THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

NOTE

SECURING U.S. ELECTION SYSTEMS: DESIGNATING U.S. ELECTION SYSTEMS AS CRITICAL INFRASTRUCTURE AND INSTITUTING ELECTION SECURITY REFORMS

*Eric Manpearl**

INTRODUCTION

The recent cyber intrusions by Russia into U.S. political parties' servers and state electoral databases as well as the broad Russian disinformation campaign during the 2016 presidential election has put the issue of election security at the forefront of national security concerns. During the campaign, the Russian government hacked the Democratic National Committee (DNC), Democratic Congressional Campaign Committee (DCCC), and campaign officials' emails.[1] Russian hackers also targeted twenty-one states and breached at least Arizona's and Illinois' voter registration databases.[2] These actions were intended to sow

* Brumley Next Generation Senior Graduate Fellow, Intelligence Studies Project, Robert S. Strauss Center for International Security and Law. B.A. 2013, Rice University; J.D. and Master of Public Affairs Candidate 2018, The University of Texas School of Law and Lyndon B. Johnson School of Public Affairs. Eric Manpearl previously served as a Summer Law Clerk with the Office of the General Counsel at the Defense Intelligence Agency, Legal Counsel Division of the Office of the General Counsel at the Department of Homeland Security, and Office of Legal Policy at the Department of Justice. The views expressed in this article are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

[1] Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), http://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html?_r=0.

[2] Sari Horwitz et al., *DHS Tells States About Russian Hacking During 2016 Election*, WASH. POST (Sept. 22, 2017), https://www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html [https://perma.cc/QWE9-CR74]; Ellen Nakashima, *Russian Hackers Targeted Arizona Election System*, WASH. 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 [http://perma.cc/9FP5-FRN9].

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

distrust in the American electoral and political processes, harm Hillary Clinton's electoral prospects or at least to diminish Clinton's potential effectiveness as president if she had won, and aide Donald Trump in defeating Hillary Clinton.[3] While these intrusions into the U.S.'s political process by a foreign adversary are extremely disconcerting, fortunately, the election itself was not hacked. The U.S. must respond to the increasing threat that future elections may be hacked, though, and take action to secure our election systems now.

Maintaining the integrity of our electoral process is vital to our democracy. Designating U.S. election systems as critical infrastructure enables federal agencies involved in elections and cybersecurity to assist states and localities with assessing vulnerabilities, mitigating vulnerabilities, improving resilience, and improving coordination in cybersecurity. While some have alleged this designation is an unconstitutional assumption of power by the Federal Government,[4] designating election systems as critical infrastructure is constitutional. States should also make immediate improvements to election systems and develop contingency plans to enhance resilience in the event of a cyberattack. Further, the Federal Government should take additional actions to improve our election systems' security across the country. This past election must serve as a signal to act and secure our election systems in a prudent manner.

Part I describes the current state of election systems in the U.S. Part II details the numerous credible threats to our election systems. Part III analyzes the security measures that are currently in place. Part IV defends the designation of U.S. elections systems, defined as voter registration systems and voting systems, as critical infrastructure and argues that this is constitutional. Part V calls on states and localities to institute reforms and Congress to pass legislation to improve the security and resilience of election systems across the country.

I. THE CURRENT STATE OF THE U.S.'S ELECTION SYSTEMS

Voting in the U.S. is extremely decentralized. Over 9,000 state and local

[3] *See* Margaret Brennan, *U.S. Has High Confidence Russian Intelligence Agency Hacked DNC, DCCC*, CBS NEWS (Dec. 12, 2016, 11:25 PM), http://www.cbsnews.com/news/us-has-high-confidence-russian-intelligence-agency-hacked-dnc-dccc/ [https://perma.cc/4SHU-ZPVE] (citing a senior official in the Obama Administration as stating the U.S. has "high confidence" that the Russian hacks into the DNC and DCCC were aimed at aiding Donald Trump and disadvantaging Hillary Clinton); *see also* Lipton et al., *supra* note 1 (detailing Russian cyber intrusions into the 2016 election and the likely aims of these intrusions).

[4] *See* Katie B. Williams, *DHS Designates Election Systems as 'Critical Infrastructure'*, THE HILL (Jan. 6, 2017, 6:10 PM), http://thehill.com/policy/national-security/313132-dhs-designates-election-systems-as-critical-infrastructure [https://perma.cc/RZS2-QYKT] (explaining that state and local election officials argued that such a designation is "a federal overreach").

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

jurisdictions are responsible for running elections,[5] and there are over 114,000 active polling places on Election Day in the U.S.[6] This means that elections in the U.S. are governed by an array of different statutes, regulations, processes, and procedures put in place at the state and local levels, and that several different types of voting equipment are used.

Following the election chaos of the 2000 presidential election, in which election issues in Florida thrust the nation into uncertainty, Congress enacted the Help America Vote Act (HAVA) to reform the election process.[7] As part of the reform, HAVA required states to create computerized voter registration lists.[8] This has led thirty-two states and the District of Columbia to allow people to register to vote online,[9] which has had the benefits of enfranchising more people and saving governments money.[10] While HAVA required states to "provide adequate technological security measures to prevent the unauthorized access to the computerized list[s]," the statute did not require the Election Assistance Commission (EAC) to develop technological standards or guidelines for these registration systems.[11] Unfortunately, states and localities have not developed robust security standards for protecting these systems. Often, state and local election authorities lack the technological knowledge necessary for protecting

[5] Julie H. Davis, *U.S. Seeks to Protect Voting System from Cyberattacks*, N.Y. TIMES (Aug. 3, 2016), http://www.nytimes.com/2016/08/04/us/politics/us-seeks-to-protect-voting-system-against-cyberattacks.html.

[6] *Cybersecurity: Ensuring the Integrity of the Ballot Box: Hearing Before the Subcomm. on Info. Tech. of the H. Comm. on Oversight & Gov't Reform*, 114th Cong. 16 (2016) (statement of Thomas Hicks, Comm'r, Election Assistance Comm'n) [hereinafter *Cybersecurity*].

[7] *See* Help America Vote Act of 2002, 52 U.S.C. §§ 20901–21145 (2012).

[8] *Id.* § 21083(a)(1)(A).

[9] Shane Harris, *Election Hackers Could Erase You*, THE DAILY BEAST (Oct. 16, 2016, 1:00 AM), http://www.thedailybeast.com/articles/2016/10/16/election-hackers-could-erase-you.html [https://perma.cc/A6LG-Z7WR] [hereinafter Harris, *Election Hackers Could Erase You*].

[10] Cory Bennett, *Election Fraud Feared as Hackers Target Voter Records*, THE HILL (May 2, 2016, 6:00 AM), http://thehill.com/policy/cybersecurity/278231-election-fraud-feared-as-hackers-target-voter-records [https://perma.cc/PW9G-79RV].

[11] 52 U.S.C. § 21083(a)(3) (2012 & Supp. III 2016). The EAC is an independent commission that was created by HAVA and is "charged with developing guidance to meet [certain] HAVA requirements, adopting voluntary voting system guidelines, . . . serving as a national clearinghouse of information on election administration[,] . . . accredit[ing] testing laboratories and certif[ying] voting systems, . . . audit[ing] the use of HAVA funds[,] . . . [and] maintaining the national mail voter registration form developed in accordance with the National Voter Registration Act of 1993." *About the US EAC*, U.S. ELECTION ASSISTANCE COMM'N, https://www.eac.gov/about-the-useac/ [https://perma.cc/T65R-G4YC] (last visited Jan. 2, 2018).

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

the data in registration systems and thus far, third-party vendors used to build and maintain the systems have not been held to a high standard.[12]

There are currently two main types of voting equipment used in the U.S—optical scan paper ballot systems and direct recording electronic (DRE) systems.[13] With optical scan paper ballot systems, voters mark paper ballots to indicate their voting selections and these paper ballots are then tabulated by scanning devices.[14] Ballots are either scanned at the polling place or collected and transported to be scanned at a central location.[15] With DRE systems, voters make their selections using pushbuttons, touchscreens, or dials and these votes are recorded directly into a computer's memory.[16] Votes are stored in the computer system and ultimately all voters' selections are combined.[17] These DRE systems became popular after the 2000 presidential election, in which many ballots were incorrectly or incompletely marked making them invalid,[18] when Congress allocated over $3 billion through HAVA to upgrade voting equipment to avoid ambiguous ballots.[19] Some DRE systems are equipped with Voter Verified Paper Audit Trail (VVPAT) printers so that voters can confirm the choices they made with the selections appearing on the computer before recording their vote into the computer's memory.[20] While both optical scan paper ballots and DRE systems depend on computers to count the votes, optical scan paper ballot systems and DRE with VVPAT systems have a preserved paper record, which can be made available in the event of a recount or audit.[21] Regular DRE systems do not produce any paper trail so there are not paper ballots for recounts or audits. Forty states primarily use either optical scan paper ballot systems or DRE with VVPAT systems (with the vast majority of these states using optical scan paper ballot systems), which have a paper trail, while

[12] Bennett, *supra* note 10.

[13] *See Voting Equipment in the United States*, VERIFIED VOTING, https://www.verifiedvoting.org/resources/voting-equipment/ [https://perma.cc/SA6P-28XG] (last visited Dec. 27, 2017).

[14] *Id.*

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] RICHARD L. HASEN, THE VOTING WARS: FROM FLORIDA 2000 TO THE NEXT ELECTION MELTDOWN 11–40 (2012) (recounting the chaos of the 2000 presidential election).

[19] See Jack Karsten & Darrell M. West, *How to Save Election Technologies from "Hanging Chads" and Software Malfunctions*, BROOKINGS INST. (Nov. 8, 2016), https://www.brookings.edu/blog/techtank/2016/11/08/how-to-save-election-technologies-from-hanging-chads-and-software-malfunctions/ [https://perma.cc/L479-BGQG] (analyzing the rise in the use of DRE systems following the 2000 presidential election).

[20] *Voting Equipment in the United States*, *supra* note 13.

[21] *Id.*

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

ten states primarily use DRE systems that do not leave a paper trail.[22] In addition, a number of jurisdictions across the country continue to use paper ballots, which allows voters to cast their votes by making marks with pen or pencil, and requires these ballots to be counted manually.[23]

Unfortunately, the U.S.'s voting technology is rapidly aging. HAVA's allocation of money to states to replace outdated voting equipment led "the vast majority of election jurisdictions in the United States [to] purchase[] and deploy[] new voting systems" by 2006.[24] The expected lifespan for the these electronic voting systems is between ten to twenty years,[25] and some experts believe the lifespan is likely closer to ten years for most systems.[26] In the 2016 election, forty-two states used election machines that were purchased at least ten years ago, and thirteen of those states used election machines that were at least fifteen years old.[27] This current state of affairs led the Presidential Commission on Election Administration (PCEA) to warn of an "impending crisis . . . from the widespread wearing out of voting machines purchased a decade ago . . . ."[28] The Brennan Center for Justice found that officials in at least thirty-one states hope to purchase new election machines before 2020, but officials from twenty-two of those states expressed that they did not know where they would get the funds to pay for new machines.[29] Replacing aging election equipment across the

[22] *Cybersecurity*, *supra* note 6, at 27–28 (statement of Andrew W. Appel, Professor, Princeton University); *see also Across the U.S., a Patchwork of Voting Methods*, PEW RESEARCH CTR. (Nov. 7, 2016), http://www.pewresearch.org/fact-tank/2016/11/08/on-election-day-most-voters-use-electronic-or-optical-scan-ballots/ft_16-11-07_votingtechnology/ [https://perma.cc/QF56-RVR7] (providing a map of voting methods used in counties across the country).

[23] *Id.*

[24] LAWRENCE NORDEN & CHRISTOPHER FAMIGHETTI, BRENNAN CTR. FOR JUSTICE, AMERICA'S VOTING MACHINES AT RISK 8 (2015).

[25] *Id.* (citing Telephone Interview with Merle King, Exec. Dir., Ctr. for Election Sys., Kennesaw State Univ. (Feb. 5, 2015)).

[26] *Id.* (citing Telephone Interview with Doug Jones, Professor, Univ. of Iowa (May 21, 2015); Telephone Interview with Daniel Lopresti, Professor of Computer Sci., Lehigh Univ. (May 26, 2015); E-mail from Rokey Suleman, former Exec. Dir. of the D.C. Board of Elections and Ethics to Lawrence Norden, Deputy Dir., Democracy Program, Brennan Ctr. for Justice (June 1, 2015, 11:50 PM)).

[27] Lawrence Norden & Christopher Famighetti, *Now is the Time to Replace Our Decrepit Voting Machines*, SLATE (Nov. 17, 2016), http://www.slate.com/articles/technology/future_tense/2016/11/now_is_the_time_to_fix_our_old_voting_machines.html [https://perma.cc/Q3Q8-WZ2X].

[28] PRESIDENTIAL COMM'N ON ELECTION ADMIN., THE AMERICAN VOTING EXPERIENCE: REPORT AND RECOMMENDATIONS 62 (2014).

[29] NORDEN & FAMIGHETTI, *supra* note 24, at 6.

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

country could cost over $1 billion.[30]

Further, thirty-one states and the District of Columbia allow military and overseas voters to return ballots electronically.[31] In 2008, nearly three million people overseas from the states that allow ballots to be returned electronically were eligible to vote in that year's election, and about 500,000 of those individuals requested ballots.[32] In addition, Alaska allows anyone in the state to submit the voter's ballot electronically.[33] These ballots are often returned "as attachments to email, as faxes, including online fax systems, as uploads to Internet portals, and even as transmissions through online ballot marking systems to a remote vendor's portal, where the ballots are rendered for printing or for electronic transmittal back to an election official."[34]

II. THE CREDIBLE THREATS FACING U.S. ELECTION SYSTEMS

U.S. election systems face credible threats. Election systems that are under government control, which are voter registration systems and voting systems, are the primary concern.

A. Voter Registration Systems

Voter registration systems are the most vulnerable part of U.S. election systems. These databases are often maintained online,[35] which makes them susceptible to illicit actors. At least two states, Arizona and Illinois, suffered cyber intrusions into their voter registration databases in 2016.[36] In Arizona, the

---

[30] *Id.* at 17.

[31] Shane Harris, *How Hackers Could Destroy Election Day*, THE DAILY BEAST (Aug. 3, 2016), http://www.thedailybeast.com/articles/2016/08/03/how-hackers-could-destroy-election-day.html [https://perma.cc/C3UL-KLQG] [hereinafter Harris, *How Hackers Could Destroy Election Day*].

[32] Ian Urbina, *States Move to Allow Overseas and Military Voters to Cast Ballots by Internet*, N.Y. TIMES (May 8, 2010), http://www.nytimes.com/2010/05/09/us/politics/09voting.html?_r=1.

[33] Harris, *How Hackers Could Destroy Election Day*, *supra* note 31; *Online Ballot Delivery*, ALASKA DIV. OF ELECTIONS, http://www.elections.alaska.gov/Core/votingbyonline.php [https://perma.cc/JR8A-6X6V] (last visited Jan. 2, 2018).

[34] David L. Dill et al., Response to Request for Information on Developing a Framework to Improve Critical Infrastructure Cybersecurity (Apr. 8, 2013), https://www.nist.gov/sites/default/files/documents/2017/06/06/040813_verified_voting_1.pdf [https://perma.cc/X6X3-WXHJ].

[35] *Online Voter Registration*, NAT'L CONF. OF ST. LEGISLATORS (Dec. 6, 2017), http://www.ncsl.org/research/elections-and-campaigns/electronic-or-online-voter-registration.aspx [https://perma.cc/6VNB-ZZNC].

[36] Nakashima, *supra* note 2.

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

attackers introduced malicious software into the state's voter registration database,[37] which led to the state shutting down its voter registration system for nearly a week.[38] Hackers obtained personal information of voters in Illinois, which forced the state to shut down its voter registration system for ten days.[39] Exfiltrating voter information is not the biggest concern in this area, though. It would be far more troubling if an attacker attempted to selectively disenfranchise voters.

One could delete voters from registration databases with the aim of aiding one candidate over another.[40] Thus, an attacker could selectively delete voters who are registered with a particular political party, or are likely to support the candidate of that party (which can often be ascertained based on how the person's community typically votes and demographic characteristics).[41] These voters could demand a provisional ballot, which must be provided under HAVA,[42] when they go to vote and find out that their names are not on the registered voter lists, though. The use of provisional ballots would still enable these voters to participate in the election, but could create many difficulties.[43]

A large number of provisional ballots being requested could lead to long lines at polling places that have many affected voters, which could in turn disincentivize people from voting because they do not have the time to wait for an extended period, and undermine peoples' confidence in the election because of concerns over tampering. A large number of provisional ballots could

---

[37] Michael Isikoff, *FBI Says Foreign Hackers Penetrated State Election Systems*, YAHOO! NEWS (Aug. 29, 2016), https://www.yahoo.com/news/fbi-says-foreign-hackers-penetrated-000000175.html [https://perma.cc/FK4M-6BRK].

[38] Nakashima, *supra* note 2.

[39] Isikoff, *supra* note 37.

[40] Michael Riley & Jordan Robertson, *Russian Cyber Hacks on U.S. Electoral System Far Wider than Previously Known*, BLOOMBERG (June 13, 2017, 5:00 AM), https://www.bloomberg.com/news/articles/2017-06-13/russian-breach-of-39-states-threatens-future-u-s-elections [https://perma.cc/K4CR-7Z2Y].

[41] *See, e.g.*, Nate Cohn, *There Are More White Voters than People Think. That's Good News for Trump*, N.Y. TIMES (June 9, 2016), https://www.nytimes.com/2016/06/10/upshot/there-are-more-white-voters-than-people-think-thats-good-news-for-trump.html (predicting how individuals are likely to vote based on demographics).

[42] 52 U.S.C. § 21082(a) (2012). Voters use provisional ballots when there is a question regarding a voter's eligibility. *Provisional Ballots*, NAT'L CONF. OF ST. LEGISLATORS (June 19, 2015), http://www.ncsl.org/research/elections-and-campaigns/provisional-ballots.aspx [https://perma.cc/HE96-7AEJ]. The provisional ballot is typically kept separate from other ballots until after the election and then a determination is made regarding whether the voter was eligible to vote. *Id.* If the voter was indeed eligible to vote, the provisional ballot will be counted. *Id.*

[43] *See* Harris, *Election Hackers Could Erase You*, *supra* note 9.

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

severely disrupt the process of determining who the election winner is, too, because states adhere to different procedures and schedules for determining whether a provisional ballot was indeed cast by an eligible voter.[44] Also, provisional balloting would not solve the problem for people who vote by mail, which occurs in great numbers in states such as California, Colorado, Nevada, Oregon, and Washington because these voters may not realize that they never received a ballot.[45]

B. Voting Systems

Voting systems are vulnerable to attack in multiple places. Voting machines themselves may be attacked, overseas voting that occurs electronically may be attacked, and the tabulation of votes may be attacked.[46] An attack on these systems would be the most damaging to U.S. election systems and the integrity of our democracy.

Although U.S. elections are extremely decentralized, which presents an added layer of protection against widespread attacks, an adversary would only need to attack the U.S. in a few key battleground states during a presidential election or competitive districts during other elections.[47] Adversaries study and understand the U.S.'s political system and can focus their efforts on specific locations where their actions would be the most likely to have an impact. Even if an adversary is unable to sway an election in a specific direction, the mere interference into the U.S.'s electoral process would greatly undermine our democratic system and could potentially delegitimize the election's winner in the eyes of many citizens.

1. Voting Machines.

Voting machines are attractive to attackers because they are computers in which votes are stored electronically, and an attacker could seek to flip votes in favor of a certain candidate. While voting machines are always supposed to be separated from the Internet, the machines connect to election management computers to load software and ballot definitions.[48] This usually occurs by inserting a cartridge or memory card into the voting machine after the cartridge or memory card has been prepared on an election management computer.[49] This

---

[44] *See id.*

[45] *Protecting the 2016 Elections from Cyber and Voting Machine Attacks: Before H. Comm. on Sci., Space & Tech.*, 114th Cong. 46–47 (2016) (statement of Dan S. Wallach, Professor, Rice University) [hereinafter *Protecting the 2016 Elections*].

[46] Ben Wofford, *How to Hack an Election in 7 Minutes*, POLITICO (Aug. 5, 2016), http://www.politico.com/magazine/story/2016/08/2016-elections-russia-hack-how-to-hack-an-election-in-seven-minutes-214144 [https://perma.cc/LFD9-EV6S].

[47] *Protecting the 2016 Elections*, *supra* note 45, at 42.

[48] *Id.* at 47.

[49] Andrew Appel, *Which Voting Machines Can Be Hacked Through the Internet?*,

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

creates a situation in which attackers may gain access to the voting machines indirectly by accessing the election management computers. In fact, election management computers are likely occasionally connected to the Internet.[50] Ultimately, this means that attackers could gain access to the election management computers when they are connected to the Internet and use this as a point of entry to corrupt the files that will ultimately be uploaded to the voting machines, which would in turn corrupt the voting machines. Voting machines connect to each other through in-precinct local networks and exchange memory cards so malware transmitted to just a small number of machines could be transmitted across all voting equipment in an entire jurisdiction by a sophisticated nation-state actor.[51]

Despite the fact that voting machines are never supposed to be connected directly to the Internet, disturbingly, voting machines in 20% of Virginia's voting precincts were actually equipped with a wireless network to allow ballot programming and voter data to be sent between machines up until 2014.[52] In the 2014 election, officials in one Virginia county became concerned when these voting machines, the AVS WINVote DRE touchscreen machines, repeatedly crashed on Election Day.[53] This led to an investigation by the Virginia State Board of Elections, who discovered that "wireless cards on the voting systems could allow 'an external party to access the [machine] and modify the data [on the machine] without notice from a nearby location.'"[54] The Board added that 'an attacker could join the wireless ad-hoc network, record voting data or inject malicious [data.]'"[55] The voting machines were in fact using "abcde" as their

FREEDOM TO TINKER (Sept. 20, 2016), https://freedom-to-tinker.com/2016/09/20/which-voting-machines-can-be-hacked-through-the-internet/ [https://perma.cc/CV2B-8FKY].

[50] *Id.*

[51] Dan Wallach, *A Response to the National Association of Secretaries of State*, FREEDOM TO TINKER (Aug. 9, 2016), https://freedom-to-tinker.com/2016/08/09/a-response-to-the-national-association-of-secretaries-of-state/ [https://perma.cc/K386-BQMU].

[52] Pam Fessler, *Vulnerable Voting Machine Raises Questions About Election Security*, NPR (Apr. 16, 2015, 5:03 AM), http://www.npr.org/sections/itsallpolitics/2015/04/16/399986331/hacked-touchscreen-voting-machine-raises-questions-about-election-security.

[53] *Id.*

[54] NORDEN & FAMIGHETTI, *supra* note 24, at 12 (quoting VA. INFO. TECH. AGENCY, SECURITY ASSESSMENT OF WINVOTE VOTING EQUIPMENT FOR DEPARTMENT OF ELECTIONS 3 (2015), https://www.elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf [https://perma.cc/F59L-LZ8Q]).

[55] *Id.* (quoting VA. INFO. TECH. AGENCY, SECURITY ASSESSMENT OF WINVOTE VOTING EQUIPMENT FOR DEPARTMENT OF ELECTIONS 7 (2015), https://www.elections.virginia.gov/WebDocs/VotingEquipReport/WINVote-final.pdf [https://perma.cc/F59L-LZ8Q]).

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

encryption key—an easy password for hackers to obtain.[56] These machines were enormously vulnerable and were decertified by the Virginia State Board of Elections after the investigation discovered this.[57] There is no way to know if these machines were ever actually hacked, but the fact that this vulnerability existed at all should be unacceptable.[58]

Even if the entire process does not connect to the Internet, there is still a threat that a nation-state attacker could gain access to voting machines. The U.S. and Israel successfully infected Iranian nuclear centrifuges with the Stuxnet malware to damage the centrifuges despite the fact that these centrifuges were never connected to the Internet.[59] It is still unknown how the Stuxnet malware gained access to the centrifuges, but the fact that it did raises the possibility that a sophisticate nation-state adversary could infect computers that are not connected to the Internet.

Further, U.S. election systems are susceptible to insider threats, which are malicious threats that come from within an organization—often from employees. A nation-state adversary could recruit an individual working for a state or local election commission or an employee of a voting machine manufacturer with direct access to voting machines or election management computers. Such an individual could hack the voting machines or election management computers that the person had access to in an effort to promote the agenda of the nation-state that the person was acting on behalf of.

In fact, any malicious individual could hack a voting machine if the person is in close physical proximity to the machine for a long enough period of time. Professor Andrew Appel has demonstrated this after purchasing a voting machine for his own research.[60] Appel simply picked the machine's lock with

---

[56] Fessler, *supra* note 52. "Encryption is the process of encoding data or information such that only those who are authorized by the creator of the information are able to access the data or information. Those who are not authorized by the creator of the data or information to have access are prevented access to encrypted data or information. Even if a third party without authorization intercepts the data or information, encrypted data or information will appear unreadable." Eric Manpearl, *Preventing "Going Dark": A Sober Analysis and Reasonable Solution to Preserve Security in the Encryption Debate*, 28 U. FLA. J.L. & PUB. POL'Y 65, 67–68 (2017) (footnotes omitted). Obtaining the encryption key would allow an attacker to access the data, though.

[57] *Id.*

[58] These machines, the AVS WINVote touchscreen machines, were not certified by the EAC and the EAC has claimed that the machines would not have passed EAC testing. NORDEN & FAMIGHETTI, *supra* note 24, at 12–13.

[59] David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html (describing the Stuxnet malware attack on Iranian nuclear centrifuges, which are machines that are used to enrich uranium).

[60] Wofford, *supra* note 46.

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

the help of a graduate student, and replaced one of the computer chips in the machine with one of his one, which was programmed to modify election results.[61] This attack only took several minutes to accomplish and could be conducted by a single person with the correct skill set and illicit intentions.[62] Such an attack could only directly affect the machines the individual gained physical access to, though, so this threat is less severe than the potential of remote hacking, which could affect a wide number of machines quickly and therefore have a larger impact on an election. Voting machines do, however, connect to each other and, ultimately, to election management systems, which, in turn, connect to other voting machines.[63] A sophisticated nation-state actor could develop malware to spread across an entire jurisdiction.[64] An attack on only one machine by such an actor could, therefore, have widespread consequences.

Voting machines are not only susceptible to illicit attacks but are also vulnerable because of their age. Machine parts, computer memory cards, and touchscreens are more likely to fail as the machines get older because of wear and tear over time.[65] Over time, the glue that is used in touchscreen machines to hold the touchscreen in place can degrade, which causes the touchscreen to shift and can result in the machine recording votes for a different candidate than the voter intended to select because of the misalignment between the screen the voter sees and the actual wiring inside the machine.[66] The Brennan Center for Justice's study on voting machines found many instances of machine parts and memory cards failing in recent elections, which caused numerous states to remove machines from service during the elections.[67] Malfunctioning machines and having to take machines out of service during elections can result in long voting lines, which in turn disenfranchises people by disincentivizing people to go vote. This is unhealthy for democracy, and greater voting machine failures due to old age would only exacerbate this problem. The main concern regarding older voting machines for the purpose of this paper, though, is that older machines can often have less robust security. For example, the Virginia AVS WINVote voting machines that turned out to be extremely vulnerable to attackers who could inject malicious software into the machines were first used

[61] *Id.*

[62] *Id.*

[63] Wallach, *supra* note 51.

[64] *Id.*

[65] NORDEN & FAMIGHETTI, *supra* note 24, at 12.

[66] *See id.* at 13.

[67] *Id.* at 13–14 (describing various errors that occur in voting machines as they age and detailing numerous instances of states having to take machines out of service because of these failures).

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

in the early 2000s and were in operation until the 2014 election.[68]

These threats are most severe when there is no paper trail to recount or audit. Even if voting machines were hacked such that they recorded vote tallies that did not accurately reflect how voters cast their ballots, optical scan paper ballot systems and DRE with VVPAT systems have a paper record of voters' choices. These paper records are kept in secure ballot boxes and can be used to conduct recounts or audits in such a situation. Thus, the availability of paper trails enables election officials to determine the true vote totals even if an election has been hacked. However, regular DRE systems do not produce any paper trail, which means one could never discern whether a voting machine's vote tally accurately reflected voters' selections or not because there would be nothing with which to compare the computer tally.

Pennsylvania is likely the greatest concern in this area. Fifty of Pennsylvania's sixty-seven counties vote on regular DRE systems that do not produce any paper trail and four additional counties in Pennsylvania have a mix of paper ballots and DRE systems that do not produce any paper trail.[69] In Pittsburgh and Philadelphia, about 900,000 voters cast their ballots in the 2016 election on these DRE systems.[70] This is a large enough portion of voters to swing the election in favor of one candidate over the other in this battleground state. In 2016, Donald Trump defeated Hillary Clinton in the presidential election in the state by under 50,000 votes and Patrick Toomey defeated Katie McGinty in Pennsylvania's Senate race by about 100,000 votes.[71] If the state's DRE voting machines—or just the DRE machines in Pittsburgh and Philadelphia—were hacked, the entire election could have been decided by the attacker without any paper trail to go back to after the fact to conduct an adequate recount or audit to determine who voters truly selected in the election.

The pitfalls of not having a paper trail actually came to fruition in Florida in 2006. Shockingly, 15% of ballots cast in a congressional race in Florida that year

---

[68] *See supra* Section II.B.1.

[69] *The Verifier - Polling Place Equipment in Pennsylvania - November 2016*, VERIFIED VOTING, https://www.verifiedvoting.org/verifier/#year/2016/state/42 [https://perma.cc/T22R-5Z2E] (last visited Jan. 28, 2018).

[70] *2016 General Election*, ALLEGHANY COUNTY, PA, http://results.enr.clarityelections.com/PA/Allegheny/63905/Web02/#/ (last updated Dec. 1, 2017) (giving election results from Pittsburgh); *2016 General President and Vice President of the United States: District Wide Results*, OFF. OF THE PHILA. CITY COMMISSIONERS, https://www.philadelphiavotes.com/en/resources-a-data/ballot-box-app (last visited Jan. 2, 2018) (giving election results from Philadelphia); *The Verifier - Polling Place Equipment in Pennsylvania - November 2016*, *supra* note 69 (showing that Allegheny County, the county in which Pittsburgh is located, and Philadelphia County, the county in which Philadelphia is located, both vote on regular DRE systems that do not produce any paper trail).

[71] *Pennsylvania Results*, N.Y. TIMES (Sept. 13, 2017, 3:24 PM), http://www.nytimes.com/elections/results/pennsylvania.

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

on DRE machines did not register any choice in the race, which equates to about 18,000 voters.[72] That race was decided by less than 400 votes.[73] It is highly unlikely that such a high number of voters who showed up to the polls that year actually intended to abstain from casting a vote in this race. However, because these DRE machines lacked a paper trail, there were no paper ballots to use in conducting a recount or audit to determine if there were errors with the machines themselves that led to votes not being recorded.[74]

2. Overseas Internet Voting.

Military and overseas voters who return ballots electronically over the Internet are the most vulnerable to hackers. The fact that these ballots are exposed to the Internet throughout the process makes them enormously susceptible to hacking, especially when they are transmitted without encryption. Ballots that are submitted as attachments to emails are perhaps the most troubling of this type of voting. David Jefferson, a computer scientist at Lawrence Livermore National Laboratory, has warned that an attacker could rather easily,

> filter, out of the vast stream of email, exactly those emailed ballots addressed for a chosen set of election email servers (such as county servers in one or more states that are of interest to the attacker), and then to automate a process to either discard ballots that contain votes she does not like, or replace them with forged ballots that she likes better, all the while keeping the voter's signed waiver and envelope attachments intact.[75]

Although military and overseas voters do not make up a large portion of the voters in any state, this could still be a significant enough number of votes to swing a close election. Also, Alaska allows anyone in the state to send their ballots in over the Internet,[76] which leaves all voters who choose to return their ballots in this manner susceptible to hackers.[77] States do not have any paper trails for votes received over the Internet other than what was sent to the states, which may be manipulated.[78] Thus, a recount or audit would be unsuccessful at

---

[72] David Jefferson, *What Happened in Sarasota County?*, 37 THE BRIDGE 17, 17 (2007); Tim Padgett, *Voting Out E-Voting Machines*, TIME (Nov. 3, 2007), http://content.time.com/time/nation/article/0,8599,1680451,00.html.

[73] *Id.*

[74] *Id.*

[75] David Jefferson, *What About Email and Fax?*, VERIFIED VOTING, https://www.verifiedvoting.org/resources/internet-voting/email-fax/ [https://perma.cc/PGG4-FRFN] (last visited Dec. 15, 2016).

[76] *See supra* Part I.

[77] Harris, *How Hackers Could Destroy Election Day*, *supra* note 31.

[78] Jefferson, *supra* note 75.

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

detecting malicious activity regarding these ballots because there is no way of knowing whether the votes received actually matched the votes submitted.[79] Faxes can also be subject to similar types of attacks as emails. Moreover, faxes submitted through online systems, which is increasingly the case, are indistinguishable from emails in terms of vulnerability.[80]

Ballots that are submitted over the Internet can actually subject entire election networks to malware.[81] Attackers could exploit the file a voter uses to return his ballot, which is often a Portable Document Format (PDF) file (a notoriously vulnerable file format),[82] such that the file carries malware into the receiving election network.[83] If voting machines are ever connected to this network, the malware could infiltrate the voting machines thereby enabling them to be hacked.

3. Vote Tabulations.

Finally, the state and local computers that aggregate the vote totals from precincts are vulnerable. While these machines are never supposed to be connected to the Internet, at least Professor Andrew Appel has questioned whether this is truly the case.[84] These computers may very well become accidentally connected to the Internet from time to time, especially because county clerks are typically not sophisticated computer security experts, and even an accidental Internet connection for a short period of time would leave these systems vulnerable to attackers.[85]

In 2014, Russian hackers—Advanced Persistent Threat (APT) 28 or Fancy Bear,[86] which is the same hacking group that was responsible, along with APT 29 or Cozy Bear (another Russian hacking group),[87] for the hacks into the DNC

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *Id.*

[83] *See id.* (discussing the possibility of a hacker using malware attached to a ballot submitted over the Internet to infiltrate an election network); *see generally* Karthik Selvaraj & Nino Fred Gutierrez, *The Rise of PDF Malware*, SYMANTEC SECURITY RESPONSE (2010), https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the_rise_of_pdf_malware.pdf [https://perma.cc/C922-C8CK] (detailing the use of PDFs for malicious activity and the current threat landscape).

[84] Wofford, *supra* note 46.

[85] *See id.*

[86] *See, e.g.*, *Who is FANCY BEAR?*, CROWDSTRIKE BLOG (Sept. 12, 2016), https://www.crowdstrike.com/blog/who-is-fancy-bear/ [https://perma.cc/MKE6-QDNZ].

[87] *See, e.g.*, Jeff Stone, *Meet Fancy Bear and Cozy Bear, Russian Groups Blamed for DNC Hack*, CHRISTIAN SCI. MONITOR: PASSCODE (June 15, 2016), https://www.csmonitor.com/World/Passcode/2016/0615/Meet-Fancy-Bear-and-Cozy-Bear-

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

and DCCC—attempted to sabotage Ukraine's elections by attacking Ukraine's Central Election Commission's computers.[88] APT 28 planned to hack the election results to show that a fringe, far-right party had won the election, when in reality they had not.[89] Fortunately, the malware was discovered shortly before election results were scheduled to be reported and dissemination of the results was delayed by a few hours while the true vote tallies were aggregated.[90] Russian-affiliated news networks nonetheless broadcasted that the fringe, far-right party that APT 28 had attempted to show as winning the election had indeed emerged victorious.[91] While Ukraine had the ability to eventually determine who the real winner was even if APT 28 had been successful in its attack, the aim of the operation was to undermine Ukrainian democracy and portray the burgeoning democratic movement in the country as being dominated by far-right fascists, thus promoting Russian interests in the region.[92] These same tactics could be used to undermine the confidence of the American electorate, even though this part of the system could be independently audited by going back to the printed precinct vote totals and manually aggregating the vote totals.[93]

III. CURRENT SECURITY MEASURES

The extreme decentralization of the U.S.'s election systems is a protective measure in itself. U.S. election systems do not have a single entry point for attackers, which would otherwise allow them to do a massive amount of damage upon exploitation. Instead, hackers must focus on numerous different states and

Russian-groups-blamed-for-DNC-hack [https://perma.cc/5EL9-KA54]; *Who is COZY BEAR?*, CROWDSTRIKE BLOG (Sept. 19, 2016), https://www.crowdstrike.com/blog/who-is-cozy-bear/ [https://perma.cc/579K-GZEZ].

[88] Levi Maxey, *Is It Possible to Hack the Vote?*, THE CIPHER BRIEF (Nov. 6, 2016), https://www.thecipherbrief.com/article/tech/is-it-possible-to-hack-the-vote [https://perma.cc/V6N6-PQAA].

[89] *Id.*

[90] *Id.*

[91] Mark Clayton, *Ukraine Election Narrowly Avoided 'Wanton Destruction' From Hackers*, CHRISTIAN SCI. MONITOR: PASSCODE (June 17, 2014), https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers [https://perma.cc/MB52-9D99]; Elias Gross, *Did Russia Really Hack U.S. Election Systems?*, FOREIGN POL'Y (Aug. 30, 2016, 8:23 PM), http://foreignpolicy.com/2016/08/30/did-russia-really-hack-u-s-election-systems/ [http://perma.cc/NZ75-ACZY].

[92] *Id.*

[93] Andrew Appel, *Security Against Election Hacking - Part 1: Software Independence*, FREEDOM TO TINKER (Aug. 17, 2016), https://freedom-to-tinker.com/2016/08/17/security-against-election-hacking-part-1-software-independence/ [https://perma.cc/J3SF-6AQL].

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

localities that use a variety of different types of voting machines and computer systems. However, while this serves as a deterrent against attacks, hackers could still affect the outcome of a close election by focusing on specific battleground states or localities. Further, even if an attack is unsuccessful in actually affecting the outcome of an election, the occurrence of the attack alone would undermine confidence in American democracy and could partially delegitimize the ultimate victor because people would be skeptical of the election results after an attack.

Beyond the deterrence of decentralization, voting machines are tested and certified by the EAC with the help of the National Institute of Standards and Technology (NIST) and the EAC monitors certified election systems. HAVA requires the EAC to develop standards for voting systems and administer testing and certification of voting systems in accordance with these standards.[94] The EAC offers these services under its Testing and Certification Program, and state participation in the program is voluntary under federal law.[95] As of 2011, thirty-five states required participation in at least some part of the Testing and Certification Program under state law.[96] The EAC's standards for voting systems are detailed in the Voluntary Voting System Guidelines (VVSG), which focus on data security and data transmission.[97] Currently, forty-seven states have adopted the VVSG into their own voting systems certification process in part or in full.[98] Voting machines are tested against VVSG requirements in EAC laboratories, and only those machines that conform to the VVSG are certified by the EAC.[99] Specifically, as part of this testing, the EAC ensures that certified voting machines cannot be connected to the Internet.[100] The EAC also monitors voting systems after they have been certified to ensure that these systems

[94] 52 U.S.C. § 21101, 20971 (2012 & Supp. III 2016) (requiring the EAC to develop standards and provide "testing, certification, decertification, and recertification" of voting systems).

[95] STATE REQUIREMENTS AND THE FEDERAL VOTING SYSTEM TESTING AND CERTIFICATION PROGRAM 3 (2009).

[96] *See* U.S. ELECTION ASSISTANCE COMM'N, CATEGORIES OF STATE, TERRITORY, AND DISTRICT OF COLUMBIA PARTICIPATION IN VOTING STANDARDS 1 (2011) (providing an updated list of states that require participation in the EAC's Testing and Certification Program as of 2011) [hereinafter CATEGORIES].

[97] *Voluntary Voting System Guidelines*, U.S. ELECTION ASSISTANCE COMM'N, https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines/ [https://perma.cc/5J66-NGYA] (last visited Dec. 15, 2016). NIST provides technical support to the EAC in drafting these guidelines. 52 U.S.C. § 20961(e)(1).

[98] *Cybersecurity*, *supra* note 6, at 18.

[99] *Id.* at 6.

[100] *EAC Commissioner: It Would Take an Army to Hack Into Our Voting System*, WASH. POST (Oct. 7, 2016), https://www.washingtonpost.com/video/postlive/eac-commissioner-it-would-take-an-army-to-hack-into-our-voting-system/2016/10/06/7489de6e-8beb-11e6-8cdc-4fbb1973b506_video.html [https://perma.cc/F6FF-JVPD].

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

continue to work properly.[101] Unfortunately, as of 2011, only thirteen states required EAC certification before a machine could be procured by the state.[102]

Some states have been proactive in instituting security measures. States use "logic and accuracy testing" to make sure voting machines are properly recording votes during voting periods.[103] This testing typically consists of election officials "casting a small number of votes for each candidate, on a handful of machines, and making sure they're all there in a mock tally."[104] Local election officials have procedures to ensure that machines are "zeroed,"[105] which guarantees that the machines do not have votes already stored on them before actual voting begins. While "logic and accuracy testing" and ensuring that machines are "zeroed" are prudent measures, passing these tests only means that the machines are not malfunctioning—not that the machines have not been compromised by a sophisticated nation-state attacker.[106] However, some election officials conduct more sophisticated "parallel testing," in which "some voting equipment is pulled out of general service and is instead set up in a mock precinct, on [E]lection [D]ay, where mock voters cast seemingly real ballots. These machines would have a harder time distinguishing whether they were in 'test' versus 'production' conditions."[107] This type of testing could detect that the machines had been hacked because the final vote tally that hacked machines would show would be different from the actual votes that were cast during testing. However, election officials would not know if a machine had failed this test until after the election was over because "parallel testing" must occur simultaneously with actual voting to guarantee that an attacker could not tell the difference between a test machine and a machine actually being used to cast real votes.[108] Unless the voting machines left a paper trail, there would be no way to determine the true intent of voters who used machines in the jurisdiction that had been attacked. This would create a chaotic situation of possibly needing to re-run the election in those jurisdictions, and would certainly undermine peoples' confidence in the democratic process. Finally, thirty-two states and the District of Columbia conduct post-election audits in which randomly-selected precincts hand count the paper voting records and compare these totals with the totals reported by the electronic voting systems to ensure that the machines accurately recorded and counted the votes.[109] Jurisdictions that use DRE systems

---

101 *Cybersecurity*, *supra* note 6, at 19–20.

102 CATEGORIES, *supra* note 96.

103 Wallach, *supra* note 51.

104 *Id.*

105 *Id.*

106 *See id.*

107 *Id.*

108 *Id.*

109 *See Post-Election Audits*, NAT'L CONF. OF ST. LEGISLATORS (Oct. 10, 2017),

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

without paper records cannot participate in these audits.

Ultimately, the current security mechanisms are insufficient to defend against current and future threats. The 2016 election must serve as a wake-up call for the U.S. to enhance the security of its election systems to protect the integrity of our democracy. There are meaningful reforms that should be enacted to prevent a catastrophic attack in the future.

IV. DESIGNATING U.S. ELECTION SYSTEMS AS CRITICAL INFRASTRUCTURE

U.S. election systems, defined as voter registration systems and voting systems, were correctly designated as critical infrastructure by Department of Homeland Security (DHS) Secretary Jeh Johnson in January 2017.[110] Presidential Policy Directive (PPD) 21: Critical Infrastructure Security and Resilience endeavors to promote a national effort to "strengthen and maintain secure, functioning, and resilient critical infrastructure."[111] PPD-21 authorizes the Secretary of DHS to identify critical infrastructure and defines critical infrastructure as "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."[112] Election systems certainly fall within this definition as the legitimacy of our government depends on having properly functioning election systems, and an attack on these systems would have a debilitating effect on the country. The main purpose of a critical infrastructure designation is to enable the Federal Government to provide as much support as possible to the identified sectors through a partnership. Thus, designating election systems as critical infrastructure enables the Federal

http://www.ncsl.org/research/elections-and-campaigns/post-election-audits635926066.aspx [http://perma.cc/3ZU9-6RDY] (detailing each state's audit procedure) [hereinafter *Post-Election Audits*, NAT'L CONF. OF ST. LEGISLATORS]; *see also Post Election Audits*, VERIFIED VOTING, https://www.verifiedvoting.org/resources/post-election-audits/ [https://perma.cc/PA5T-LQZC] (last visited Dec. 15, 2016) [hereinafter *Post Election Audits*, VERIFIED VOTING]. Although Kentucky and Pennsylvania both have auditing requirements, these states have widespread use of DRE systems that do not produce paper trails so it is impossible for these states to actually conduct audits, which were statutorily enacted before DRE systems were adopted. *Id.*

[110] Press Release, U.S. Dep't of Homeland Sec., Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector (Jan. 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical [http://perma.cc/M2QU-4C3J].

[111] *Presidential Policy Directive - 21: Critical Infrastructure Security and Resilience*, WHITE HOUSE (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil [http://perma.cc/C45M-M737].

[112] *Id.*

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

Government to provide robust assistance to state and local election officials and aid these officials in assessing vulnerabilities, mitigating vulnerabilities, improving resilience, and improving coordination. Also, designating election systems as critical infrastructure helps promote a norm against cyber-interference in elections because this action demonstrates that the U.S. views its election systems as vital.[113]

Currently, the U.S. has sixteen identified critical infrastructure sectors.[114] The most beneficial aspect of being designated critical infrastructure for these sectors has been the sector-specific Information Sharing and Analysis Centers (ISACs). ISACs bring members of a specific sector together and enable the sharing of information and analysis.[115] For instance, the financial sector ISAC has quickly provided sector-specific cybersecurity threat information to private businesses in the financial services industry and provided firms in the sector with "procedures and best practices for guarding against known and emerging

[113] The U.S. should retaliate against Russia for the cyber intrusions into our election process during the 2016 election as part of promoting norms against cyber-interference in elections. While interference in other countries' elections frequently occurred during the Cold War, such interference in a U.S. election is unprecedented. *See* Don H. Levin, *When the Great Power Gets a Vote: The Effects of Great Power Electoral Interventions on Election Results*, 60 INT'L STUD. Q. 189, 189 (2016) (calculating that the U.S. and U.S.S.R. interfered with other countries' elections a combined total of 117 times during the Cold War); *see also* Eric Manpearl, *Presidential Elections: A Perilous Time for U.S. Intelligence*, LAWFARE RES. PAPER SERIES, Sept. 2016, at 1 (2016) (analyzing when intelligence issues have intersected with presidential politics throughout U.S. history and failing to find a robust interference campaign by a foreign power). The U.S. cannot stand for this type of meddling into our democracy and taking offensive retaliatory measures would help establish deterrence against future intrusions into our election systems. The U.S. should be wary of responding through cyber actions against Russia, though, because the U.S. is itself tremendously dependent on cyber security. As such, escalation in this domain would likely ultimately leave the U.S. more exposed, despite our greater offensive capabilities. Instead, the U.S. should leverage its advantages in other domains to ensure that Russia pays an extremely large cost for its interference in the U.S. election. While a discussion about what deterrence should consist of is an enormously important topic, the focus of this paper is instead on the defensive security mechanisms that the U.S. should put in place to protect its election systems.

[114] *Presidential Policy Directive - 21: Critical Infrastructure Security and Resilience*, *supra* note 111. The sixteen critical infrastructure sectors are: chemical; commercial facilities; communications; critical manufacturing; dams; defense industrial base; emergency services; energy; financial services; food and agriculture; government facilities; health care and public health; information technology; nuclear reactors, materials, and waste; transportation systems; and water and wastewater systems. *Id.*

[115] *See Information Sharing*, U.S. DEP'T OF HOMELAND SEC., https://www.dhs.gov/topic/cybersecurity-information-sharing [https://perma.cc/XW5J-A2TM] (last updated Sept. 27, 2016) (describing ISACs in detail).

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

security threats."[116] During the 2016 election, DHS reached out to state and local officials, shared information with election officials to improve their awareness of the existing cyber threats, and shared information with election officials to help them combat the existing cyber threats through the Multi-State ISAC.[117] DHS should not have to find a circular method to enable information sharing regarding threats against U.S. election systems and defenses to protect these systems. Instead, there should be an election-systems-sector-specific ISAC to facilitate constant information sharing among election officials and cybersecurity experts. Such an ISAC can now be created following the designation of election systems as critical infrastructure. Secretary Johnson took an important step in securing U.S. election systems by making this designation.

Some have argued that DHS designating election systems as critical infrastructure is unconstitutional, and even made the unfortunate claim that the goal of designating election systems as critical infrastructure is to enable a federal takeover of election administration.[118] The Constitution provides that "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."[119] Professor John Yoo (a former Deputy Assistant Attorney General in the Office of Legal Counsel at the Department of Justice (DOJ))[120] and Hans von Spakovsky (a senior fellow at the Heritage

---

[116] *About FS-ISAC*, FIN. SERVS. INFO. SHARING & ANALYSIS CTR., https://www.fsisac.com/about [https://perma.cc/6YM4-BL84] (last visited Dec. 15, 2016).

[117] *Cybersecurity*, *supra* note 6, at 9 (testimony of Andy Ozment, Assistant Sec'y, U.S. Dep't of Homeland Sec.).

[118] *See id.* at 25 (statement of Brian P. Kemp, Sec'y of State, State of Georgia); Timothy Courtney, *Department of Homeland Security to Intervene in State Elections*, FEDERALIST SOC'Y (Aug. 31, 2016), http://www.fed-soc.org/blog/detail/department-of-homeland-security-to-intervene-in-state-elections [https://perma.cc/8Z66-YZPP] (compiling a variety of statements from several law professors and former Department of Justice (DOJ) officials decrying a potential critical infrastructure designation as an unconstitutional infringement upon states' rights); Hans A. von Spakovsky, *Why Does DHS Want to Designate Election Booths 'Critical Infrastructure?'*, THE HERITAGE FOUND. (Aug. 17, 2016), http://www.heritage.org/election-integrity/commentary/why-does-dhs-want-designate-election-booths-critical-infrastructure [https://perma.cc/78CV-RJCX] (asserting that the idea of a critical infrastructure designation is really being promoted in an effort to nationalize election administration). Those opposed to having election systems designated as critical infrastructure assert that "[t]he D.C. response to [the cyberattacks] has been to take steps towards federalizing aspects of elections, election systems, and standardizing security measures," *Cybersecurity*, *supra* note 6, at 23.

[119] U.S. CONST. art. I, § 4, cl. 1.

[120] *John Yoo*, U.C.–BERKLEY SCH. OF L., https://www.law.berkeley.edu/our-faculty/faculty-profiles/john-yoo/ [https://perma.cc/SXZ6-E44G] (detailing Professor John

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

Foundation, former member of President Trump's now terminated Presidential Advisory Commission on Election Integrity, former member of the Federal Election Commission (FEC), and former DOJ lawyer)[121] have argued that DHS would violate this clause by designating election systems as critical infrastructure because this designation would be an invasion of authority reserved to the states.[122] The National Association of Secretaries of State (NASS) has also opposed DHS's designation of election systems as critical infrastructure, citing states' authority to regulate elections and declaring that "the U.S. Department of Homeland Security has no authority to interfere with elections, even in the name of national security."[123] However, these arguments misunderstand the nature of critical infrastructure designations.

Although the Secretary of DHS designating election systems as critical infrastructure is an unprecedented declaration by the Executive Branch,[124] the action does not constitute a regulation. Designating a sector as critical infrastructure does not impose any regulations on the sector or provide the Federal Government with any regulatory authority. Instead, as discussed *supra*, the Federal Government seeks to "work with critical infrastructure owners and operators . . . to take proactive steps to manage risk and strengthen the security and resilience of the Nation's critical infrastructure."[125] Thus, designating election systems as critical infrastructure does not violate the Constitution by infringing upon the states' roles in elections in any manner.

Further, designating election systems as critical infrastructure is not an attempt to assert federal power over states. Again, the Federal Government's role is coordination, assessment, and information sharing. The Federal Government has not used the critical infrastructure designation to direct or control any of the sixteen current critical infrastructure sectors, and the result

Yoo's biography).

[121] Exec. Order 13,820, 83 Fed. Reg. 969 (Jan. 3, 2018) (terminating the Presidential Advisory Commission on Election Integrity); *Hans A. von Spakovsky*, HERITAGE FOUND., http://www.heritage.org/staff/hans-von-spakovsky [https://perma.cc/JX65-EZM3] (detailing Hans von Spakovsky's biography).

[122] Courtney, *supra* note 118.

[123] Nat'l Ass'n of Secretaries of State, *NASS Resolution Opposing the Designation of Elections as Critical Infrastructure*, at 21–22 (Feb. 18, 2017).

[124] Questions regarding the Federal Government's power in relation to this clause of the Constitution have previously revolved around congressional action, and the Legislative Branch's authority in this field. *See, e.g.*, Arizona v. Inter Tribal Council of Arizona. Inc., 133 S. Ct. 2247, 2253 (2013) (recognizing that "[t]he Elections Clause has two functions. Upon the States it imposes the duty ('shall be prescribed') to prescribe the time, place, and manner of electing Representatives and Senators; upon Congress it confers the power to alter those regulations or supplant them altogether.").

[125] *Presidential Policy Directive - 21: Critical Infrastructure Security and Resilience*, *supra* note 111.

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

will be the same with an election systems sector. Our election systems are vital to our democracy, and we should aim to protect these systems to the greatest extent possible, which means collaborating at all levels of government. Designating election systems as critical infrastructure allows for just that.

V. ADDITIONAL ACTIONS TO IMPROVE THE SECURITY OF U.S. ELECTION SYSTEMS

Designating election systems as critical infrastructure should only be the initial step in improving the security of U.S. election systems. States and localities should institute reforms and Congress should pass legislation to improve the security and resilience of election systems across the country.

A. State and Local Reforms

All states and localities responsible for running elections should institute a series of legislative and procedural reforms. In regards to registration systems, election officials should maintain paper copies of voter registration lists to serve as back-ups to the voter registration database systems in case malicious attackers try to manipulate the databases. Jurisdictions that use electronic registration lists to check the eligibility of voters for in-person voting during voting periods should have printed copies of registration lists as back-ups as well.[126] States and localities should guard against insider threats by requiring all staff with access to voting machines to undergo background checks.[127]

Also, all states should conduct "parallel testing" during voting periods. Although "parallel testing" would not inform election officials that machines had been hacked until the voting period ended, this is still the best testing mechanism to determine whether machines have been hacked. Congressional legislation to mandate paper trails[128] would alleviate the concern that "parallel testing" does not alert officials to an attack until after the voting period ends because election officials would have a paper record of voters' selections to use in conducting a manual recount. In addition, states that allow military and overseas voters to return ballots electronically should quarantine any ballot received over the Internet, especially those received through emails, such that these ballots are never opened on the same networks that connect to any part of election systems. Election officials should operate under the assumption that

[126] Appel, *supra* note 93.

[127] *Ten Things Election Officials Can Do to Help Secure and Inspire Confidence in This Fall's Elections*, ELECTION VERIFICATION NETWORK 2 (Sept. 9, 2016), https://electionverification.org/wp-content/uploads/2014/11/EVN-Top-Ten-List.pdf [https://perma.cc/A2HQ-5UJL] (suggesting background checks as a security precaution).

[128] *See* discussion *infra* Section V.B.

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

these ballots contain malware and manually tally these votes.[129]

Further, all states should require post-election audits through legislation and statutorily create robust procedures for these audits.[130] Post-election audits reveal when recounts are necessary because they facilitate the catching of errors that have been made in the vote counting process, whether as the result of malicious attacks, machine malfunctions, or accidental errors.[131] Also, audits deter malicious actors because they create a much greater likelihood that the attackers' efforts to influence election results will be discovered and thwarted.

Finally, states and localities should develop emergency contingency plans that are ready to be put in place in the event that a successful attack does occur and is discovered during or immediately following the voting period. These contingency plans should ensure that precincts have enough provisional ballots to accommodate voters whose names may have been illicitly deleted from registration databases. The plans should also develop procedures for extending voting past the deadline at locations affected by an attack that is discovered during a voting period, and to re-run an election in the worst-case scenario of a debilitating attack. These contingency plans would be prudent resilience mechanisms to ensure that U.S. election systems can quickly recover from an attack and would help to reassure people whose confidence in our democratic system may become shaken as a result of a successful attack.

B. Congressional Reforms

Congress should respond to the cyber intrusions during the 2016 election by enacting legislation to improve the security of election systems across the country. Most importantly, Congress should mandate that all federal election systems allow for a paper trail that is verifiable after the election.[132] In effect, this requirement would mean that DRE systems that do not produce a paper trail could not be used in federal elections. Optical scan paper ballot systems and DRE with VVPAT systems could still be used following this regulation. Paper

---

[129] Karen H. Flynn & Pamela Smith, *Commentary: Why Voting Systems Must be as Secure as the U.S. Power Grid*, REUTERS (Aug. 17, 2016, 10:41 PM), http://www.reuters.com/article/us-security-internet-voting-commentary-idUSKCN10S08G [https://perma.cc/C33N-WAE4] (recommending that election officials count ballots returned over the Internet manually because of the risk that they contain malware that could infect an entire election system).

[130] Currently thirty-two states and the District of Columbia conduct post-election audits. *Post-Election Audits*, NAT'L CONF. OF ST. LEGISLATORS, *supra* note 109.

[131] *Post Election Audits*, VERIFIED VOTING, *supra* note 109.

[132] *See, e.g.*, Zeynep Tufekci, *The Election Won't be Rigged. But it Could be Hacked.*, N.Y. TIMES (Aug. 12, 2016), http://www.nytimes.com/2016/08/14/opinion/campaign-stops/the-election-wont-be-rigged-but-it-could-be-hacked.html?_r=0 (advocating for the use of paper trails).

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

trails are much more resistant to tampering than electronic voting machines and enable robust post-election audits to occur. If hacking did occur, these paper records would allow election officials to use the paper ballots to conduct recounts to ensure that voters' true selections were counted in the election.

Congress should also require that all federal elections are subject to post-election audits. Post-election audits are prudent mechanisms for finding errors in the voting process and deterring malicious actors from attempting to interfere in elections. This requirement should not create a specific federal post-election audit standard, though. Instead, this should be left to the states—who should statutorily create robust audit procedures as called for *supra* in Part V(A)—because states are the ones who best understand the make-up of their own election precincts and state officials are the ones who actually procure voting machines to use in their jurisdictions. Thus, states are better equipped to understand the specific audit procedures that should be put in place to maintain the integrity of elections within their jurisdictions.

Further, Congress should create a better system for military and overseas voters to cast their ballots by instituting international kiosk voting. Military and overseas voters should be able to "go to a nearby embassy, consulate, or military base" to cast their vote rather than having these voters either return their ballots by mail, which is slow and unreliable, or electronically, which makes them vulnerable to attack.[133] Returning ballots by mail or electronically could still be used as a last resort for those military and overseas voters who are unable to get to a nearby embassy, consulate, or military base and the ballots that are returned electronically should be quarantined as described *supra* in Part V(A). This action would better serve military and overseas voters, who deserve to have their rights to vote fully protected, and would reduce the vulnerability in this voting mechanism by drastically decreasing the number of ballots that would be returned electronically.

Finally, Congress must invest in the security of U.S. election systems. Congress needs to allocate funds to states to purchase new voting systems that are more secure and reliable than the ones that are currently in use. This would enable states to fully move away from DRE systems that do not have paper trails—which should be effectively prohibited by legislation mandating that all federal election systems allow for a paper trail that is verifiable after the election—and finally purchase badly needed new machines to alleviate what the PCEA has deemed an "impending crisis . . . from the widespread wearing out of voting machines purchased a decade ago . . . ."[134] Also, this legislation should create grants for developing secure and reliable election systems that use open-source software. Open-source software allows for the code to be publicly

[133] *See Protecting the 2016 Elections*, *supra* note 45, at 52 (advocating for remote kiosk voting for military and overseas voters).

[134] PRESIDENTIAL COMM'N ON ELECTION ADMIN., *supra* note 28.

THIS VERSION MAY CONTAIN INACCURATE OR INCOMPLETE PAGE NUMBERS. PLEASE CONSULT THE PRINT OR ONLINE DATABASE VERSIONS FOR THE PROPER CITATION INFORMATION.

examined, which facilitates the discovery of vulnerabilities.[135] Currently, Los Angeles County, California, and Travis County, Texas, are working to create new election systems using sophisticated encryption and open-source software to ensure that the systems are secure and reliable.[136] Grants would promote these types of innovative improvements to U.S. election systems.

VI. CONCLUSION

Maintaining the integrity of our electoral process is vital to our democracy. U.S. election systems face a variety of credible threats. Voter registration systems are the most vulnerable because these databases are often maintained online, which makes them susceptible to manipulation by illicit actors.[137] Voting systems are also vulnerable to attacks on voting machines, overseas voting that occurs electronically, and the tabulation of votes.[138] The cyber intrusions during the 2016 election should serve as a wake-up call to act now to secure our election systems in a prudent manner. Designating U.S. election systems as critical infrastructure is constitutional and will enable federal agencies involved in elections and cybersecurity to assist states and localities with assessing vulnerabilities, mitigating vulnerabilities, improving resilience, and improving coordination in cybersecurity.[139] Also, states and localities should institute a series of legislative and procedural reforms to improve our election systems' security and develop contingency plans to enhance resilience in the event of a successful attack. Finally, Congress should enact new legislation to improve the security of election systems across the country.

---

[135] Richard Clarke, *Yes, It's Possible to Hack the Election*, BELFER CTR. (Aug. 19, 2016), http://belfercenter.ksg.harvard.edu/publication/26902/yes_its_possible_to_hack_the_election.html [https://perma.cc/39Z5-RCN2].

[136] *See Cybersecurity*, *supra* note 6, at 49 (statement of Lawrence D. Norden, Deputy Dir., Brennan Ctr. For Justice) (describing the current efforts in Los Angeles County, California and Travis County, Texas and calling on Congress to create grants to support these projects).

[137] Nakashima, *supra* note 2.

[138] *Id.*

[139] *See* discussion *supra* Part IV.