 20902, 20982.

122 Senate Historical Office, "Featured Bio: Senator Arthur Vandenberg," *United States Senate*, https://www.senate.gov/artandhistory/history/common/generic/Featured_Bio_Vandenberg.htm.

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at **www.brennancenter.org.**
Sign up for our electronic newsletters at **www.brennancenter.org/signup.**

Latest News | Up-to-the-minute information on our work, publications, events, and more.

Justice Update | Snapshot of our justice work and latest developments in the field.

Money in Politics | Latest state and national developments and original analysis.

Redistricting Round-Up | Analysis of current legal battles and legislative efforts.

Fair Courts | Comprehensive news roundup spotlighting judges and the courts.

Liberty & National Security | Updates on privacy, government oversight, and accountability.

Twitter | www.twitter.com/BrennanCenter
Facebook | www.facebook.com/BrennanCenter
Instagram | www.instagram.com/BrennanCenter

NEW AND FORTHCOMING BRENNAN CENTER PUBLICATIONS

Secret Spending in the States
Chisun Lee, Katherine Valde, Benjamin T. Brickner, and Douglas Keith

Noncitizen Voting: The Missing Millions
Myrna Pérez, Christopher Famighetti, and Douglas Keith A

Federal Agenda to Reduce Mass Incarceration
Inimai M. Chettiar, Ames Grawert, and Natasha Camhi

Extreme Maps
Laura Royden and Michael Li

Crime in 2016: Final Year-End Data
Ames Grawert and James Cullen

The Islamophobic Administration
Faiza Patel and Rachel Levinson-Waldman

The New Era of Secret Law
Elizabeth Goitein

For more information, please visit **www.brennancenter.org.**

BRENNAN
CENTER
FOR JUSTICE
TWENTY
YEARS

at New York University School of Law

120 Broadway
New York, NY 10271
646-292-8310
www.brennancenter.org