R Street

Free markets. Real solutions.

R STREET POLICY STUDY NO. 140
April 2018

THINKING ANALYTICALLY ABOUT ELECTORAL SECURITY

Paul Rosenzweig

CONTENTS

INTRODUCTION

The cornerstone of democracy is the electoral process, as the very definition of a democratic country is one that conducts free, fair and open elections. Indeed, more than any other democratic norm, the concept of a periodic election that counts the votes of citizens and allows a peaceful transition of power is the most fundamental tenet of America's understanding of a liberal world order.

Sadly, however, our electoral infrastructure is out of date. Some portions of it are so old, in fact, that they are running "severely outdated operating systems like Windows XP, which has not been patched [...] since 2014."[1] Such a reality leaves the integrity of our voting system at risk, and the mitigation of that risk must be a federal priority.

Concern about the potential vulnerability of our electoral infrastructure naturally stems from reports about potential interference by foreign interests in the 2016 presidential election. Foreign electoral interference is nothing new. For example, one recent study found that, from 1946 to 2000, both the United States and Russia tried to influence foreign elections a total of 117 times, using both overt and covert methods.[2] But events during the Presidential Election of 2016 showed that the old tactic could be adapted to the digital age.[3]

We now know that the election process is potentially vulnerable to manipulation by hostile powers.[4] We also know that, even beyond social media manipulation, Russia quite brazenly hacked into the IT systems of political campaign committees and tried to gain access to data held by local elections boards. Though direct manipulation of the election results does not appear to have happened, the mere fact that the effort was made serves to undermine confidence in democracy and subvert our society's willingness to accept the announced results as legitimate.

There is no reason at all to think that this effort was a one-off experience. Indeed, quite to the contrary, given the poverty of America's response (one that spans multiple administrations and parties), the nation's adversaries have every reason to continue their efforts. After all, thus far, they have achieved significant disruption at virtually no cost to themselves. Or, as the Department of Homeland Security warned in recent testimony before the Senate:

[1] Bruce Schneier, "By November, Russian Hackers Could Target Voting Machines," *The Washington Post*, July 27, 2016. https://www.washingtonpost.com/posteverything/wp/2016/07/27/by-november-russian-hackers-could-target-voting-machines/?utm_term=.a7aed2770208..

[2] Don H. Levin, "When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results," *International Studies Quarterly* 60 (2016), p. 189.

[3] Robert Hackett, "Clinton Foundation Denies Hacking Claims," *Fortune*, October 4, 2016. http://fortune.com/2016/10/04/clinton-foundation-guccifer-hack-claim..

[4] To date, our experience has been that efforts to intrude on election systems have stemmed from the actions of other nation-states. However, as with any other aspect of cyber vulnerability, there is no reason to think such exploitation is limited to State actors. Indeed, we both can and should anticipate the possibility that vulnerabilities in the future may be exploited by non-State actors. In fact, one can readily imagine any number of threat vectors (ranging from identity theft to ransomware attacks on a database) that more likely originate from a non-State actor.

> Russian efforts to influence the 2016 U.S. presidential election demonstrated a significant escalation in directness, level of activity, and scope of effort compared to previous operations […] The 2018 U.S. midterm elections are a potential target for Russian influence operations.[5]

Put simply, we need to deter these attacks in the future. And, although some of these efforts may involve diplomatic responses, efforts by the intelligence community or even ways to manage attempts to influence social media, these discussions are left for another day.[6]

Instead, this paper focuses on an equally important part of the problem: namely, how America can strengthen the security of our electoral infrastructure against cyber intrusions. Today, the election system is a lot like the electrical grid system of the early 2000s in that it is a diffuse system with limited resources and insufficient awareness of potential threats. And, accordingly, just as we have significantly improved the resilience of the electrical grid, we can do the same for the electoral system.

In service of this goal, the present study first provides a descriptive summary of how voting works in America[7] and offers a characterization of the system's vulnerabilities. Second, it identifies several areas of convergence where viable solutions might be developed. In so doing, the goal is not to be prescriptive, but rather, the intention is to define some of the boundary conditions of the current electoral system that constrain the definitions of success and then explore the nature of appropriate solutions within those boundaries.

AMERICA'S ELECTORAL INFRASTRUCTURE

It is easy to think of elections as simply the process of voting and then counting the votes to see who the winner is. In reality, however, the electoral system in America is far more complex and involves a number of steps both before and after the actual voting process. Each of these steps is administered, often independently, by some electoral authority and each has its own aspects of cyber vulnerability. For these reasons, any effort to secure the elections against cyber intrusion needs to begin from an understanding of the end-to-end nature of the election process which is, in a sense, a "system of systems."

In broad strokes, the election system begins with voter registration and that registration is then maintained in a database that forms the basis for precinct-level voter lists (typically known as "voting books"). Individuals who are in a local voting book are then authorized to cast a ballot on election day (or, alternatively, by mail or in person prior to the date of election). These ballots are tallied in a tabulation that sums individual voting preferences to identify a winner. Finally, that final tabulation is sometimes subject to a post-election review, whether through statistical analysis or a recount. Each of these steps involve the collection, storage and transformation of data that, in the end, is potentially subject to cyber intrusion through degradation, disruption, denial or destruction. The following sections provide more detailed accounts of each particular step in the voting process and their current level of functioning.

Registration

The election process begins with the registration of potential voters. This can happen when a new voter seeks to register for the first time (e.g., after their 18th birthday) or when an existing voter wishes to modify their registration (e.g., if they move). In either case, the initial part of the registration has two closely related but distinct components. First, it is necessary to make sure that the registrant is, in fact, who he or she says they are. Second, new registrants must be entered into the voter registration database in a unique, non-duplicative manner.[8]

Notably, the initial registration and verification typically involves a different agency or institution than the one who maintains the database. For example, a new registrant may be enrolled at the state Department of Motor Vehicles when obtaining a license or may do so at the time of a naturalization ceremony. In short, there are multiple points of entry into the system – each of which is a potential source of vulnerability.

In general, the registration requirements are set by federal law. The Help America Vote Act of 2002 (HAVA) sets minimum standards for election administration by the states. Among its requirements is the provision that, with some minor exceptions, applicants for voter registration are required to provide a current and valid driver's license number (or a state-issued, non-driver's identification). In the absence of one of these forms, they can provide the last four

[5] Testimony of Department of Homeland Security, Senate Select Committee on Intelligence, "Election Security" [hereinafter "DHS Testimony"], 115th Congress, March 21, 2018. https://www.dhs.gov/news/2018/03/21/written-testimony-dhs-senate-select-committee-intelligence-hearing-titled-election.

[6] The Russian social media effort is detailed in *United States v. Internet Research Agency, et. al.*, (D.D.C. Feb. 16, 2018). https://www.justice.gov/file/1035477/download. Twitter's own review of Russia's use of social media is also instructive. See, "Update on Twitter's Review of the 2016 U.S. Election," *Twitter Public Policy*, Jan. 19, 2018. https://blog.twitter.com/official/en_us/topics/company/2018/2016-election-update.html. However, some of the social media influencing was not done by foreign nations. See, e.g., Andrew Keane Woods, "The Cambridge Analytica-Facebook Debacle: A Legal Primer," *Lawfare Blog*, March 20, 2018. https://lawfareblog.com/cambridge-analytica-facebook-debacle-legal-primer.

[7] Given our focus on the American system, much of what we consider will not translate well to other national systems. That said, almost all electoral systems in the West are under pressure and thus attention to the attendant vulnerabilities is warranted.

[8] See, e.g., "Improving State Voter Registration Databases: Final Report," National Research Council, 2010, pp. 7-16. https://www.nap.edu/read/12788/chapter/4#9.

digits of their Social Security number (SSN). In turn, these are linked to an individual through a biometric confirmation – typically a signature.

Database Maintenance

All of the data relating to the registrant (name, address, method of identification, party registration) is then maintained in a voter registration list. At the time that a new entry is added to the list, the database must be updated to include the information. It must also be updated every time an entry is modified (e.g., when a registered voter moves) or when an entry is deleted (because a voter has left the jurisdiction or died).

Under HAVA, which was adopted in response to the *Bush v. Gore* election controversy of 2000, every state is required to maintain:

> a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level that contains the name and registration information of every legally registered voter in the State and assigns a unique identifier to each legally registered voter in the State.[9]

Database maintenance is usually handled by state IT workers, most often within the Secretary of State's office (or equivalent). Election databases are just one of several that are typically maintained in the office and they may or may not be segregated (physically or logically) from other systems. In other words, the same computer system may maintain both election records and, for example, business filings accessible online, which means that a flaw in the authentication of business records access could give access to election records too.

Precinct Voting Books

On the day of the election (or days in states with early voting) the general state election database is abstracted into precinct-level voting books. These books are intended to identify eligible voters within a specific geographic precinct. Eligible voters who appear on the list and provide adequate identification (typically only a voting card with no photo or a state-issued driver's license) are provided a ballot to cast. In cases of doubt or dispute, the voter may be permitted to cast a provisional ballot, the validity of which will be adjudicated at a later time.

Not every voter will receive the same ballot. Most obviously, on a primary voting day, a voter may only receive the ballot for his or her party primary. Other variations are also possible. For example, eligibility may vary for an election to a school board. Or, there may be subdivisions within a precinct (in DC, for example, there are Advisory Neighborhood Commissions with representatives for every few square blocks and since there are several in each precinct, voters get a ballot that specifically applies only to their small ANC voting area).

And here another feature of the distributed American voting system comes into focus. Precinct voting books are created at the state level, using commercial technology (at least one provider of which may have been the victim of a cyberattack).[10] However, access to the ballot and administration of the voting books on the day of the election typically involve part-time workers who are not as professionalized as state staff. Indeed, given the nature of their employment (one day, every two years—often as a supplement to retirement income) precinct employees have little, if any, opportunity for cybersecurity training.

Voting and Tabulation

At this point, with ballot in hand, comes the actual casting of votes. In the modern era, there are only a few, very small jurisdictions where *only* paper ballots are used and where the results are counted by hand. In the overwhelming majority of jurisdictions, some form of automated counting occurs.

For example, there are some wherein optical character recognition (OCR) systems are used. These require voters to ink in a circle on a paper ballot and then the OCR machine reads the ballot and tallies the vote. In others, an electronic system is used to cast the ballot, so a machine tallies votes by means of a ballot display. When a voter presses a button (or a portion of the video screen) the balloting system is activated and the vote recorded. That vote is then tabulated by a computer program that records voting data and sometimes a ballot image in the computer's memory. In some areas of the country, the machine also creates a paper printout of the ballot to serve as an auditable backup system to check the accuracy of the electronic count. Finally, in a number of locations, a direct-recorded-electronic (DRE) voting system is used. The DRE system functions in the same manner as the electronic ballot system with the critical exception that no paper record is created.[11] The only record is the virtual one retained in the computer's memory.

[9] HAVA, § 303(a)(1)(A). https://www.congress.gov/bill/107th-congress/house-bill/3295/text.

[10] Nicole Perlroth et al., "Russian Election Hacking Efforts, Wider Than Previously Known, Draw Little Scrutiny," *The New York Times*, Sept. 1, 2017. https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html.

[11] 13 States have electronic-only systems with no paper record. See, Lawrence Norden, "Clear and Present Danger to U.S. Vote," *Newsday*, March 5, 2018. https://www.brennancenter.org/analysis/clear-and-present-danger-us-vote.

Finally, of course, all of these ballots are counted. Tallies from individual machines are accumulated (either by hand or by automated machine count) into a voting total for the precinct. That vote total is then conveyed—typically via an internet application on the web—to the central state voting authorities. A provisional total is done. Contested and provisional ballots are adjudicated and, in the end, a state official certifies the winner of the election.

Audits and Recounts

The final step in the election system is the post-election verification of the results. This step does not happen for every election. Indeed, it does not for most since state law generally limits the situations in which a recount may occur. Typically, recounts are done only when the results are very close and are thus disputed. Often, even in those situations, a loser must request the recount, as they are not conducted automatically.

More problematically, a "recount" is frequently not a verification of the original results by independent means. In its simplest form, a recount involves rechecking the math for the tabulation of the original results or reviewing the transcription of votes from machine to tally sheet. At a slightly higher level of inquiry, the recount may involve reviewing some of the ballots, for example, those that are cast provisionally or are otherwise in dispute. However, since a number of systems use Direct Electronic Voting (DEV), there is often no paper record against which to compare the electronic ballot for verification and thus only rarely will a full recount by re-tabulating paper or electronic ballots be requested or even feasible.

More recently, a number of experts have suggested the development of a routine systematic audit for all elections; that is, a process by which a statistically significant number of ballots is sampled and the results compared to the reported results.[12] Should the comparison produce an anomaly of significant proportion, it would signal further inquiry and possibly a full recount. For example, if a sample of 1000 ballots suggests that candidate X won 55% of the vote but the reported results are that X won by 65%, such a discrepancy would be cause for concern and further review. Of course, this method also works far more effectively with paper ballots as a fail-safe cross-check for review.

VULNERABILITIES OF THE ELECTORAL SYSTEM

In light of the foregoing, it is reasonably clear that there are many ways in which the electoral system is at risk. Avenues of vulnerability are many and varied or, as some in the security community would say, the "attack surface" is broad and diverse.

After all, at its most basic, the election system is built on data, as its very purpose is the creation and tabulation of information. And, if we have learned anything over the past 15 years of cyber intrusions, it is that data is at risk of degradation, disruption, denial or destruction. On the other hand, the hallmark of a *secure* data system is one marked by data integrity, availability and confidentiality.

When those characteristics are absent (or, more accurately, where we cannot be confident that they are present) the system is insecure. And the election data system is one that is rife with avenues by which the data that are critical to a full, fair, honest and open election can be manipulated. Consider just a few examples (selected from a much larger set of potential vulnerabilities):[13]

- The registration data for voters could be manipulated and degraded rendering it unreliable and inaccurate thereby creating questions as to who is an eligible voter;
- Voter rolls could be amended or supplemented to add or delete potential voters;
- The entire voting database could be encrypted by a ransomware attack on the day before an election, rendering it unusable;[14]
- Precinct-level vote books could be likewise degraded, destroyed or rendered unavailable for use;
- The actual voting totals in individual machines could be altered; or
- The broader voting tallies across county or state-level organizations could be manipulated via interception and modification during the course of transmission to state authorities.

In reality, the possibilities are limited only by the imagination of the adversary. Indeed, none of this parade of horri-

[12] Colorado adopted a requirement for risk-limiting audits of this sort in 2009. The first of these occurred following the 2016 election. See Jesse Paul, "Colorado embarks on a first-of-its-kind election audit that's drawing interest from out of state," *The Denver Post*, Nov. 16, 2017. https://www.denverpost.com/2017/11/16/colorado-election-audit. For a helpful summary of what a risk-limiting audit is and how it functions, see "Understanding Risk Limiting Audits," State of Colorado. https://www.sos.state.co.us/pubs/elections/VotingSystems/riskAuditFiles/UnderstandingRiskLimitingAudits.pdf.

[13] For a more detailed account of some remote-access vulnerabilities of election machines and a description of how they might be exploited, see Kim Zetter, "The Myth of the Hack-Proof Voting Machine," *The New York Times*, Feb. 21, 2018. https://www.nytimes.com/2018/02/21/magazine/the-myth-of-the-hacker-proof-voting-machine.html.

[14] In a close parallel to this, in late 2017, it was reported that a California election database of registered voters had been breached and that the thieves were demanding a bitcoin ransom to return the data. See, e.g., Dell Cameron, "Stolen California Voter Database Held for Bitcoin Ransom," *Gizmodo*, Dec. 15, 2017. https://gizmodo.com/stolen-california-voter-database-held-for-bitcoin-ranso-1821325023.

ble events need actually occur for the integrity of the election to be called into question. All that is necessary is for a sufficiently large number of voters to believe that an attack might have occurred to cast doubt upon the accuracy of the reported result.[15]

There is, of course, one modest comfort to the size and variety of the attack surface for electoral interference: its heterogeneity is a strength, as each individual system or subsystem poses its own access and exploitation challenges to the adversary. Figuring out how to alter the vote tallies in Ohio does not, for example, readily translate into an ability to exploit the voting system of North Dakota.

However, that heterogeneity is also a source of vulnerability that may ultimately outweigh any benefits. But we should not rush headlong to a uniform voting system without acknowledging that standardization carries risks of its own.

ROLES AND RESPONSIBILITIES

Given the current election infrastructure, there are some characteristics that define it in ways that differ from (though may be similar to) other aspects of American infrastructure. First, and most obviously, most parts of the American infrastructure are owned and operated by the private sector. To be sure, that sector is often heavily regulated (as, for example, with the financial services industry) but nevertheless, the owners and operators of the systems of concern are private actors.[16]

By contrast, the electoral system is exclusively governmental in nature. It is mostly based on a state governance model that rests upon a constitutional foundation. Article I, Section IV directs:

> The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Places of chusing Senators.[17]

One consequence of the state-focused nature of the system is that our elections are subject to widely varying laws, policies and procedures. Often, for example, voting is implemented at a more localized level (such as the county) and those counties vary in size and capability. It is fair to say that the largest such county (Los Angeles with more than five million voters)[18] likely approaches elections differently than a rural county with no more than 10,000.

Jurisdiction and responsibility for the operation of the electoral system is similarly diffuse and disaggregated. Although the states have the primary responsibility for operating the machinery of the election, there is a strong overlay of federal requirements. HAVA sets some of these for the more procedural aspects of voting, while substantive laws like the Voting Rights Act define some aspects of eligibility requirements.[19] There are even constitutional requirements (such as the mandate that 18 year-olds be permitted to vote).

As a result, the panoply of laws and regulations stems from many sources. State legislatures play a leading role, but Congress and its various committees often express their own mandates, which can be implemented through a host of federal agencies. Consider, for example, that the Department of Homeland Security sets policy regarding infrastructure protection while the Election Assistance Commission (EAC), established by the Help America Vote Act of 2002,[20] provides independent, bipartisan guidance to meet HAVA requirements. Indeed, the EAC has adopted voluntary voting system guidelines[21] and serves as a national clearinghouse of information on election administration. The EAC also accredits testing laboratories and certifies voting systems.[22] And elements of the national security system (like the Intelligence Community) may have information about vulnerabilities relevant to election infrastructure. This is merely one demonstration of the complexity of federal involvement in elections.[23]

At the other end of the spectrum is the inherently local nature of actual election venues. Unlike most infrastructure, much of the electoral infrastructure is operated by volunteers and quasi-volunteers. While the principal state databases are maintained by state-employed professionals, the bulk of the activity on the day of voting is managed by part-time workers with limited training.

[15] While this sort of wide-spread conspiracy theory seems inherently unlikely, we live in a world in which "Pizzagate" and "QAnon" are real phenomenon, inexplicable by rational analysis.

[16] This is, of course, not universally true. Some systems (e.g. water treatment facilities) may be operated and maintained by state or local governments. In many cases, however, they are providing a private good (such as clean water) by governmental means.

[17] US Constitution Article I, Section 4, Clause 1.

[18] Elections Division, "Report of Registration: LA County," California Secretary of State, April 6,2018. https://lavote.net/docs/rrcc/election-info/Los-Angeles-60-Day-ROR.pdf.

[19] Passed in 1965, the Voting Rights Act was adopted to eliminate racial discrimination in voting. Its general provisions, for example, outlaw literacy tests that had been used to suppress minority voting. It also contains special provisions that apply only to jurisdictions with a history of discrimination.

[20] "Help America Vote Act," U.S. Election Assistance Commission, 2018. https://www.eac.gov/about/help-america-vote-act.

[21] "Voluntary Voting Assistance Guidelines," U.S. Election Assistance Commission, 2018. https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines.

[22] "System Certification Process," U.S. Election Assistance Commission, 2018. https://www.eac.gov/voting-equipment/system-certification-process-s.

[23] Although they do not have a direct relation to the security of the election system, we should note that other regulatory agencies, like the Federal Election Commission, also play a role in managing American elections.

All of these factors create multiple, significant vulnerabilities within the election system that vary by location, operator and system implementation. At one end, the voting machine itself might be penetrated (with the intention of manipulating the tally).[24] At the other end, there may be efforts to degrade the integrity of the registration system. Such a diverse "ecosystem" means that a "one-size-fits-all" solution is impossible to imagine.

To further compound the issue, prior to 2016, the state and local operators of the election system lacked any situational awareness about the nature of threats to the infrastructure. In hindsight, this lack of concern was overly optimistic. Just as the use of aircraft as weapons on 9/11 was a strategic surprise, 2016's nascent attempts to penetrate the election system were – not unreasonably – unexpected. Happily, however, such efforts have given us fair warning of the potential. According to DHS, 21 states were the victims of intrusion attempts.[25] Illinois has publicly acknowledged that its systems were actually penetrated, though the effect (if any) of that penetration has yet to be disclosed.[26] Meanwhile, public reports suggest that an election manager in Arizona had the user name/password combination for access stolen.[27] And, perhaps most ominously, there have also been public reports that an e-voting company in Florida was penetrated, with a plausible link to adverse voting effects in precincts that used its machines.[28]

DEFINING SOLUTIONS

Such a diverse system in terms of scale, training, resources and situational awareness makes for a difficult comparison. However, the most salient one can be found in the experiences with electric grid security in the first decade of the 21st century. This is, of course, because the electrical system is similarly diverse in terms of roles and responsibilities, it has operators of different sizes, and substantial variation in training, resources and situational awareness. Further, as in the case of election security, the consequences of failure are highly variable in scope.

Further, as with elections today, in 2007, there was also a significant underinvestment in cybersecurity defense. If cybersecurity was a line item in the budget at all, it was modest because electricity providers did not see themselves as targets. By contrast, today, most electrical system providers have made substantial investments in IT security—so much so that annual expenditures are often on par with physical security.

One final aspect of the analogy bears particular emphasis. Many electrical systems are subject to substantial local control because a local political subdivision either directly operates the system or closely regulates how the private provider does. In either case, electricity costs are closely watched as part of the local political landscape.

The same is true of the election system, if not more so. State and local officials closely guard their prerogatives in the management and conduct of elections and this often brings a healthy dose of skepticism to the prospect of federal assistance. Here, too, the nature of the election system mirrors that of the electrical system and suggests that the principal avenue for improvement and intervention should be the states rather than the federal government.

In terms of electoral infrastructure, the problem set can be defined by three interrelated characteristics:

- The electoral infrastructure system is severely underresourced;
- A lack of standards or best practices creates a heterogenous attack surface;
- Electoral infrastructure lacks a central clearinghouse for information regarding threats and vulnerabilities.

None of these are new problems. Indeed, we have faced similar situations when we began the process of strengthening the security of the electrical grid, which is the reason such a comparison is instructive here, as the first approximations of a solution are not necessarily novel. This is not, of course, to suggest that these efforts are a panacea, but it is to say that there are plenty of low-hanging fruit from which we can derive significant security benefits.

Information Sharing

One lesson learned from the electric grid experience is the value of sharing threat and vulnerability information among those within a sector who are affected. When a particular technique or vector of attack is identified in an effort to penetrate one election agency, others should readily be made

[24] At DEFCON 25 in Las Vegas last year, the hacking convention hosted a "hacking village" that identified cyber vulnerabilities in U.S. election equipment, databases and infrastructure. See, e.g., Blaze et al., "DEFCON 25 Voting Machine Hacking Village," September 2017. https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf.

[25] Tal Kopan, "DHS Officials: 21 States potentially targeted by Russian hackers pre-election," *CNN*, July 18, 2017. https://www.cnn.com/2017/06/21/politics/russia-hacking-hearing-states-targeted/index.html.

[26] Rick Pearson, "Illinois election officials say hack yielded information on 200,000 voters," *Chicago Tribune*, Aug. 29, 2016. http://www.chicagotribune.com/news/local/politics/ct-illinois-state-board-of-elections-hack-update-met-0830-20160829-story.html.

[27] Ellen Nakashima, "Russian hackers targeted Arizona election system," *The Washington Post*, Aug. 29, 2016. https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.html.

[28] Perlroth et al. https://www.nytimes.com/2017/09/01/us/politics/russia-election-hacking.html.

aware of the forensic information identifying the threat. We need to establish and authorize a presumption for information sharing by the state electoral organizations with the Department of Homeland Security, as well as reciprocal DHS information sharing with states. One of the failures of the past election cycle was the notification by DHS to 21 states that they had been targeted for possible intrusion – long after the election was over. Timely, actionable cyber-threat intelligence is essential to an effective response.

The creation of such a sharing system was the principal effect of the determination by the Obama administration to treat the election system as "critical infrastructure."[29] Though election infrastructure does not fit perfectly into the existing statutory definition thereof,[30] the objection that the federal government lacks statutory authority also seems rife for policy objections.

Thus, all observers should welcome and acknowledge the recent creation of an Election Infrastructure Information Sharing and Analysis Center (EI-ISAC). Announced in March 2018,[31] such a step is an important improvement on prior arrangements that had seen election infrastructure information sharing subsumed within a broader Multi-State ISAC that shared security information about threats to *all* state cyber infrastructure.[32] The election system has some unique characteristics and is mission-critical to a functioning democracy. Accordingly, it deserves its own purpose-specific ISAC.[33]

One critical political factor to be overcome is that the designation of the election system as critical infrastructure has been challenged by some of the states as an attempted federal "takeover" of the election system. Though such language seems overblown,[34] there are real questions about how states and the federal government will cooperate going forward. As Connie Lawson, Indiana's secretary of state and president of the National Association of Secretaries of State (NASS) has said of the process:

> We were reluctant because we didn't understand what it meant and what could DHS do for us if they couldn't already do if that designation had not been made [...] We're getting along as well as we can in any forced marriage [...] Even though we didn't originally agree with the designation of critical infrastructure, we need to be at the table. And we as election officials need to teach DHS how they can help us and how they can communicate.[35]

While perhaps understandable, this sort of caution and concern needs to be addressed and ameliorated. After all, progress can only be made if all the relevant actors are convinced of each other's good will, and that the external threat is significant.

Standard Setting

A second lesson we have learned is that many actors who are aware of cyber threats are more than happy to respond, but they simply do not know what to do or how to do it. For example, small electricity providers simply did not have the technical expertise to develop plans for security improvement. One of the most successful efforts of the last five years to enhance cybersecurity was the effort by the National Institute for Standards and Technology (NIST) to develop a baseline set of standards, known as the Cybersecurity Framework. Built in a collaborative, non-regulatory manner, the NIST framework is a useful guide to best practices.

Such a process should be replicated in the electoral system. This could be achieved either through the NIST or perhaps through a separate panel of experts on election cybersecurity who, in consultation with other federal agencies and state authorities, would identify such things as best practices, guidance, requirements and audit protocols.

This is a sound idea. One concern would, however, be that it may be too slow, as the process of chartering and developing a new advisory committee is turgid at best. A better option, then, would be to build on the existing NIST structure with the addition of any unique, requisite expertise in election security. Alternatively, the development of electoral security

[29] Tim Starks, "DHS labels elections as 'critical infrastructure,'" *Politico*, Jan. 6, 2017. https://www.politico.com/story/2017/01/elections-critical-infrastructure-homeland-security-233304.

[30] The term "critical infrastructure" is defined in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)) as: "namely systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." There is a slightly plausible argument that the electoral system does not fit comfortably into this definition.

[31] Zaid Shoorbajee, "Election infrastructure ISAC created to share threats specific to voting systems," *Cyberscoop*, March 18, 2018. https://www.cyberscoop.com/election-infrastructure-isac-dhs-cis.

[32] For a description of the MS-ISAC, see "Multi-State Information Sharing & Analysis Center," Center for Internet Security, 2018. https://www.cisecurity.org/ms-isac.

[33] DHS has also created an industry-led Sector Coordinating Council (SCC). In general, the SCC is self-organized, self-run and self-governed, with leadership designated by the sector membership. The SCC serves as the industry's principal entity for coordinating with the government on critical infrastructure security activities and issues related to sector-specific strategies and policies. See, e.g., "DHS Testimony." https://www.dhs.gov/news/2018/03/21/written-testimony-dhs-senate-select-committee-intelligence-hearing-titled-election. It is therefore broader than, and a good supplement to, the EI-ISAC.

[34] Paul Rosenzweig, "No, DHS is Not Going to 'Take Over' the Electoral System," *Lawfare Blog*, Sept. 6, 2016. https://www.lawfareblog.com/no-dhs-not-going-take-over-electoral-system.

[35] Zaid Shoorbajee, "Information sharing on election security is getting better, officials say," *Cyberscoop*, March 16, 2018. https://www.cyberscoop.com/election-security-information-sharing-dhs-cis.

standards could be undertaken by existing structures in the Election Assistance Commission and at DHS. Any other model could mean that no recommendations would be returned before the 2020 election. However, America simply cannot afford to wait that long.

Even without prejudging the result of such an effort, the outlines of a series of best practices begins to emerge. A non-comprehensive list of items to be considered is as follows:

- The introduction of physical security requirements for voting machines and systems. We have already learned that voting systems are far more vulnerable when malicious actors have direct physical access to them. Remote manipulation is systematically more complex and difficult to achieve;36
- Maintenance of physical paper voting records. In an understandable reaction to the "hanging chad" problems of the 2000 election,37 America moved to electronic voting systems. But without a paper back-up record, an audit is not feasible. As one analyst has noted: "With paper, you can recount or audit that paper and carefully check the performance of the voting system, ensuring that the electronic result would match what a full hand count would show [...] Without a paper audit trail, any recount is just like hitting enter on the keyboard over and over again: You get the same answer and you have no clue if that answer is correct."38
- Implement other standard cybersecurity measures. In other critical systems, security experts have recommended the implementation of any number of relatively simple, standard protective measures. Of course, not all of these will be feasible for every election system, but all state and local election boards should be encouraged to implement any of them that are. For example, logins to critical databases should require two-factor authentication to reduce the possibility of malicious access. Further, wherever possible, election records should be encrypted and remote access to election systems via virtual private networks (VPNs) should be restricted or eliminated altogether.

It should be noted that these suggestions are not novel ones. They simply require time, money and the will to implement them.

Resources

The final piece of the puzzle, also well-known from past experience, is the question of resources. To implement recommended practices and procedures costs money.[39] And worse yet, it is money that is often not thought of as "well-spent" since the mark of success is a lack of failure. Nobody in government (or the private sector for that matter) likes to spend money on prevention, as it is cost without any readily apparent benefit.

Here, however, Congress has a role, as it can and should provide grants to states that want to modernize their infrastructure. The use of federal grant authority is a powerful way of driving the adoption of improved standards across the board. While the best rule is for the federal government *not* to dictate any particular solution, federal funding can and should be used to incentivize improvements.

Thus, the federal government should assist states and local agencies that want to move toward the aforementioned standards. The funding should be contingent on improvement but in order to avoid any argument that the federal government was commandeering state resources, it should also be voluntary with states free to decline funding if they wish.[40] Here, too, the government has begun moving in the right direction. The recently passed Omnibus spending bill includes $380 million for Election Assistance Commission grants to states "to improve the administration of elections for Federal office, including to enhance election technology and make election security improvements."[41] While that broad mandate has yet to be defined, one can easily imagine that the funding will be used for a host of security improvements.

In addition, the spending bill also attempts to give greater capability to law enforcement to counter the Russian efforts directly. It increases funding for the FBI, with some money to be used for "the counterintelligence and cyber-related investments necessary to help respond to foreign actors, including those seeking to compromise democratic institutions and processes."[42] The Department of Homeland

[36] Voting machines are used only once every two or four years. In the past, there have been jurisdictions where the machines are stored in unsecured warehouses during the intervening time, which makes them relatively easy to access.

[37] In the 2000 election, some paper ballots were incompletely punched and thus were ambiguous records.

[38] "Pennsylvania race shows need for U.S. voting machine upgrades: experts," *Reuters*, March 14, 2018. https://www.reuters.com/article/us-usa-election-pennsylvania-votingmachi/pennsylvania-race-shows-need-for-u-s-voting-machine-upgrades-experts-idUSKCN1GQ2NX.

[39] Thirty-three states have said that they need to replace their systems before 2020, but don't have the funds necessary to do so. See Norden. https://www.brennancenter.org/analysis/clear-and-present-danger-us-vote.

[40] Compare *South Dakota v. Dole*, 483 U.S. 203 (1987) [https://goo.gl/81P1JD] with *New York v. United States*, 505 U.S. 144 (1992) [https://goo.gl/fs9V2g].

[41] See Omnibus Bill, Division E. http://docs.house.gov/billsthisweek/20180319/DIV%20E%20FSGG%20SOM%20FY18%20OMNI.OCR.pdf.

[42] Ibid., Division B. http://docs.house.gov/billsthisweek/20180319/DIV%20B%20CJS%20SOM-%20FY18-OMNI.OCR.pdf.

Security title also specifies funding "to support the new Election Infrastructure Security Initiative (EISI)."[43] This commitment of resources is not the end of the story, but it is certainly a good beginning.

Other Suggestions

These are not the only things that might help, of course. For example, federal assets could be used to conduct a threat assessment of a state system or to run a "Red Team" exercise[44] to test vulnerability. Some proposals based on that idea include the establishment of a "hack the election program." This would be modeled on the successful DefCon program last year and would offer a bug bounty and a safe harbor to those who find vulnerabilities in existing systems. Third-party validation is always more convincing than internal auditing because there is an inherent perception that the vendor will cover up bad news.

We might also introduce a liability rule that makes voting machine manufacturers responsible for ensuring machines are up-to-date on patches, that any external communications (modems, routers, firewalls, etc.) managed by government agencies are configured securely, that they are open to outside bug finders, and that critical tabulation systems are segregated from communications systems—just to name a few. Here, again, the costs would be significant, but a federal funding model could at least mitigate the problem.

Finally, some of the ballot access rules that have been part of expanding the franchise might also be a potential avenue of vulnerability that needs to be addressed. In Maryland, for example, voters can request their ballot through an online application.[45] Recently, legislators there have begun to consider whether this policy decision—adopted for the valid reason of enhancing access to the ballot—might not also be a source of increased vulnerability. As we move forward in securing the electoral infrastructure, a careful assessment of the security implications of ballot access initiatives may be appropriate.

CONCLUSION

There are any number of possible ways forward to improve cybersecurity. Within the federal government, the Secure Elections Act,[46] recently introduced by a bipartisan group of senators, is a good start for the conversation about how to improve the security of our election system. It has a number of excellent ideas that merit serious consideration by Congress, the Trump administration and the states.

Those proposals are, in turn, broadly consistent with the recommendations of the Senate Select Committee on Intelligence, following its investigation of Russian influence operations in the 2016 election. The recommendations[47] make clear that states should retain the primary role of protecting the election system; that information sharing, enhanced cybersecurity and the replacement of outdated voting machines is essential;[48] and that Congress has a role in assisting the states, at least in part through funding.[49]

Meanwhile states can, and should, take the lead in securing their own systems. Illinois is an instructive example. Two years ago, their systems were breached. Today the state has "added firewalls, installed software designed to prevent intrusions and shifted staffing to focus on the threats."[50] In addition, the state has allowed their systems to be regularly scanned by the federal government and will soon be the subject of a comprehensive risk assessment by DHS.[51] In doing this, Illinois takes advantage of a suite of technical assistance programs offered to the states by DHS.[52] This sort of federal-state partnership is precisely what is necessary to combat such a grave threat to our democracy.

There is no shortage of good ideas for improving election cybersecurity. Much of what can be done merely involves simple steps that merit widespread support. Congress (and in particular the Senate) and many of the states deserve

[43] Ibid., Division F. http://docs.house.gov/billsthisweek/20180319/DIV%20F%20HOMELAND%20SOM%20FY18%20OMNI.OCR.pdf.

[44] This refers to the practice of having someone simulate the actions of an adversary attempting to attack a system.

[45] See, e.g., Rachel Chason, "Here's why cybersecurity experts say Maryland's ballot delivery system is a target for hackers," *The Washington Post*, April 1, 2018. https://www.washingtonpost.com/local/md-politics/heres-why-cybersecurity-experts-say-marylands-ballot-delivery-system-is-a-target-for-hackers/2018/04/01/403edb94-2e21-11e8-8688-e053ba58f1e4_story.html?utm_term=.60ecaaed1fca.

[46] "Safe Elections Act," S.2261, 115th Congress. https://www.congress.gov/bill/115th-congress/senate-bill/2261/text.

[47] "Russian Targeting of Election Infrastructure During the 2016 Election," Senate Select Committee on Intelligence, March 20, 2018. https://www.lawfareblog.com/document-senate-intelligence-committee-report-election-security.

[48] Securing voting machines is also the objective of the Securing America's Voting Equipment (SAVE) Act. See, e.g., Office of Senator Susan Collins, "Collins, Heinrich Unveil Bipartisan Legislation to Protect U.S. Election Systems from Foreign Interference," Press Release, Oct. 31, 2017. https://www.collins.senate.gov/newsroom/collins-heinrich-unveil-bipartisan-legislation-protect-us-election-systems-foreign.

[49] SSCI also recommends the development of a diplomatic and military deterrence strategy; a recommendation consistent with proposals by Senators Van Hollen and Rubio. https://www.rubio.senate.gov/public/_cache/files/1467ea7c-ca91-45a6-be41-f5043d4bce88/BCFC8F63C1D8049CF5593DEB32703C2C.hen18060revised.pdf.

[50] "Collins, Heinrich Unveil Bipartisan Legislation to Protect U.S. Election Systems from Foreign Interference." https://www.collins.senate.gov/newsroom/collins-heinrich-unveil-bipartisan-legislation-protect-us-election-systems-foreign.

[51] "Security of state voter rolls a concern as primaries begin," *Associated Press*, March 18, 2018. https://wtop.com/national/2018/03/illinois-primary-puts-focus-on-security-of-state-voter-rolls.

[52] In addition to cyber hygiene scans and risk assessments, DHS offers incident response assistance, field based advisors, information sharing and training assistance. See "DHS Testimony." https://www.dhs.gov/news/2018/03/21/written-testimony-dhs-senate-select-committee-intelligence-hearing-titled-election. While much of this is useful, in the absence of a presidential commitment, the priority is not as high as perhaps it should be.

praise for beginning the conversation. Those who have stuck their heads in the sand for political reasons must be persuaded that the problem is exigent and imminent. What America needs right now is commitment to carry through proposed reform to completion.

ABOUT THE AUTHOR

Paul Rosenzweig is a senior fellow of with the R Street Institute, where he works on legal and policy issues relating to cybersecurity and tech policy, including the intersection of privacy and security.

The author thanks Joe Kane and Caleb Watney for their research assistance, and Charles Duan and Zach Graves for their comments.