EMORY | LAW

Emory Law Journal

Volume 70 | Issue 2

2020

The Elections Clause Obligates Congress to Enact a Federal Plan to Secure U.S. Elections Against Foreign Cyberattacks

Suman Malempati

THE ELECTIONS CLAUSE OBLIGATES CONGRESS TO ENACT A FEDERAL PLAN TO SECURE U.S. ELECTIONS AGAINST FOREIGN CYBERATTACKS

ABSTRACT

While foreign adversaries continue to launch cyberattacks aimed at disrupting elections in the United States, Congress has been reluctant to take action. After Russia interfered in the 2016 election, cybersecurity experts articulated clear measures that must be taken to secure U.S. election systems against foreign interference. Yet the federal government has failed to act. Congress's reticence is based on a misguided notion that greater federal involvement in the conduct of elections unconstitutionally infringes on states' rights. Both state election officials and certain congressional leaders operate under the assumption that federalism principles grant states primacy in conducting federal elections.

This Comment dispels the myth that Congress must defer to states to regulate federal elections. The text of the Elections Clause in Article I, Section 4 of the U.S. Constitution confers to Congress final authority in determining the "Times, Places and Manner" of federal elections. Therefore, the system of administering federal elections is based on decentralization rather than federalism.

The risk of foreign interference in U.S. elections was a precise reason the founders bestowed on Congress ultimate control over federal elections. States and municipalities lack the capacity to effectively combat foreign cyber invasion. This Comment makes the case that Congress has a responsibility to exercise its power under the Elections Clause to create a federal plan to secure voter registration databases and voting mechanisms against cyberattacks in order to protect the integrity of American democracy.

INTRODUCTION

Does federalism prevent Congress from taking action to secure U.S. elections against foreign cyberattacks? Since its founding, the United States has grappled with how to balance the authority of state governments against that of the federal government in managing elections.[1] Article I, Section 4 of the U.S. Constitution, often called the "Elections Clause," grants each state the power to designate the "Times, Places and Manner" of federal elections, but it also states that "Congress *may at any time* by Law make or alter such Regulations."[2] Despite the seemingly sweeping power designated to Congress by the Elections Clause, scholars and the Supreme Court have traditionally viewed the regulation of elections and the voting process through the lens of state sovereignty.[3] Currently, U.S. election infrastructure consists of a heterogeneous array of voter registration procedures, registered voter databases, pollbooks, voting machines, and vote counting mechanisms that vary from state to state.[4] States are also inconsistent in the degree to which they delegate election management to counties and municipalities.[5]

Two hundred and thirty years ago in the Federalist Papers, Alexander Hamilton explained the rationale for embedding Congress's power to regulate elections into the Constitution.[6] Hamilton explained that leaving control of federal elections solely in the hands of state governments could create an existential risk to the nation.[7] With the Elections Clause, the drafters of the Constitution "reserved to the national authority a right to interpose, whenever *extraordinary circumstances* might render that interposition necessary to its safety."[8] Hamilton presciently recognized that the threat of foreign interference

---

[1] Guy-Uriel E. Charles & Luis Fuentes-Rohwer, *State's Rights, Last Rites, and Voting Rights*, 47 CONN. L. REV. 481, 514 (2014) ("This struggle between the states and the national government with respect to the apportionment of powers over elections has waxed and waned throughout American history.").

[2] U.S. CONST. art. I, § 4 (emphasis added).

[3] *See, e.g.*, Shelby Cnty. v. Holder, 570 U.S. 529, 535 (2013) (stating the Voting Rights Act of 1965 which granted federal oversight over the voting laws of certain states was "a drastic departure from the principle of federalism"); Justin Weinstein-Tull, *Election Law Federalism*, 114 MICH. L. REV. 747, 753 (2016) (describing "election law federalism" as consisting of "multiple sovereigns" at the federal, state, and local government levels).

[4] Weinstein-Tull, *supra* note 3, at 754 (listing the differences in voting hours, funding schemes, absentee voting rules, and voter registration, or the "nuts and bolts of the election").

[5] *Id.*

[6] THE FEDERALIST NO. 59 (Alexander Hamilton).

[7] *Id.* ("With so effectual a weapon in [state legislators'] hands as the exclusive power of regulating elections for the national government, a combination of few such men, in a few of the most considerable States, where the temptation will always be the strongest, might accomplish the destruction of the union.").

[8] *Id.* (emphasis added).

in U.S. elections would be such an extraordinary circumstance.[9] He wrote in *Federalist 59* that "a firm union of this country, under an efficient government, will probably be an increasing object of jealousy to more than one nation of Europe; and that enterprises to subvert it will sometimes originate in the intrigues of foreign powers."[10]

In 2016, for the first time in the history of this nation, Hamilton's prediction of foreign interference came true when Russia attempted to interfere with and influence the U.S. presidential election.[11] Along with a campaign of misinformation, Russia directly attacked U.S. election systems.[12] Beginning as early as 2014, the Russian government directed extensive activity against U.S. election infrastructure at the state and local levels.[13] A 2018 report by the Senate Intelligence Committee revealed that Russian operatives attempted to hack into the election systems of each of the fifty states.[14] Russia attacked a point of vulnerability in U.S. election infrastructure—states' supposed primacy in conducting federal elections.[15] According to the Senate Intelligence Report, "[s]tate elections officials, who have primacy in running elections, were not sufficiently warned or prepared to handle an attack from a hostile nation-state actor."[16] Hamilton's interpretation of the Elections Clause suggests that Russian aggression is a clear reason for Congress to exert its constitutional authority to protect U.S. election infrastructure.[17]

Despite the obvious risk that our democracy may be undermined by foreign interference, some members of Congress have expressed reluctance to take a greater role in protecting federal elections.[18] State officials have also pushed back and even rejected federal help in securing their state and local election

---

[9] *Id.*

[10] *Id.*

[11] NAT'L ACAD. OF SCIS., ENG'G & MED., SECURING THE VOTE: PROTECTING AMERICAN DEMOCRACY 13 (2018) [hereinafter NAS REPORT].

[12] *Id.* at 14.

[13] S. SELECT COMM. ON INTEL., S. REP. NO. 116-XX, REPORT ON RUSSIAN ACTIVE MEASURES CAMPAIGNS AND INTERFERENCE IN THE 2016 U.S. ELECTION 3 (2019) (partially redacted) [hereinafter SENATE INTELLIGENCE REPORT].

[14] *Id.* at 12.

[15] *Id.* at 4 ("Russian efforts exploited the seams between federal authorities and capabilities, and protections for the states.").

[16] *Id.*

[17] *See infra* Part III.

[18] *See, e.g.*, Dean Dechiaro, *Election Officials Want Security Money, Flexible Standards*, ROLL CALL (Aug. 15, 2019), https://www.rollcall.com/news/congress/election-officials-want-security-money-flexible-standards (describing Senate Majority Leader Mitch McConnell's reluctance to bring House-passed election security bills up for votes in the Senate).

systems out of concern for maintaining state sovereignty.[19] Although Congress has previously overridden the right of states to conduct elections by passing the Voting Rights Act of 1965 (VRA) under the Fifteenth Amendment, it has yet to invoke its full Elections Clause powers.[20] With its holding in *Shelby County v. Holder* in 2013, the Supreme Court gutted the VRA, tilting the balance toward state autonomy in conducting elections.[21] Therefore, Congress can no longer rely solely on its power to enforce the Reconstruction Amendments to supersede state authority over elections.[22]

This Comment argues that the threat of foreign attacks against U.S. election infrastructure requires Congress to exercise its power under the Elections Clause to enact legislation establishing a uniform system for federal elections.[23] This Comment takes the position that foreign cyber intrusion is the type of existential threat for which the Elections Clause gives Congress the authority to act. Because the Constitution grants Congress the ultimate authority to regulate federal elections, the creation of a federal system for elections does not intrude on state sovereignty.

Part I describes the current cybersecurity threat to U.S. election infrastructure. A paucity of federal regulations poses significant risks in the face of such twenty-first century threats. This Part describes the scope of Russia's attacks on state and local election systems during the 2016 election and catalogs the recommendations of cybersecurity experts in how best to secure election infrastructure against future attacks. By detailing how state and local election officials responded ineffectively to cyberattacks in 2016 and leading up to the 2018 election, this Comment predicts that without a comprehensive federal plan, Russia and other foreign actors may successfully disrupt future federal elections.

---

[19] *See infra* Part III.B.

[20] Voting Rights Act of 1965, 52 U.S.C. § 10301; *see* South Carolina v. Katzenbach, 303 U.S. 301, 308 (1966) (upholding the invalidation of state laws restricting voter access to the polls as an appropriate means for carrying out Congress's constitutional responsibilities under the Fifteenth Amendment).

[21] 570 U.S. 529, 557 (2013).

[22] The Thirteenth, Fourteenth, and Fifteenth Amendments to the U.S. Constitution are often called the "Reconstruction Amendments." The Thirteenth Amendment prohibited slavery. U.S. CONST. amend. XIII. The Fourteenth Amendment established birthright citizenship and created due process and equal protection rights against state action. U.S. CONST. amend. XIV. The Fifteenth Amendment guaranteed the right to vote regardless of color or condition of previous servitude. U.S. CONST. amend. XV.

[23] This Comment does not address one aspect of Russia's interference in the 2016 election—a social media campaign of disinformation aimed at influencing voters. For a summary of that issue and recommendations for confronting Russia's efforts, see Alex Stamos, Sergey Sanovich, Andrew Grotto & Allison Berke, *Combatting State-Sponsored Disinformation Campaigns from State-aligned Actors*, *in* SECURING AMERICAN ELECTIONS: PRESCRIPTIONS FOR ENHANCING THE INTEGRITY AND INDEPENDENCE OF THE 2020 U.S. PRESIDENTIAL ELECTION AND BEYOND 43 (Michael McFaul ed., 2019).

Next, Part II explores the history of the Supreme Court's interpretation of constitutional provisions that confer differential authority to states and the federal government to regulate federal elections. This Part describes how the Court's recognition of congressional authority to control federal elections has waxed and waned over the past 150 years. The Court has previously granted relatively broad powers to Congress to invalidate state legislation that infringed on citizens' right to vote under the enforcement provisions of the Fourteenth and Fifteenth Amendments.[24] The expansion of congressional authority under the Reconstruction Amendments was followed by a reversion to greater state sovereignty over elections with the Court's holding in *Shelby County*.[25] This Part explains that *Shelby County* represents a shift in the Court's view towards greater state autonomy in conducting elections. Therefore, Congress must find another source of authority to enact federal election legislation. Part II argues that such authority can be found in the Elections Clause, which provides an underrecognized source of power for Congress to regulate federal elections. Despite the Supreme Court's reluctance to infringe on states' purported sovereignty in conducting elections, the Elections Clause gives Congress the power to supersede any state action regarding elections. The text and purpose of the Elections Clause provide a system for U.S. elections based on decentralization rather than federalism.

Part III contends that, for three main reasons, Congress has an obligation to use its Election Clause authority to enact a federal election plan. First, foreign attacks on U.S. election infrastructure fall within the category of "extraordinary circumstances" as described by Hamilton, which provides the impetus for Congress to regulate the "Times, Places and Manner" of federal elections.[26] Cyber invasion by Russia and potentially other nation-states is a matter of national security that requires a federal response. Second, state and local officials lacked the capacity to manage the attacks during the 2016 U.S. election. Cyberattacks will continue to intensify without a coordinated national response, and states cannot be left to defend election infrastructure from such attacks. Third, insecure voting systems in several states violate the rights of voters under the Fourteenth Amendment by preventing voters from confidently knowing that their votes will count.[27] Therefore, despite the Supreme Court's holding in *Shelby County*, Congress also has a responsibility to step in where states have

---

[24] U.S. CONST. amend. XIV, § 5; U.S. CONST. amend. XV, § 2.

[25] *Shelby County*, 570 U.S. at 544; Charles & Fuentes-Rohwer, *supra* note 1, at 514–15, 518.

[26] U.S. CONST. Article I, § 4; THE FEDERALIST NO. 59 (Alexander Hamilton).

[27] *See* Curling v. Kemp, 334 F. Supp. 3d 1303, 1328 (N.D. Ga. 2018) ("A wound or reasonably threatened wound to the integrity of a state's election system carries grave consequences beyond the results in any specific election, as it pierces citizens' confidence in the electoral system and the value of voting.").

failed in securing their election systems pursuant to the Fourteenth Amendment's enforcement provision.

Lastly, Part IV provides a prescriptive solution and suggests legislation that Congress may enact. Namely, Congress should enact a federal election plan that provides for federal oversight of uniform procedures and standards that each state must follow while maintaining the decentralized conduct of elections.[28] The plan should include federally mandated standards for maintaining registration databases and electronic pollbooks. The federal plan should also require that all states use the same mechanism to generate voter-verified paper ballots, which are read by federally certified optical scanners. Finally, a federal election plan should mandate that all states submit to federal post-election audits.

I. THE CURRENT CYBERSECURITY THREAT TO U.S. ELECTION INFRASTRUCTURE

Securing U.S. elections and citizens' confidence in the election process is of paramount importance to maintain this nation's republican form of government. After the 2016 presidential election, evidence is clear that foreign powers are capable of interfering with U.S. election systems to, at minimum, erode voter confidence and at worst, suppress voter turnout, manipulate vote tallies, and sway election results.[29] Along with hacking into the Democratic National Committee's servers and launching a disinformation campaign on social media, Russia directly targeted U.S. election infrastructure and continues to do so.[30] Cybersecurity experts are fully aware of the vulnerability of U.S. election systems and have developed clear, consensus recommendations on how best to secure elections against cyberattacks.[31] The onus is now on the federal government to create a national plan that will implement these recommendations.

While decentralization provides some protection from a single crippling attack, it also creates a barrier to generating a cohesive and uniform response to foreign cyberattacks.[32] Although states and municipalities play a critical administrative role in conducting elections, they are generally ill-prepared to

---

[28] *See* NAS REPORT, *supra* note 11, at 16 n.11 (noting decentralization of U.S. elections is one aspect of the current U.S. election system that protects against cyberattacks).

[29] Kim Zetter, *The Crisis of Election Security*, N.Y. TIMES MAG. (Sept. 26, 2018), https://www.nytimes.com/2018/09/26/magazine/election-security-crisis-midterms.html.

[30] *See generally* SENATE INTELLIGENCE REPORT, *supra* note 13; NAS REPORT, *supra* note 11.

[31] *See infra* Part I.B.

[32] Lawrence Norden, *How to Secure Elections for 2020 and Beyond*, BRENNAN CTR. FOR JUST. (Oct. 23, 2019), https://www.brennancenter.org/our-work/research-reports/how-secure-elections-2020-and-beyond.

confront a threat from a foreign nation-state.[33] States and municipalities have demonstrated an inability to handle attacks from a foreign nation-state and have still not taken adequate steps to secure election infrastructure at the local level.[34] Therefore, a foreign threat to U.S. elections requires a uniform federal response, and Congress must pass legislation to preserve the integrity of federal elections.

A. Russian Interference in the 2016 U.S. Election

The 2016 U.S. election presented challenges that states, municipalities, and the nation had not previously faced. Russia made a concerted to effort to interfere with and disrupt many aspects of the election.[35] One line of attack was to launch cyberattacks against electronic components of state election systems.[36] Actors sponsored by the Russian government "obtained and maintained access to multiple U.S. state or local electoral boards."[37] Although the Senate Intelligence Committee found no evidence that vote tallies were changed or that voter registration records were altered, the committee's insight is limited in this regard because a full forensic analysis has not been done.[38] What is certain is that Russian government-affiliated actors "conducted an unprecedented level of activity" that targeted state election systems leading up to the 2016 election.[39]

Russian hacking into U.S. election infrastructure was a "watershed moment" in the history of U.S. elections.[40] Protecting election infrastructure became a national security issue when Russia targeted cyberattacks against U.S. voter databases and election systems.[41] The Intelligence Community first detected evidence of hacking into state election systems in the summer of 2016.[42] In July

---

[33] *Id.* ("[I]t is not reasonable to expect each of these state and local election officials to independently defend against hostile nation-state actors.") (statement of Bob Brehm, co-executive director of the New York State Board of Elections) (internal quotation marks omitted); *see infra* Part III.B.

[34] *See infra* Part III.B.

[35] SENATE INTELLIGENCE REPORT, *supra* note 13, at 3.

[36] NAS REPORT, *supra* note 11, at 1.

[37] *Id.* (quoting OFF. OF THE DIR. OF NAT'L INTEL., ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS iii (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.)

[38] NAS REPORT, *supra* note 11, at 2 n.3. The NAS committee was not aware of any ongoing investigation into the possibility that vote tallies were changed. Deficiencies in "intelligence gathering, information sharing, and reporting" leave some uncertainty about the exact consequences of Russia's attacks. *Id.*; SENATE INTELLIGENCE REPORT, *supra* note 13, at 5; Zetter, *supra* note 29.

[39] SENATE INTELLIGENCE REPORT, *supra* note 13, at 5.

[40] NAS REPORT, *supra* note 11, at xii.

[41] *Id.* at 117.

[42] SENATE INTELLIGENCE REPORT, *supra* note 13, at 6. The U.S. Intelligence Community consists of sixteen agencies working under the coordination of the Office of the Director of National Intelligence. The sixteen agencies are: Central Intelligence Agency, Defense Intelligence Agency, Federal Bureau of Investigation, National Geospatial-Intelligence Agency, National Reconnaissance Office, National Security

2016, Illinois noticed unusual activity on the state's Board of Elections voter registry website.[43] An FBI investigation discovered that the activity resulted in data being exfiltrated from the voter registration database.[44] Ultimately, the FBI determined that Russian actors successfully penetrated Illinois's voter registration database, viewed multiple database tables, and eventually accessed up to 200,000 voter registration records.[45] Russian cyber actors were in a position to delete or change voter data, although there is no evidence that they did so.[46]

Further, evidence shows that Russian operatives targeted several small jurisdictions around the country. In the summer of 2016, General Staff of the Russian Army (GRU) officers sought "access to state and local election computer networks by exploiting known software vulnerabilities" on state and local government websites.[47] By mid-August 2016, federal cybersecurity personnel became confident that Russian cyber actors were probing the election infrastructures and voter registration databases of several states.[48] By late September of that year, U.S. intelligence agencies identified twenty-one states that were targeted by Russian government cyber actors.[49] Eventually, intelligence officials concluded that Russia had attempted to invade the election systems of all fifty states.[50]

In one line of attack, GRU officers sent spear-phishing emails to over 120 Florida county election officials.[51] The emails contained an attached Word document carrying a virus that would permit the GRU to access an infected computer.[52] The FBI believes, through this operation, the GRU was able to gain access to the network of at least one county government in Florida.[53] Eventually,

---

Agency/Central Security Service, U.S. Department of Energy, U.S. Department of Homeland Security, U.S. Department of State, U.S. Department of the Treasury, Drug Enforcement Administration, U.S. Air Force, U.S. Army, U.S. Coast Guard, U.S. Marine Corps, and U.S. Navy. NAS REPORT, *supra* note 11, at 1 n.2. Russian activity began as early as 2014. SENATE INTELLIGENCE REPORT, *supra* note 13, at 3.

43 SENATE INTELLIGENCE REPORT, *supra* note 13, at 6.

44 *Id.*

45 *Id.* at 22.

46 *Id.*

47 Michael McFaul & Bronte Kass, *Understanding Putin's Intentions and Actions in the 2016 U.S. Presidential Election*, *in* SECURING AMERICAN ELECTIONS, *supra* note 23, at 5, 14.

48 SENATE INTELLIGENCE REPORT, *supra* note 13, at 7.

49 *Id.*

50 *Id.* at 12.

51 Herbert Lin, Alex Stamos, Nate Persily & Andrew Grotto, *Increasing the Security of U.S. Election Infrastructure*, *in* SECURING AMERICAN ELECTIONS, *supra* note 23, at 17, 18.

52 ROBERT S. MUELLER, III, U.S. DEP'T OF JUST., REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 51 (2019).

53 *Id.*

a Russian operative was indicted by Special Counsel Robert Mueller for probing election websites of certain rural counties in Georgia, Florida, and Iowa in October 2016.[54]

Russia also targeted electronic pollbook systems in several states.[55] In one example of an attack on Election Day in 2016, registered voters in North Carolina were denied the right to vote when the local electronic pollbook systems could not locate their records.[56] Although hacking was never proven to be the cause of the electronic pollbook discrepancy, a forensic analysis was not conducted as county election officials in North Carolina declined the FBI's offer to investigate.[57]

The Intelligence Community understood the seriousness of the foreign attacks.[58] In October 2016, the Department of Homeland Security (DHS) and the Office of the Director on National Intelligence issued a joint statement on election security, which revealed that the probing of state election systems had originated from "servers operated by a Russian company."[59] The statement also warned state and local governments about the cybersecurity threats and asked them to seek assistance from DHS.[60] In January 2017, then-DHS Secretary Jeh Johnson issued a statement designating U.S. election infrastructure as a part of the nation's critical infrastructure, which made election systems an ongoing "priority for cybersecurity assistance and protections" from DHS.[61] Members of the Intelligence Community generally agreed that some of Russia's motives for the cyberattack were to sow discord and undermine voters' confidence in the

---

[54] Indictment at 26, U.S. v. Netyksho, No. 18-cr-00215 (D.D.C. Jul. 13, 2018).

[55] Benjamin Wofford, *The Hacking Threat to the Midterms Is Huge. And Technology Won't Protect Us*, VOX (Oct. 25, 2018, 5:00 AM), https://www.vox.com/2018/10/25/18001684/2018-midterms-hacked-russia-election-security-voting.

[56] *Id.* Electronic pollbooks are electronic voter check-in databases that are increasingly being used in place of paper voter rolls in precincts around the U.S. *See infra* Part I.B.

[57] Wofford, *supra* note 55.

[58] SENATE INTELLIGENCE REPORT, *supra* note 13, at 7–8.

[59] Press Release, DHS & ODNI Election Sec., Joint Statement on Election Security (Oct. 7, 2016), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2016/item/1635-joint-dhs-and-odni-election-security ("We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.").

[60] *Id.*

[61] Press Release, Jeh Johnson, DHS Sec'y, Statement 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. Election infrastructure is comprised of "storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments." *Id.*

U.S. election system.[62] However, intelligence officials believed that the general public did not fully comprehend the threat and had a dim understanding of the vastness of Russia's attack during the 2016 election.[63]

The attacks did not subside after the 2016 election. Russia continued to attack U.S. election infrastructure for the purpose of interfering with the 2018 midterm elections.[64] The Intelligence Community was clearly aware of the ongoing threat from Russia.[65] As one U.S. cybersecurity expert noted before the 2018 midterm elections, "The Russians will attempt, with cyberattacks and with information operations, to go after us again. They're doing it right now."[66] An October 11, 2018, DHS Report stated, "We judge that numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election. We are aware of a growing volume of malicious activity targeting election infrastructure in 2018[.]"[67] There is now abundant evidence that Russia targeted the campaigns of at least a dozen House and Senate candidates in the 2018 midterm elections.[68] The Intelligence Community also believes that Russia continued its activity against state and local election systems.[69] The extent to which Russia succeeded in its endeavors in 2018 is still not known.[70]

Russia has demonstrated it has sufficient sophistication and knowledge of U.S. voting patterns to understand that cyberattacks on local election systems could cause significant disruption.[71] Although it may be difficult to change vote tallies across the country in national elections, cyber actors can access databases in particular districts, manipulate voter files, and cause enough voter suppression to impact the outcome.[72] Therefore, an attack on a few key battleground states

---

62 SENATE INTELLIGENCE REPORT, *supra* note 13, at 35–36.

63 Wofford, *supra* note 55.

64 *Id.*

65 *Id.*

66 *Id.* (quoting Eric Rosenbach, former Pentagon Chief of Staff).

67 SENATE INTELLIGENCE REPORT, *supra* note 13, at 21.

68 Wofford, *supra* note 55.

69 *See* SENATE INTELLIGENCE REPORT, *supra* note 13, at 10 (stating that prior to the 2018 midterm election, DHS determined "numerous actors are regularly targeting election infrastructure, likely for different purposes, including to cause disruptive effects, steal sensitive data, and undermine confidence in the election").

70 *See* Lin et al., *supra* note 51, at 18–19 ("[T]here is no evidence that votes were actually changed and that no lasting damage was done to voter registration databases. Nonetheless, these incidents should be viewed as precursors or dress rehearsals for similar attacks against the 2020 U.S. presidential election.").

71 Eric Manpearl, *Securing U.S. Election Systems: Designating U.S. Election Systems as Critical Infrastructure and Instituting Election Security Reforms*, 24 B.U. J. SCI. & TECH. L. 168, 175 (2018).

72 *Id.* at 173–74; Zetter, *supra* note 29.

during a presidential race could swing the election.[73] Because small manipulations are easier to perpetrate without detection, the risk that cyberattacks may affect the result of an election is "greatest when the electorate is evenly divided and vote counts are close, as has been the case recently in a number of Presidential elections."[74] Attacks on specific competitive districts during congressional elections could also substantially change the composition of the federal legislature.[75] No proof exists that such attacks have occurred, but they are certainly a risk for the future.[76] The consensus opinion among the Intelligence Community is that the threat of foreign cyberattacks on U.S. election systems persists.[77] And the risk is not just from Russia. Evidence shows that China, Iran, North Korea, and ISIS have all conducted cyber intrusions against U.S. election infrastructure.[78]

B. Recommendations of Cybersecurity Experts to Strengthen U.S. Election Infrastructure

Election cybersecurity experts generally agree that certain remedies would create a more secure U.S. election system. Because of long-standing concerns about insecure voting systems and the recent recognition of foreign cyberattacks, the National Academy of Sciences, Engineering, and Medicine ("NAS") appointed an ad hoc committee to consider the future of voting in the United States.[79] The NAS committee determined that, due to the events of the 2016 election and the ongoing threat of cyberattacks, the current U.S. system of voting must evolve.[80] In its report, the NAS committee noted that because of the new

---

[73] Manpearl, *supra* note 71, at 175; NAS REPORT, *supra* note 11, at 16 n.11; *see* Zetter, *supra* note 29 (describing how a few thousand missing votes and a 537-vote victory for George W. Bush in Florida determined the result of the 2000 presidential election).

[74] Lin et al., *supra* note 51, at 19.

[75] Manpearl, *supra* note 71, at 175; NAS REPORT, *supra* note 11, at 16 n.11.

[76] Zetter, *supra* note 29.

[77] SENATE INTELLIGENCE REPORT, *supra* note 13, at 43 (quoting *Russian Interference in the 2016 U.S. Elections: Open Hearing Before the S. Comm. on Intelligence*, 115th Cong. 117 (2017) (statement of Alex Halderman, Professor of Computer Science and Engineering, University of Michigan)); *see* Jeremy Herb, Brian Fung, Jennifer Hansler & Zachary Cohen, *Russian Hackers Targeting State and Local Governments Have Stolen Data, US Officials Say*, CNN, https://www.cnn.com/2020/10/22/politics/russian-hackers-election-data/index.html (Oct. 23, 2020, 11:39 AM) (reporting that "Russian state-sponsored hackers" targeted state and local government and stole voter registration information in the weeks leading up to the 2020 election).

[78] William Roberts, *Election Security: The Fight to Secure the Vote*, 33 WASH. LAW. 12, 14 (2018).

[79] The committee was charged with: (1) documenting the current state of technology, standards, and resources for voting technologies; (2) examining the challenges arising out of the 2016 federal election; (3) evaluating advances in current and upcoming technology that can improve voting; and, (4) providing recommendations to make voting "easier, accessible, reliable, and verifiable." NAS REPORT, *supra* note 11, at 3–4.

[80] *Id.* at 121.

foreign threat, "[w]e must think strategically and creatively about the administration of U.S. elections" and must "seriously reexamine . . . the role of federal and state governments in securing our elections."[81] While cybersecurity experts are not in a position to opine on the constitutionality of federal authority to regulate states in conducting federal elections, they have a strong, coherent, consensus opinion on how best to secure election infrastructure against cybersecurity threats. Experts recommend measures to secure two critical aspects of elections: voter registration databases and vote-casting mechanisms.[82]

First, voter registration lists must be complete and accurate.[83] The Help America Vote Act of 2002 (HAVA) required each state to create a statewide voter database, rather than leave the maintenance of voter registration to counties and municipalities.[84] The administration of voter registration databases requires two main large scale tasks.[85] Election administrators must (1) maintain the correct status and relevant information of citizens who are properly registered to vote; and (2) deliver precinct-specific lists of registered voters to each precinct.[86]

Because of the complexity and flexibility needed to maintain accurate, up-to-date lists of registered voters, lists are by necessity kept electronically.[87] Electronic voter registration databases are easier than paper counterparts to manage and maintain but are vulnerable to cyberattacks.[88] And in many states, "databases containing voter registration lists are connected, directly or indirectly, to the Internet or to state computer networks."[89] This connectivity creates a significant risk of cyber invasion and manipulation.[90] Manipulation of voter registration data would cause chaos when voters arrive at the polls and find their names have been removed from the rolls.[91] Removing or changing data for a small number of voters in contentious congressional races or in swing states

---

81 *Id.*

82 Lin et al., *supra* note 51, at 17.

83 NAS REPORT, supra note 11, at 59.

84 Help America Vote Act of 2002, Pub. L. No. 107-252, 116 Stat. 1666 (codified as amended at 42 U.S.C. §§ 15301–15545) (requiring "a single, uniform, official, centralized, interactive, computerized statewide voter registration list defined, maintained, and administered at the state level").

85 Lin et al., *supra* note 51, at 17.

86 *Id.*

87 NAS REPORT, *supra* note 11, at 57–61.

88 *Id.* at 61.

89 *Id.* at 57.

90 *See infra* Part I.C. Russia breached online voter databases in Illinois and Arizona, obtaining personal information on tens of thousands of registered voters. SENATE INTELLIGENCE REPORT, *supra* note 13, at 22–24; NAS REPORT, *supra* note 11, at 25.

91 SENATE INTELLIGENCE REPORT, *supra* note 13, at 2.

for a presidential race could change the results of an election.[92] The NAS recommends that election administrators routinely assess the integrity of voter registration databases and put in place systems that detect evidence of probing or tampering with the system.[93] The Senate Intelligence Committee recommends updating software in state voter registration systems and maintaining paper backup copies of registration databases.[94]

Managing statewide voter registration databases requires states to deliver precinct-specific lists, also known as pollbooks, to each precinct.[95] Pollbooks, which can either be paper-based or electronic, are used to verify voter eligibility and check-in voters.[96] Over 80% of jurisdictions use preprinted paper pollbooks to check-in voters, but the use of electronic pollbooks (e-pollbooks) is increasing.[97] Between 2012 and 2016, there was a 75% increase in use of e-pollbooks, and now almost half of voters are checked in electronically.[98]

E-pollbooks, which may or may not be networked or connected to the internet, provide some advantages over paper pollbooks. E-pollbooks generally speed up the check-in process and can better track which voters have already cast ballots.[99] When networked, e-pollbooks allow polling places to send and receive real-time updates to voter registration data, which is critical for states that use same-day registration.[100] However, e-pollbooks are vulnerable to cyberattacks that could change voter data, disrupt check-in procedures, and manipulate information on who has and has not voted.[101] Alternatively, a "denial of service" attack could simply shut down operation of an e-pollbook, which would altogether disrupt voting at a particular precinct.[102]

Currently no national security standards exist for e-pollbooks, and security practices vary by state.[103] The NAS recommends jurisdictions that use e-pollbooks have paper backup lists available to be used in the event of any

---

92 Manpearl, *supra* note 71, at 175.

93 NAS REPORT, *supra* note 11, at 63.

94 SENATE INTELLIGENCE REPORT, *supra* note 13, at 57 (noting that one state's voter registration system is more than ten years old).

95 NAS REPORT, *supra* note 11, at 69.

96 *Id.* at 69–70.

97 *Id.* at 70.

98 *Id.*

99 *Id.*

100 *Id.* at 71.

101 *Id.*

102 *Id.* at 72.

103 *Id.* at 71.

disruption or compromise to the electronic version.[104] The NAS also recommends that Congress provide funds for the U.S. Election Assistance Commission to develop national security standards for the use of e-pollbooks.[105]

Second, cybersecurity experts generally agree that cybersecurity risks are inherent when states rely entirely on computers for voters to cast ballots.[106] Currently, jurisdictions use a variety of types of ballots, including paper, card, and machine-only, and votes are cast by a variety of mechanisms.[107] In the majority of jurisdictions, voters mark their choices on paper ballots, either by hand or by using a ballot-marking device (BMD).[108] Paper ballots are either hand-counted or machine-counted, most commonly by optical scanners.[109]

Several states use direct recording electronic (DRE) voting machines in at least some jurisdictions.[110] DREs are free-standing computer units that record selections voters make using a touchscreen.[111]

States purchased DREs with funding from HAVA, which was passed as a response to the problems with lever machines and punch card ballots in the 2000 presidential election.[112] The advent of DREs introduced "new technical challenges," such as touchscreen miscalibration, which causes a voter's intended selection of one candidate to be misinterpreted as a vote for another candidate.[113] Almost immediately, several security risks with DREs were identified, leading some states to decertify and stop using the machines as early as 2007.[114]

Cybersecurity experts now recognize the full extent of the cybersecurity risks with DREs. In its report on election security, the NAS noted that because they are completely paperless, DREs create a risk that a cyberattack on the

---

104 *Id.* at 72.

105 *Id.*

106 *Id.* at 78.

107 *Id.* at 37, 39.

108 When voting with a BMD, a voter uses a touchscreen or keypad to mark his or her choices, after which the BMD prints a paper copy of the selections. The paper printout is human-readable. The paper is then scanned and tabulated by a separate device. With some BMD printouts, an optical scanner records and tallies the human-readable ballot. With other BMDs, the actual selections are recorded on a barcode, which is then read by the tabulating machine. *Id.* at 39.

109 *Id.* at 80.

110 Lawrence Norden & Andrea Cordova, *Voting Machines at Risk: Where We Stand Today*, BRENNAN CTR. FOR JUST. (Mar. 5, 2019), https://www.brennancenter.org/our-work/research-reports/voting-machines-risk-where-we-stand-today.

111 NAS REPORT, *supra* note 11, at 78.

112 Zetter, *supra* note 29.

113 NAS REPORT, *supra* note 11, at 78.

114 Zetter, *supra* note 29.

machines will be undetectable.[115] A computer virus could steal votes from one candidate and assign them to another or could stop a machine from accepting votes altogether.[116] According to the Senate Intelligence Report, DRE voting machines "can be programmed to show one result to the voter while recording a different result in the tabulation."[117] Therefore, the report called for states to discontinue using DREs, which "are now out of date."[118] A cybersecurity expert actually demonstrated in a courtroom how a DRE machine could be infected with malware that could alter vote counts on the machine.[119] The same expert showed that malware could be introduced remotely and be spread from machine to machine.[120]

The Senate Intelligence Report concluded that "[p]aper ballots and optical scanners are the least vulnerable to cyberattack."[121] Secure voting systems must allow a voter to verify that the recorded ballot reflects his or her intent, which is not possible with paperless DRE machines.[122] Therefore, the NAS recommends that "[w]ell designed, voter-marked paper ballots" be the standard way for voters to cast their votes.[123] The consensus opinion from national cybersecurity experts is that an independent record of the voter's physical ballot is essential as a reliable audit tool.[124] An auditable record can be achieved by using hand-marked paper ballots.[125] When voting machines are used to mark ballots, the machine must provide a physical, human-readable record of the voter's selections.[126]

National security experts also agree that the threat of foreign interference in U.S. elections persists.[127] In his testimony before Senate Intelligence Committee, former Assistant Attorney General for National Security John Carlin stated,

> I'm very concerned about . . . our actual voting apparatus, and the attendant structures around it . . . . We've literally seen it already, so

---

115 NAS REPORT, *supra* note 11, at 78.

116 SENATE INTELLIGENCE REPORT, *supra* note 13, at 42.

117 *Id.*

118 *Id.* at 59; *see also* Zetter, *supra* note 29 (noting that as early as 2007, some states have decertified electronic voting machines after finding them to be susceptible to viruses and malicious software).

119 Curling v. Kemp, 334 F. Supp. 3d 1303, 1308 (N.D. Ga. 2018).

120 *Id.* at 1309. Accordingly, a federal judge in Georgia ordered a permanent injunction against the use of DRE machines in the state after 2019. *See infra* Part III.C.

121 SENATE INTELLIGENCE REPORT, *supra* note 13, at 59.

122 NAS REPORT, *supra* note 11, at 79.

123 *Id.*

124 *Id.* at 79–80.

125 *Id.* at 42.

126 *Id.* at 78.

127 SENATE INTELLIGENCE REPORT, *supra* note 13, at 43.

> shame on us if we can't fix it heading into the next election cycles. And it's the assessment of every key intel professional, which I share, that Russia's going to do it again because they think it was successful. So we're in a bit of a race against time heading up to the two-year election. Some of the election machinery that's in place should not be.[128]

Consequently, "[g]iven Russian intentions to undermine the credibility of the election process, states should take urgent steps to replace outdated and vulnerable voting systems."[129]

C. States Responded Inadequately and Ineffectively to Russian Cyberattacks

In the summer of 2016, after it became clear to the Intelligence Community that foreign actors were attacking state election infrastructure, intelligence officials began the process of reaching out to states to offer cybersecurity support.[130] During a call with state election officials on August 15, 2016, DHS Secretary Jeh Johnson offered to provide help to states by inspecting voting systems for viruses and other signs of cyber invasion.[131] DHS proposed conducting on-site risk and vulnerability assessments as well as remote "cyber hygiene scans" on internet-connected election management systems such as voter registration databases.[132] Several states rejected the offer for help. According to Secretary Johnson, the general response from state officials was "[t]his is our responsibility and there should not be a federal takeover of the election system."[133] Then-Georgia Secretary of State Brian Kemp cited concerns about "federal overreach" and claimed that help from federal intelligence agencies would "subvert the [C]onstitution to achieve the goal of federalizing elections under the guise of security."[134] Similarly, Louisiana Secretary of State Tom Schedler chided Congress for overemphasizing the extent of the risk and stated that election administration should be left to the states because "[t]hat's

---

[128] *Id.* (quoting Interview by Senate Select Comm. on Intel. with John Carlin, Former Assistant Att'y Gen. for Nat'l Sec. (Sept. 25, 2017)).

[129] *Id.* at 58.

[130] *Id.* at 46–47.

[131] *Id.* at 47–48; Aliya Sternstein, *At Least One State Declines Offer for DHS Voting Security*, NEXTGOV (Aug. 25, 2016), https://www.nextgov.com/cybersecurity/2016/08/some-swing-states-decline-dhs-voting-security-offer/131037/.

[132] SENATE INTELLIGENCE REPORT, *supra* note 13, at 52.

[133] *Id.* at 47.

[134] Sternstein, *supra* note 131.

what the Constitution says."[135] Republican legislators also blocked funds for election security in Minnesota and Arizona.[136]

Even more concerning, many states failed to recognize the extent or seriousness of the threat and chose not to heed warnings from the Intelligence Community.[137] Several states also opposed the decision of Secretary Johnson to designate U.S. election systems as critical infrastructure.[138] DHS initially intended to make the designation in August 2016 but held off until January 2017 because of pushback from state election officials.[139] Again rejecting federal support, the National Association of Secretaries of State (NASS) expressed opposition to DHS's critical infrastructure designation, mistakenly citing states' primacy in regulating elections.[140] The NASS stated that DHS "has no authority to interfere with elections, even in the name of national security."[141] Secretary Kemp declared that "[d]esignating voting systems or any other election system as critical infrastructure would be a vast federal overreach."[142]

Despite the dire warnings and offers to help from the Intelligence Community, states did little to respond to the ongoing threat of cyberattacks on election systems. Even after the breaches to databases in Illinois and Arizona were known, states continued to struggle to respond to security risks.[143] States have displayed widely varying degrees of concern about election security and efforts to address the security risks. For the most part, states relied on the same insecure infrastructure to conduct elections in 2018 as they did in 2016, despite the known risks.[144] But the attacks on local elections systems did not subside

---

135 Aliya Sternstein, *9 States Accept DHS's Election Security Support*, NEXTGOV (Sept. 21, 2016), https://www.nextgov.com/cybersecurity/2016/09/9-states-accept-dhss-election-security-support/131741/.

136 Gopal Ratnam, *Democrats Target State Elections with Focus on Election Security*, ROLL CALL (Aug. 22, 2019), https://www.rollcall.com/news/congress/democrats-target-state-elections-focus-election-security.

137 *See infra* Part III.B.

138 Manpearl, *supra* note 71, at 186. The purpose of a critical infrastructure designation is to allow the Federal Government to partner with and provide support to the identified sectors. The designation added U.S. election systems to the other critical infrastructure sectors: 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. Press Release, Off. of the Press Sec'y, Presidential Policy Directive—Critical Infrastructure Security and Resilience (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

139 SENATE INTELLIGENCE REPORT, *supra* note 13, at 48–49.

140 Manpearl, *supra* note 71, at 187.

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

142 Sternstein, *supra* note 131.

143 SENATE INTELLIGENCE REPORT, *supra* note 13, at 39; Norden & Cordova, *supra* note 110.

144 Wofford, *supra* note 55.

after the 2016 election, and states continue to be ill-equipped to handle the attacks.[145]

Georgia, for example, exhibited a grossly inadequate response to the cybersecurity challenges that came to light in the 2016 election. The Georgia Secretary of State's Office left its registration database completely open to hackers with 6.5 million voter records exposed during a six-month period in 2016–17.[146] U.S. cybersecurity experts were able to access the database and even plant files during that time.[147] Malicious actors could have manipulated the data, including dropping voters from the database or changing their data.[148] But Georgia election officials claimed they saw no evidence that any election related data was compromised.[149] However, a forensic evaluation was not done initially because Georgia officials wiped the server that housed the data after the breach was discovered.[150] Evidence from an FBI image taken of the server before it was wiped shows that there may have been signs of tampering.[151]

Georgia also knew of the substantial evidence that Russia was targeting election systems and that its paperless, internet-connected voting system was ripe for hacking.[152] Yet, it made no significant changes, and in the 2018 federal election, voters cast ballots on the same outdated, insecure system used in 2016.[153] Georgia election officials were reluctant to acknowledge the full extent of the vulnerability of Georgia's electronic voting equipment even though security flaws in DRE machines had been known for over a decade and Georgia had not updated the software on its machines since 2005.[154] Therefore, Georgia voters used the same hackable and non-auditable voting machines in the 2018

---

145 *Id.*

146 NAS REPORT, *supra* note 11, at 58.

147 Frank Bajak, *Georgia Election Server Wiped After Suit Filed*, PBS NEWSHOUR (Oct. 26, 2017, 9:34 AM), https://www.pbs.org/newshour/politics/georgia-election-server-wiped-after-suit-filed.

148 NAS REPORT, *supra* note 11, at 57.

149 Frank Bajak, *Georgia Election Server Showed Signs of Tampering*, AP (Jan. 16, 2020), https://apnews.com/39dad9d39a7533efe06e0774615a6d05.

150 Kim Zetter, *Georgia Election Systems Could Have Been Hacked Before 2016 Vote*, POLITICO (Jan. 16, 2020, 11:07 PM), https://www.politico.com/news/2020/01/16/georgia-election-systems-could-have-been-hacked-before-2016-vote-100334.

151 *Id.*

152 *See* Curling v. Kemp, 334 F. Supp. 3d 1303, 1327 (N.D. Ga. 2018) ("[Georgia] stood by for far too long, given the mounting tide of evidence of the inadequacy and security risks of Georgia's DRE voting system and software.").

153 *See* Curling v. Raffensperger, 397 F. Supp. 3d 1334, 1382–92 (N.D. Ga. 2019) (summarizing the affidavits of 137 Georgia voters, 2 county pollworkers, and 15 pollwatchers, and concluding that the "same pattern of problems with Georgia's voting systems and registration databases has persisted across multiple elections cycles").

154 *Id.* at 1339, 1348.

midterm elections.[155] As a result, voters in Georgia experienced significant difficulty voting in 2018.[156] Problems reported by voters included long lines due to malfunctioning machines being taken out of service, machines selecting the wrong candidates when voters marked their choices on touchscreens, and check-in problems with e-pollbooks, including incorrect polling places or incorrect addresses listed for voters.[157] A federal court noted that Georgia state election officials had "stood by for far too long" and "buried their heads in the sand" rather than address the inadequacy and insecurity of Georgia's voting system.[158]

Similarly, North Carolina refused an offer from the FBI to investigate election irregularities in 2016.[159] A forensic analysis was never conducted after registered voters could not be located in local e-pollbook systems.[160] Although hacking was never proven as the cause of the e-pollbook discrepancy, it was discovered that Russia targeted e-pollbook systems in several states, including North Carolina.[161] Despite knowing that information, county election officials in North Carolina declined the FBI's offer to investigate.[162]

Given that some states and municipalities have demonstrated they are incapable and, in some instances, even unwilling to secure election infrastructure, the United States needs a national election infrastructure plan. Such a plan should follow the recommendations of national cybersecurity experts to provide uniformity and address vulnerabilities in many state and local election systems.

II. THE LANDSCAPE OF CONGRESSIONAL AUTHORITY OVER FEDERAL ELECTIONS

Many state election officials, scholars, and federal legislators consider primary authority over the conduct of federal elections to belong to the states. For example, the first recommendation in the Senate Intelligence Report on

---

155 *Id.* at 1392; *see* Adam Levin & Beau Friedlander, *Georgia's Shaky Voting System*, N.Y. TIMES (Nov. 13, 2018), https://www.nytimes.com/2018/11/13/opinion/voting-machines-georgia-security.html (describing how Georgia, for its 2018 gubernatorial election, relied on the same voting system it used in 2016 despite the cybersecurity vulnerabilities that had been identified).

156 Mark Niesse, *Long Lines and Equipment Problems Plague Election Day in Georgia*, AJC (Nov. 6, 2018), https://www.ajc.com/news/state—regional-govt—politics/long-lines-and-equipment-problems-plague-election-day-georgia/l7NUidWbMetr5OFdGcb5ZM/.

157 *Curling*, 397 F. Supp. 3d at 1383.

158 *Curling*, 334 F. Supp. 3d at 1327.

159 Wofford, *supra* note 55.

160 *Id.*

161 *Id.*

162 *Id.*

Russian interference in the 2016 election is to "reinforce states' primacy in running elections."[163] The Supreme Court's view on whether the federal government or states have the ultimate right to prescribe the manner in which federal elections are conducted has been unclear. The pendulum of the Court's interpretation of the differential authority between Congress and the states over federal elections has swung back and forth for two centuries. From the antebellum era to the Reconstruction Amendments to the VRA to the Court's decision in *Shelby County*, the Court has expanded and contracted congressional authority relative to state sovereignty. But even this pendulum swing has remained in a somewhat narrow range because Congress has never attempted to exercise the full breadth of its authority under the Elections Clause.

The vast majority of congressional action to regulate elections since the Civil War has been pursuant to the Reconstruction Amendments rather than the Elections Clause.[164] Even when congressional authority was at its peak under the VRA, Congress approached election legislation from a deferential framework. Congress only passed the VRA after the Civil Rights Movement's expansive and concerted fight for voting rights in the South brought national attention and shifted public opinion on this issue.[165] The Supreme Court upheld this action by Congress under the Enforcement Clause of the Fifteenth Amendment because of the long-standing and pernicious evil of racial discrimination in voting.[166] But Congress has yet to exercise and the Court has yet to uphold the full extent of Congress's power to enact federal election legislation under the Elections Clause, which extends beyond anti-discrimination.

A. Congressional Authority Under the Reconstruction Amendments and the Voting Rights Act

The end of the Civil War and the Reconstruction era brought a new paradigm to the balance of federal authority versus state autonomy. The Fourteenth Amendment provided an avenue for Congress to ensure that each state did not abridge or deny certain rights to its own citizens.[167] The Fifteenth Amendment

---

163 SENATE INTELLIGENCE REPORT, *supra* note 13, at 54.

164 Franita Tolson, *The Spectrum of Congressional Authority Over Elections*, 99 B.U. L. REV. 317, 341 (2019).

165 CAROL ANDERSON, ONE PERSON, NO VOTE: HOW VOTER SUPPRESSION IS DESTROYING OUR DEMOCRACY 21–22 (2018); *see* South Carolina v. Katzenbach, 303 U.S. 301, 315 (1966) ("The burden is too heavy—the wrong to citizens is too serious—the damage to our national conscience too great not to adopt more effective measures than exist today.").

166 *Id.* at 303–04.

167 U.S. CONST. amend. XIV.

prohibited states from denying the right to vote "on account of race, color, or previous condition of servitude."[168] Despite the Fifteenth Amendment guarantee, many former Confederate states still prevented African American citizens from exercising their new constitutional right to vote.[169] But embedded in the Reconstruction Amendments were enforcement provisions that established a role for Congress to protect the rights of all citizens against state action.[170] The constitutional enfranchisement of African American voters created a new framework for Congress to play a greater role in elections in order to protect the right to vote.

While Congress had the power to enforce the Reconstruction Amendments to prevent states from infringing on their citizens' right to vote, the Reconstruction-era framework preserved a concept of federalism and state sovereignty over the conduct of elections.[171] Congress attempted to exert broad authority to regulate elections through the Enforcement Acts of 1870 and 1871, which instituted a system of federal oversight for congressional elections.[172] However, despite Congress's greater power to protect voters under the Reconstruction Amendments, the Supreme Court did not allow Congress full license to regulate elections. In *United States v. Reese*, the Court struck down provisions of the Enforcement Act of 1870 because they exceeded the scope of Congress's mandate under the Fifteenth Amendment.[173] The Court held that section 4 of the statute was invalid because it created criminal penalties for state officials who denied citizens the right to vote.[174] According to the Court, the Fifteenth Amendment did not confer upon Congress expansive power to regulate elections and protect voters, but simply prevented states from discriminating based on race.[175]

Similarly, the Court restrained Congress from using the Enforcement Act of 1870 to assert broad authority over states pursuant to the Fourteenth Amendment in *United States v. Cruikshank*.[176] In that case, election inspectors in Louisiana were criminally charged with conspiring to prevent two African American

---

168 U.S. CONST. amend. XV, § 1.

169 ANDERSON, *supra* note 165, at 2.

170 U.S. CONST. amend. XIII, § 2; U.S. CONST. amend. XIV, § 5; U.S. CONST. amend. XV, § 2.

171 Tolson, *supra* note 164, at 354.

172 Enforcement Act of 1870, ch. 114, 16 Stat. 140; Enforcement Act of 1871, ch. 99, 16 Stat. 433; Tolson, *supra* note 164, at 358.

173 United States v. Reese, 92 U.S. 214, 220 (1875).

174 *Id.* at 217–18, 220.

175 *Id.* at 217.

176 United States v. Cruikshank, 92 U.S. 542, 555 (1875).

citizens from exercising their right to vote.[177] The Court dismissed the indictments, holding that the Louisiana officials did not intentionally discriminate based on race.[178] Importantly, the Court noted that the federal government had authority to prohibit discrimination under the Fourteenth Amendment, but the right to vote itself came from the states.[179] The Court, however, did not address Congress's power to regulate elections and ensure the right to vote under the Elections Clause.

The post-Reconstruction era, beginning with the federal government's withdrawal of military troops in 1876, allowed Southern states to construct significant structural barriers to African American suffrage.[180] Discriminatory devices to prevent African Americans from voting were enacted into state laws and even embedded into the constitutions of several former Confederate states.[181] In addition to literacy tests, poll taxes, and good-morals requirements, the small percentage of African Americans who were able to cast ballots in the South often had to overcome outright violence.[182]

During the Jim Crow era of renewed disenfranchisement, the Supreme Court invalidated several state laws designed to prevent African Americans from voting as violations of the Fourteenth and Fifteenth Amendment.[183] However, case-by-case litigation was essentially a game of whack-a-mole. Each time federal courts struck down a discriminatory state law that restricted the right of its citizens to vote, states found insidious, creative alternative ways to disenfranchise African American voters.[184] For example, after two Supreme Court decisions invalidated all-white primary elections, states such as South Carolina and Texas found ways to unofficially hold "pre-primaries" without such laws being on their books.[185] The Civil Rights Movement forced Congress

---

177 *Id.* at 544–45.

178 *Id.* at 556–57.

179 *Id.* at 554–56 (holding that the Fourteenth Amendment only confers on Congress the power to ensure that states do not deny the equality of rights of their citizens, but states still assume the primary duty to guarantee these rights: "The power of the national government is limited to the enforcement of this guaranty.").

180 ANDERSON, *supra* note 165, at 2–3.

181 Virginia E. Hench, *The Death of Voting Rights: The Legal Disenfranchisement of Minority Voters*, 48 CASE W. RES. L. REV. 727, 733–43 (1998).

182 ANDERSON, *supra* note 165, at 14–18.

183 *See, e.g.*, Schnell v. Davis, 336 U.S. 933, 933 (1949) (striking down, as a violation of the Equal Protection Clause, a provision of the Alabama state constitution that required citizens to understand and explain an article of the U.S. Constitution in order to exercise the right to vote).

184 ANDERSON, *supra* note 165, at 13.

185 Smith v. Allwright, 321 U.S. 649, 656–57 (1944); ANDERSON, *supra* note 165, at 13.

to enact a comprehensive plan to "banish the blight of racial discrimination in voting."[186]

Nearly a century after the Fourteenth and Fifteenth Amendments were ratified, Congress responded to the grassroots efforts of the Civil Rights Movement by passing the Voting Rights Act of 1965.[187] The VRA prescribed remedies for voting discrimination that it imposed on particular states that were known to have constructed the greatest barriers for African American voters.[188] By exercising its power under the Enforcement Clause of the Fifteenth Amendment, Congress supplanted the right of states to enact particular discriminatory voter qualification laws.[189] The VRA placed significant constraints on states' autonomy in determining voter qualifications.[190] Section 5 of the VRA required states or counties that had a history of discriminating against African American voters, as defined in section 4(b), to submit to preclearance by the U.S. Attorney General of any new law that impacted voter qualifications or registration.[191] The Act also authorized federal examiners to directly place and remove voters from the registration lists of states and localities who fell under the VRA's coverage formula.[192]

When the Supreme Court upheld the VRA as "an appropriate means for carrying out Congress' constitutional responsibility," federal authority to regulate elections under the Reconstruction Amendments was at its zenith.[193] South Carolina challenged the VRA on the grounds it exceeded Congress's powers and infringed on a function that had traditionally been left to states.[194] But the Court dismissed these concerns.[195] The Court held that "[a]s against the reserved powers of the States, Congress may use any rational means to effectuate the constitutional prohibition of racial discrimination in voting."[196] The Court in

---

[186] South Carolina v. Katzenbach, 383 U.S. 301, 308 (1966); ANDERSON, *supra* note 165, at 21–22.

[187] The Voting Rights Act was signed into law by President Lyndon Johnson on August 6, 1965. *See* Voting Rights Act of 1965, Pub. L. No. 89-110, §§ 1–19, 79 Stat. 437 (codified as amended in scattered sections of 52 U.S.C.); *see* Eric S. Lynch, *Trusting the Federalism Process Under Unique Circumstances: United States Election Administration and Cybersecurity*, 60 WM. & MARY L. REV. 1979, 1991–92 (2019) (noting that President Johnson introduced the voting rights bill to Congress three days after the "Bloody Sunday" Selma-to-Montgomery march).

[188] §§ 1–7, 79 Stat. at 437–41.

[189] U.S. CONST. amend. XV, § 2 ("Congress shall have the power to enforce this provision through appropriate legislation."); §§ 1–2, 79 Stat. at 437.

[190] §§ 1–6, 79 Stat. at 437–40.

[191] §§ 4(b)–5, 79 Stat. at 438–39.

[192] § 7, 79 Stat. at 440–41.

[193] South Carolina v. Katzenbach, 303 U.S. 301, 308 (1966).

[194] *Id.* at 323.

[195] *Id.*

[196] *Id.* at 324.

South Carolina v. Katzenbach stated that Congress's authority relative to states' rights under the Enforcement Clause of the Fifteenth Amendment is just as broad as Congress's power under the Necessary and Proper Clause.[197] Therefore, to prevent racial discrimination, the Supreme Court established that Congress had paramount authority to supersede state autonomy in determining who was eligible to cast a ballot.

According to the Court, "[t]he Voting Rights Act was designed by Congress to banish the blight of racial discrimination in voting, which has infected the electoral process."[198] The Court emphasized the "unique circumstances" that permitted Congress to exert such expansive powers to violate state sovereignty under the Fifteenth Amendment.[199] The unique circumstances to which the Court referred were the overt discriminatory actions of several former slave states that violated the Fifteenth Amendment.[200] In *Katzenbach*, the Court's ratification of Congress's power to enact the VRA was specific to the era as well as the manner and degree to which the infringement on the rights of African Americans were being infringed.[201]

Over the next almost fifty years, the Supreme Court continued to uphold the VRA as a legitimate exercise of Congress's power to enforce the Fifteenth Amendment.[202] The Court recognized Congress's authority to invalidate provisions that did not have a stated discriminatory purpose but had a disparate impact on the right of African Americans to vote. In *City of Rome v. United States*, the Court upheld the VRA's ban on changes to a municipality's voting provisions that would have had a discriminatory effect.[203] In that case, the city of Rome, Georgia challenged the VRA on federalism grounds.[204] But the Court made clear that the mandate embedded in the enforcement provisions of the Reconstruction Amendments trumped federalism concerns.[205] The Court stated that "principles of federalism that might otherwise be an obstacle to

---

[197] *Id.* at 325–26; *see Ex parte* Virginia, 100 U.S. 339, 345–46 (1879) ("Whatever Legislation is appropriate, that is, adapted to . . . secure to all persons the enjoyment of perfect equality of civil rights and the equal protection of the laws against State denial or invasion, if not prohibited, *is brought within the domain of congressional power*.") (emphasis added).

[198] *Katzenbach*, 383 U.S. at 308.

[199] *Id.* at 335 ("Under the compulsion of these unique circumstances, Congress responded in a permissibly decisive manner.").

[200] *Id.*

[201] *Id.* at 326–31.

[202] *See, e.g.*, Lopez v. Monterey Cnty., 525 U.S. 266, 287 (1999); City of Rome v. United States, 446 U.S. 156, 173 (1980).

[203] *City of Rome*, 446 U.S. at 173.

[204] *Id.* at 178.

[205] *Id.* at 179.

congressional authority are necessarily overridden by the power to enforce the Civil War Amendments 'by appropriate legislation.'"[206] The Court held that Congress has the power to impose voting regulations on states and their political subdivisions because the "[Reconstruction] Amendments were specifically designed as an expansion of federal power and an intrusion on state sovereignty."[207]

The Supreme Court took its view of federal power over state regulations under the Fifteenth Amendment one step further in *Lopez v. Monterey County*.[208] In that case, Monterey County was subject to the coverage formula under section 4(b) of the VRA, but the State of California as a whole was not.[209] California passed a state law that determined the manner in which county judges were to be elected.[210] Voters alleged that the law was invalid as applied to Monterey County because any changes to existing law that applied to the county had to be precleared by the federal government.[211] The Court determined that the California law could not take effect in Monterey County until it received preclearance pursuant to section 5 of the VRA.[212] Therefore, the Court recognized that Congress's authority to enforce the Reconstruction Amendments includes the power to supersede the rights of states to regulate their own counties. Accordingly, at end of the twentieth century, Congress had broad authority under the Fifteenth Amendment to regulate federal elections through the VRA.

B. The Demise of the Voting Rights Act and the Shifting State-Federal Authority to Regulate Elections

The twenty-first century brought a dramatic shift in the Supreme Court's deference to Congress to enforce the Fifteenth Amendment through the VRA, which culminated in the Court's gutting of the VRA in *Shelby County v. Holder*.[213] Chief Justice John Roberts's general ideology appears to limit congressional power in favor of state sovereignty through principles of federalism.[214] Relying on federalism, the Roberts Court has limited Congress's

---

206 *Id.* (quoting Fitzpatrick v. Bitzer, 427 U.S. 445, 456 (1976)).

207 *Id.* at 179–80.

208 Lopez v. Monterey Cnty., 525 U.S. 266, 287 (1999).

209 *Id.* at 269.

210 *Id.*

211 *Id.* at 271, 274.

212 *Id.* at 287.

213 Shelby Cnty. v. Holder, 570 U.S. 529, 556–57 (2013).

214 Joshua A. Douglas, *(Mis)Trusting States to Run Elections*, 92 WASH. U. L. REV. 553, 580 (2015); *see* Adam B. Cox & Thomas J. Miles, *Judging the Voting Rights Act*, 108 COLUM. L. REV. 1, 3 (2008) (demonstrating

ability to oversee elections and has elevated the role of states in regulating various aspects of the voting process and election conduct.[215] In sharp contrast to the Civil Rights era that led to the VRA, the Court in recent years has more closely scrutinized Congressional regulation of voting and elections while affording more deference to election laws enacted by states.[216]

In 2009, the Court foreshadowed its holding in *Shelby County* by expressing outright hostility to the VRA in *Northwest Austin Municipal Utility District Number One v. Holder*.[217] In that case, a Texas municipal district challenged the VRA's preclearance requirement.[218] The Court avoided the question of the VRA's constitutionality by resolving the district's claims on statutory grounds.[219] In dicta, however, the Court raised concerns about whether the VRA was constitutional.[220] In his majority opinion, Chief Justice Roberts noted that section 5 of the VRA "authorizes federal intrusion into . . . state and local policymaking" and "imposes substantial 'federalism costs.'"[221] The Court also stated that section 5 exceeded Congress's mandate under the Fifteenth Amendment by suspending all changes to election law in the jurisdictions falling under its coverage formula.[222] In the concluding paragraphs of the opinion, which foreshadowed *Shelby County*, the Court claimed that the "exceptional conditions" that justified the VRA no longer exist as "we are now a very different Nation."[223]

Four years later, in *Shelby County*, the Supreme Court struck down section 4(b) of the VRA.[224] Section 4(b) had delineated the "coverage" formula that determined which states and localities were subject to federal preclearance before enacting new voting legislation.[225] In invalidating portions of the VRA, the Court described its rationale as a combination of federalism issues, concerns

---

that judicial ideology impacts judicial decisions regarding voting rights).

215 Douglas, *supra* note 214, at 583.

216 *Id.* at 579; *see* Franita Tolson, *Election Law "Federalism" and the Limits of the Anti-Discrimination Framework*, 59 WM. & MARY L. REV. 2211, 2215 (2018) (arguing that recent case law has limited the extent of Congress's powers under the Fourteenth and Fifteenth Amendments due to federalism concerns and the Supreme Court now views states as having broad authority to regulate federal elections).

217 Nw. Austin Mun. Util. Dist. No. 1 v. Holder, 557 U.S. 193, 203 (2009).

218 *Id.* at 196.

219 *Id.* at 205–06.

220 *Id.* at 204.

221 *Id.* at 202 (quoting Lopez v. Monterey Cnty., 525 U.S. 266, 282 (1999)).

222 *Id.*

223 *Id.* at 211.

224 Shelby Cnty. v. Holder, 570 U.S. 529, 556–57 (2013).

225 Voting Rights Act of 1965, Pub. L. No. 89-110, § 4(b), 79 Stat. 437, 438 (codified as amended in scattered sections of 52 U.S.C.).

about equal sovereignty among states, and changed conditions regarding racial inequality in voting.[226] A concern for state sovereignty predominated Justice Roberts's majority opinion.[227] The Court described the VRA's requirement that certain states obtain federal permission before enacting voting laws as "a drastic departure from basic principles of federalism."[228]

Scholars and interested parties soon discovered that the *Shelby County* decision definitively altered the Court's view of the balance between state and federal government in regulating elections under the Reconstruction Amendments.[229] Prior to *Shelby County*, the Court had generally recognized Congress's authority to supersede state laws regulating elections in order to protect voters' rights.[230] *Shelby County* turned that assumption on its head. Contrary to the prior understanding of the federal-state balance regarding elections, the Court stated that the original intent of the framers was for states to have primary authority to regulate federal elections.[231] The Court in *Shelby County* held that the VRA was only a legitimate exercise of Congress's power when it was enacted because it was the product of a particular time in history.[232]

However, the Court's emphasis in *Shelby County* on federalism and state sovereignty in conducting elections was misguided. The Court viewed the authority to regulate elections solely from an antidiscrimination perspective and, ignoring its *City of Rome* precedent, focused on overt discriminatory intent.[233] By only evaluating Congress's power to protect the rights of minority voters under the Fourteenth and Fifteenth Amendments, the Court discounted Congress's broad powers to contradict state laws and regulate elections under the Elections Clause.

C. The Elections Clause Grants Congress Broad Authority to Regulate Federal Elections

Congress's authority to regulate federal elections under the Elections Clause

---

226 *Shelby County*, 570 U.S. at 534–44, 547.

227 *Id.* at 535 (stating that the VRA infringed on state sovereignty and section 4 violated "the principle that all states enjoy equal sovereignty").

228 *Id.*

229 *See* Charles & Fuentes-Rohwer, *supra* note 1, at 488, 522 (presenting the case against an "optimistic" reading of the *Shelby County* holding for voting rights advocates).

230 *Id.* at 500–01, 516.

231 *Id.* at 517.

232 *Id.* at 495 (noting that Chief Justice Roberts' majority opinion stated that the VRA was only acceptable in 1966 because "exceptional conditions can justify legislative measures not otherwise appropriate" (quoting South Carolina v. Katzenbach, 303 U.S. 301, 334 (1966))).

233 *See Shelby County*, 570 U.S. at 551, 553, 556.

is significantly broader than the Court has acknowledged since *Shelby County*.[234] In *Federalist 59*, Alexander Hamilton explained that the Elections Clause invested ultimate authority to regulate federal elections in "the national legislature."[235] Because of the clear mandate of the Elections Clause, the Supreme Court was remiss in *Shelby County* to overvalue state sovereignty in regard to the conduct of federal elections.[236] The Court mistakenly relied on what it called a "prevailing view that federalism best explains" the U.S. election system.[237]

1. Decentralization Versus Federalism

The Elections Clause precludes viewing the balance of state-versus-federal authority to regulate elections through traditional notions of federalism.[238] The text and history of the Elections Clause demonstrate that the Constitution prescribed a system for federal elections based on decentralization rather than federalism.[239] Though often conflated, "federalism" and "decentralization" are distinct concepts.[240] Decentralization is a hierarchically organized "managerial concept" in which the leader at the top has plenary power over the subordinate units.[241] Federalism may be structurally similar to decentralization.[242] But as a political concept, federalism implies that the subordinate units retain certain rights and "areas of jurisdiction that cannot be invaded by the central authority[.]"[243] In the United States, federalism denotes separate sovereignty and a "system of parallel federal and state governance."[244]

Regarding federal elections, the Elections Clause prescribes a system of decentralization rather than federalism.[245] A traditional notion of federalism does not bar Congress from enacting broad legislation to dictate the manner in

---

234 Tolson, *supra* note 216, at 2217.

235 THE FEDERALIST NO. 59 (Alexander Hamilton).

236 Tolson, *supra* note 216, at 2214.

237 *Id.* at 2216.

238 *Id.* at 2215–18; *see* Tolson, *supra* note 164, at 321–22.

239 U.S. CONST. art. I, § 4; *see* Franita Tolson, *Reinventing Sovereignty?: Federalism as a Constraint on the Voting Rights Act*, 65 VAND. L. REV. 1195, 1247 (2012) ("The organizational structure of the [Elections] Clause itself is not really federalist, but reflects a decentralized organizational structure that is often confused with federalism."); Weinstein-Tull, *supra* note 3, at 790 (noting that some scholars argue that federal election statutes do not implicate federalism, but demonstrate a form of "managerial decentralization").

240 Edward L. Rubin & Malcolm Feeley, *Federalism: Some Notes on a National Neurosis*, 41 UCLA L. REV. 903, 910–11 (1994).

241 *Id.*

242 *Id.* at 911.

243 *Id.*

244 Weinstein-Tull, *supra* note 3, at 775.

245 Tolson, *supra* note 239, at 1202, 1247.

which federal elections will be conducted.[246] In contrast, states have no plenary power to regulate federal elections.[247] States can administer federal elections under direct grant from the Elections Clause but subject to Congress's ultimate authority.[248] Pursuant to the Elections Clause, "the Constitution primarily treats states as election administrators rather than sovereign entities."[249] Therefore, states may only regulate federal elections in a managerial sense.[250] Congress has the final say in how authority is delegated and has generally left states "to fill in . . . the blanks with respect to the nuts and bolts of federal elections[.]"[251]

2. Congress Has Used Its Election Clause Authority to a Limited Degree

In addition to exercising federal authority over elections under the Fifteenth Amendment, Congress has, at times, used its Elections Clause power.[252] Two examples of statutes enacted under the Elections Clause that have been upheld by courts are the National Voter Registration Act of 1993 (NVRA) and the Help America Vote Act of 2002 (HAVA).[253]

Congress enacted the NVRA to increase voter participation in elections by making voter registration easier for all eligible citizens.[254] The NVRA requires states to provide opportunities to register to vote when citizens interact with various state government offices, such as applying for driver's licenses or applying for aid through public assistance and disability services offices.[255] The NVRA also authorizes the federal government to enforce its provisions through civil actions against states.[256]

Federal courts have generally upheld the NVRA as a legitimate exercise of Congress's Elections Clause authority.[257] Despite giving no weight to the

---

246 Tolson, *supra* note 216, at 2216 ("Congress and the courts can disregard state sovereignty in enacting, enforcing, and resolving the constitutionality of legislation passed pursuant to the Elections Clause.").

247 Michael T. Morley, *The Intratextual Independent "Legislature" and the Elections Clause*, 109 NW. U. L. REV. 847, 849 (2015).

248 *Id.*

249 Harkless v. Bruner, 545 F. 3d 445, 454 (6th Cir. 2008).

250 *See* Tolson, *supra* note 239, at 1197.

251 Tolson, *supra* note 216, at 2218.

252 Franita Tolson, *The Elections Clause and Underenforcement of Federal Law*, 129 YALE L.J. F. 171, 173 (2019).

253 *See* Help America Vote Act of 2002, Pub. L. No. 107-252, §§ 101–906, 116 Stat. 1666 (codified as amended at 52 U.S.C. §§ 20901–21145); *see* National Voter Registration Act of 1993, Pub. L. No. 103-31, §§ 1–13, 107 Stat. 77 (codified as amended at 52 U.S.C. §§ 20501–20511).

254 § 2, 107 Stat. at 77.

255 §§ 4–5, 7, 107 Stat. at 78, 80–81.

256 § 11, 107 Stat. at 88.

257 *See* Weinstein-Tull, *supra* note 3, at 762–63, 765.

Elections Clause in *Shelby County*, the Supreme Court recognized Congress's broad power to regulate voter qualification standards under the Elections Clause in *Arizona v. Inter Tribal Council of Arizona, Inc.*[258] In *Inter Tribal Council*, the Court held that the NVRA preempted an Arizona state law.[259] The Court noted that the Elections Clause grants Congress final policymaking authority over many aspects of federal elections.[260] The NVRA required states to accept a national mail registration form developed by the Federal Election Commission.[261] The Court held that the NVRA mandate that states "accept and use" a federal form to register voters superseded Arizona's law that required voters to present proof of citizenship to register to vote.[262]

In some cases, courts have noted that Congress's right to disregard states' autonomy under the Elections Clause is even broader than its powers under the Commerce Clause.[263] For example, "[i]f Congress determines that the voting requirements established by a state do not sufficiently protect the right to vote, it may force the state to alter its regulations."[264] In *ACORN v. Miller*, the Sixth Circuit rejected Michigan's challenge to the NVRA.[265] Michigan argued that "Congress overstepped its power to regulate federal elections by compelling state legislation to effectuate a federal program, directing states to legislate toward a federal purpose, and forcing states to bear the financial burden of enacting a federal scheme."[266] However, the Sixth Circuit held that, unlike the Commerce Clause, the Elections Clause "specifically grants Congress the authority to force states to alter their regulations regarding federal elections."[267]

Congress's power under the Elections Clause extends as far as commandeering state offices and state election officials to carry out federal

---

[258] Arizona v. Inter Tribal Council of Arizona, Inc., 570 U.S. 1, 14–15 (2013).

[259] *Id.* at 14–15, 20.

[260] *Id.* at 8–9.

[261] National Voter Registration Act of 1993, Pub. L. No. 103-31, § 6, 107 Stat. 77, 79–80 (codified as amended at 52 U.S.C. §§ 20501–20511). When HAVA was enacted, this function of the Federal Election Commission transferred to the Election Assistance Commission. *See* Help America Vote Act of 2002, Pub. L. No. 107-252, § 303, 116 Stat. 1666, 1713–14 (codified as amended at 52 U.S.C. §§ 20901–21145).

[262] *Inter Tribal Council*, 570 U.S. at 15.

[263] *See* Harkless v. Bruner, 545 F. 3d 445, 454 (6th Cir. 2008) ("[U]nlike the Commerce Clause . . . Article I section 4 specifically grants Congress the authority to force states to alter their regulations regarding federal elections." (quoting ACORN v. Miller, 129 F.3d 833, 836 (6th Cir. 1997))). Congress's power to prescribe the details that state legislatures must adopt to hold federal elections stands in stark contrast to virtually all other provisions of the Constitution. *Id.*

[264] *ACORN*, 129 F.3d at 837.

[265] *Id.* at 837–38.

[266] *Id.* at 836.

[267] *Id.*

law.[268] For example, the NVRA imposes duties on state officials: each state must designate a particular state election official to be responsible for carrying out state obligations under the Act.[269] States have claimed that the NVRA violates the anticommandeering doctrine because it forces them to enact new legislation to administer a federal program.[270]

The anticommandeering doctrine prohibits the federal government from compelling states to "implement, by legislation or executive action, federal regulatory programs."[271] However, as it relates to commandeering, courts have distinguished the source of congressional power in upholding federal election legislation.[272] The prohibition on commandeering under Congress's Commerce Clause authority does not extend to Congress's authority under the Elections Clause.[273] In contrast to the Commerce Clause, the Elections Clause allows Congress to "conscript state agencies" to administer a federal election scheme.[274] Therefore, under the Elections Clause, Congress may "enact election legislation that forces a state to take action it might not otherwise take, without violating the anticommandeering doctrine."[275] Despite this mandate, Congress has been reluctant to use the full extent of its Elections Clause authority because of "federalism" concerns.[276]

Congress passed HAVA in response to the challenges encountered in the 2000 presidential election.[277] That election was plagued by unreliable voting systems that varied by jurisdiction, culminating in the "hanging chad" debacle in Florida.[278] HAVA provided federal funds for states to update their voting machines while placing several requirements on states.[279] HAVA's mandatory provisions include allowing voters to review and verify votes before casting a

---

268 Tolson, *supra* note 216, at 2220 (noting that Congress's primacy in regulating elections is embodied by "its independent authority to make legislation, alter state law, and commandeer state officials to implement federal law").

269 National Voter Registration Act of 1993, Pub. L. No. 103-31, § 10, 107 Stat. 77, 87 (codified as amended at 52 U.S.C. §§ 20501–20511)

270 Voting Rts. Coal. v. Wilson 60 F.3d 1411, 1415–16 (9th Cir. 1995); *see* ACORN v. Edgar, 56 F.3d 791, 793 (7th Cir. 1995) (describing an argument by the state of Illinois that the NVRA would require it to change its state laws that govern voter registration).

271 Printz v. United States, 521 U.S. 898, 925 (1997).

272 Weinstein-Tull, *supra* note 3, at 782.

273 *Id.*

274 *Voting Rts. Coal.*, 60 F.3d at 1415.

275 Weinstein-Tull, *supra* note 3, at 782.

276 *See infra* Part III.A.

277 Weinstein-Tull, *supra* note 3, at 757.

278 *Id.*

279 Help America Vote Act of 2002, Pub. L. No. 107-252, §§ 102, 301, 303, 116 Stat. 1666, 1670–71, 1704–05, 1708 (codified as amended at 52 U.S.C. §§ 20901–21145).

ballot, making voting accessible to people with disabilities, and centralizing voter registration databases at the state level.[280] But HAVA did not "fully nationalize election administration."[281] Even after HAVA, states and municipalities remain relatively autonomous in conducting elections.[282]

With HAVA, Congress used a carrot as much as a stick to coax states into making voting more secure and accessible.[283] HAVA required states to update voting machines and provided funds for the upgrades, but left states to determine which systems to use.[284] HAVA requires that elections be auditable, but stops short of requiring paper ballots.[285] In March 2018, the U.S. Election Assistance Commission announced that it would provide $380 million in election security grants to states, but it left states with discretion in how to use the funds.[286] Under the Elections Clause, Congress has much more authority than it exercised with HAVA. Congress can create a national plan for elections and force states to comply with and administer the plan.[287]

Thus, unlike the antidiscrimination framework of the Fourteenth and Fifteenth Amendments, Congress is not constrained by federalism when it exerts its authority under the Elections Clause.[288] Courts can and should disregard claims of state sovereignty in resolving the constitutionality of legislation passed pursuant to the Elections Clause.[289] But Congress has exercised its Elections Clause power far less often than it has used its authority to enforce the Fourteenth and Fifteenth Amendments.[290] Because the Supreme Court's decision in *Shelby County* diminished Congress's power to regulate elections under the Reconstruction Amendments, Congress must rely on its Elections Clause authority to enact legislation that protects U.S. election infrastructure.[291]

---

280 §§ 301, 303, 116 Stat. at 1704–05, 1708.

281 Weinstein-Tull, *supra* note 3, at 759.

282 *Id.*

283 *Cf.* JAMES T. BENNET, MANDATE MADNESS: HOW CONGRESS FORCES STATES AND LOCALITIES TO DO ITS BIDDING 211, 214–15 (2014) (describing and criticizing the "carrot and stick" approach of HAVA, which provided federal funds to help induce states to comply with the statute's requirement that they update and modernize voting equipment).

284 §§ 102–305, 116 Stat. at 1670–71, 1714.

285 §§ 301, 116 Stat. at 1704–06.

286 *U.S. Election Assistance Commission to Administer $380 Million in 2018 HAVA Election Security Funds*, U.S. ELECTION ASSISTANCE COMM'N NEWS (Mar. 29, 2018), https://www.eac.gov/news/2018/03/29/us-election-assistance-commission-to-administer-380-million-in-2018-hava-election-security-funds.

287 *See infra* Part III.A.

288 Tolson, *supra* note 252, at 173.

289 Tolson, *supra* note 216, at 2216.

290 Tolson, *supra* note 252, at 173.

291 Tolson, *supra* note 216, at 2215.

While Congress has not previously exercised the full extent of its power under the Elections Clause, it could do so to create a uniform federal election system.

III. CONGRESS SHOULD ACT TO PROTECT U.S. ELECTION INFRASTRUCTURE

Due to the threat of foreign interference in U.S. elections, Congress has both the authority and an obligation to act. The notion that Congress cannot create a federal plan for elections because such action would infringe on states' rights misinterprets the Constitution. The Elections Clause gives Congress a definitive right to regulate federal elections.[292] The combination of multiple sources of constitutional authority—the Elections Clause and the Reconstruction Amendments—provides Congress with even greater power to act.[293] Congress is also duty-bound to protect the integrity of our democracy and to ensure the rights of all citizens to have their votes properly counted.[294] It has a responsibility to take action to protect U.S. election infrastructure in the face of cybersecurity threats because state and local election officials are incapable of doing so.[295]

Therefore, to combat foreign interference, Congress must enact legislation to improve the security of election systems throughout the country. Congress should pass a federal plan for three main reasons. First, the structure and purpose the Elections Clause bestows upon Congress a duty to maintain the legitimacy of the federal government.[296] In other words, Congress must ensure that the result of federal elections reflects the will of voters. Second, states are ill-equipped and reticent to take the cybersecurity measures necessary to protect election infrastructure.[297] Third, the enforcement clauses of the Fourteenth and Fifteenth Amendments obligate Congress to protect the right of all citizens to vote.[298]

A. Congress Has an Obligation Under the Elections Clause to Protect U.S. Democracy

The integrity of elections is critical to maintaining democracy in the United States. Almost 150 years ago, the Supreme Court analogized the power to

---

[292] *See supra* Part II.C.

[293] Tolson, *supra* note 164; *see infra* Part III.C.

[294] *See* United States v. Slone, 411 F.3d 643, 649 (2005) ("Under the Elections Clause, Congress is authorized to protect the integrity of federal elections.").

[295] *See infra* Part III.B.

[296] *See* U.S. CONST. art. I, § 4, cl. 1; Tolson, *supra* note 216, at 2218.

[297] *See infra* Part III.B.

[298] U.S. CONST. amend. XIV, § 5; U.S. CONST. amend. XV, § 2; *see infra* Part III.C.

regulate federal elections to the right to defend the nation itself.[299] In *Ex parte Yarbrough*, the Court stated "[t]hat a government whose essential character is republican . . . has no power by appropriate laws to secure this election from the influence of violence, of corruption, and of fraud, is a proposition so startling as to arrest consideration and demand the gravest consideration."[300] Foreign interference in U.S. elections is not a necessary, but a sufficient, condition for Congress to exercise its authority under the Elections Clause. Congress has a constitutional responsibility to ensure the integrity of the U.S. election process and to protect the fundamental right of citizens to vote.

The overarching purpose of the Elections Clause "is to ensure the continued existence and legitimacy of federal elections."[301] Hamilton described the critical point of the Elections Clause: "every government ought to contain in itself the means of its own preservation."[302] According to Hamilton, Congress must use its authority to assume from states the responsibility of regulating the manner of federal elections "whenever extraordinary circumstances might render that imposition necessary to its safety."[303] Foreign interference in U.S. elections is one such extraordinary circumstance.[304] Therefore, for the safety of the nation and the preservation of confidence in federal elections, Congress has an obligation to invoke the Elections Clause to create a federal plan for election administration.[305]

While Congress has occasionally exercised its broad powers to regulate elections under the Elections Clause, it has been reluctant to take full action against the threat of foreign interference. In response to Russia's cyberattacks in 2016 and 2018, the Democratic-led House of Representatives attempted to take small steps to improve the security of federal elections. In 2018, Congress authorized $380 million under HAVA for states to bolster their election security.[306] While several states used the HAVA funds to strengthen cybersecurity and purchase new voting equipment, the amount of money is far

---

299 *Ex parte* Yarbrough, 110 U.S. 651, 657–58 (1884).

300 *Id.* at 657.

301 Tolson, *supra* note 216, at 2218.

302 THE FEDERALIST NO. 59 (Alexander Hamilton).

303 *Id.*

304 Lynch, *supra* note 187, at 2008–11.

305 Tolson, *supra* note 216, at 2218.

306 Dustin Volz, *U.S. Spending Bill to Provide $380 Million for Election Cyber Security*, REUTERS (Mar. 21, 2018, 1:30 PM), https://www.reuters.com/article/us-usa-fiscal-congress-cyber/u-s-spending-bill-to-provide-380-million-for-election-cyber-security-idUSKBN1GX2LC; Norden & Cordova, *supra* note 110.

from sufficient.[307] Congress has otherwise been reluctant to pass legislation that would be effective enough to prevent further cyberattacks.[308]

Although the House passed three election security bills in 2019, predominantly along party-line votes, the bills have made no progress in the Senate.[309] Congressional Republicans have downplayed the extent of foreign interference in the 2016 and 2018 elections.[310] Objecting to the 2019 Securing America's Federal Elections (SAFE) Act, Representative Rodney Davis (R-Ill.) stated that Congress should not force states to update voting technology because "there is no evidence of voting machines being hacked in 2016, 2018[,] or ever[.]"[311] Senate Majority Leader Mitch McConnell (R-Ky.), who has refused to bring any of the House bills up for a vote in the Senate, has also minimized the risk.[312] Senator McConnell even chided the media for fostering panic among voters and for not giving more credit to the current administration for preventing major security breaches in the 2018 election.[313]

However, in objecting to the SAFE act, Congressional Republicans have primarily argued that the bill's provisions interfere with the authority of states and localities to conduct elections.[314] Senator McConnell stated that while he believes Russian meddling to be real, he doesn't believe that the federal government should tell states how to run elections.[315]

The Republican sentiment, as expressed by Senator McConnell, misinterprets the authority granted to Congress under the Constitution. Because the Elections Clause gives Congress final policymaking authority over the times, places, and manners of federal elections, it "allows Congress to legislate independent of and without deference to state sovereignty."[316] Therefore, the

---

307 Norden & Cordova, *supra* note 110.

308 *Id.*

309 For the People Act of 2019, H.R. 1, 116th Cong.; Stopping Harmful Interference in Elections for a Lasting Democracy (SHIELD) Act, H.R. 4617, 116th Cong.; Securing America's Federal Elections (SAFE) Act, H.R. 2722, 116th Cong.

310 Maggie Miller & Julie G. Brufke, *House Passes Sweeping Democratic-Backed Election Security Bill*, HILL (Jun. 27, 2019, 5:00 PM), http://thehill.com/homenews/house/450737-house-passes-sweeping-democrat-backed-election-security-bill; Hailey Fuchs & Karoun Demirjian, *Divided House Passes Election Security Legislation over Republican Objection*, WASH. POST (Jun. 27, 2019, 4:45 PM), https://www.washingtonpost.com/powerpost/divided-house-passes-election-security-legislation-over-republican-objections/2019/06/27/a071c10c-98f1-11e9-8d0a-5edd7e2025b1_story.html.

311 Miller & Brufke, *supra* note 310.

312 Fuchs & Demirjian, *supra* note 310.

313 *Id.*

314 *Id.*

315 DeChiaro, *supra* note 18.

316 Tolson, *supra* note 164, at 324.

notion that Congress must cajole states to undertake security fixes to their election systems and abide by federal security standards is grossly misguided.[317] Congress has an obligation under the Elections Clause to preserve the legitimacy of the federal government by ensuring that federal elections reflect the will of the people.[318] A strong and uniform federal plan is needed to protect against efforts by foreign actors to disrupt U.S. elections.

B. Congress Has a Duty to Secure U.S. Elections Against Foreign Interference Because States Are Ill-Equipped and Reluctant to Do So

The United States is unique in that it currently has no nationwide election authority.[319] Conducting elections in the United States is a complex process "that involves multiple levels of government, personnel with a variety of skills and capabilities, and numerous electronic systems that interact in the performance of a multitude of tasks."[320] State or local officials manage elections in accordance with state laws and local regulations.[321] Elections are administered by over 9,000 state and local jurisdictions containing over 114,000 polling places.[322] The thousands of jurisdictions vary widely in size, in funding available for election administration, and in the ability to detect and manage irregularities, particularly cyberattacks.[323] Several of the small elections offices "have few dedicated staff and little access to the latest information technology (IT) training or tools."[324]

A lack of cyber sophistication was evident in the 2016 election as states and municipalities were unequipped to deal with the severity of the threat. One state official said, "I don't think any of us expected to be hacked by a foreign government."[325] Another official stated, "If a nation-state is on the other side, it's not a fair fight. You have to phone a friend."[326] In most states, the decentralized structure means that counties and municipalities have varying

---

317 *See* SENATE INTELLIGENCE REPORT, *supra* note 13, at 54 (stating in its recommendations that "[s]tates should remain firmly in the lead on running elections, and the federal government should ensure they receive the necessary resources and information").

318 *See* THE FEDERALIST NO. 59 (Alexander Hamilton) ("Every government ought to contain in itself the means of its own preservation.").

319 NAS REPORT, *supra* note 11, at 31.

320 *Id.* at 4.

321 NAS REPORT, *supra* note 11, at 17.

322 Manpearl, *supra* note 71, at 169.

323 NAS REPORT, *supra* note 11, at 17. *See generally* David C. Kimball & Brady Baybeck, *Are All Jurisdictions Equal? Size Disparity in Election Administration*, 12 ELECTION L.J. 130 (2013) (discussing how size disparities lead to diverging experiences for election officials and voters in large versus small jurisdictions).

324 NAS REPORT, *supra* note 11, at 17.

325 SENATE INTELLIGENCE REPORT, *supra* note 13, at 39.

326 *Id.*

levels of resources to conduct elections.[327] County election officials, who are on the front lines of defending election equipment, often have very limited IT support.[328] A Wisconsin state election administrator noted that some counties' election teams may only consist of "a county clerk and one more person working on elections."[329]

Many county officials have not received any cybersecurity training, even after the 2016 cyberattacks were made known. In Pennsylvania, election officials in three of the four largest counties had not received cybersecurity training as of August 2017.[330] In Michigan, officials in fewer than one-third of counties indicated that they received formal cybersecurity training.[331] And in Arizona, officials in only five of fifteen counties received such training.[332]

States also vary widely in the level of security they maintain around voter registration databases. DHS analysis of state election systems found significant variance in the security of state voter registration databases, including lack of encryption and lack of backups in many states.[333] As of May 2017, forty-one states were still using voter registration systems that were created more than a decade prior.[334] Types of vote casting systems also vary dramatically from state to state. Forty-five states continue to use outdated voting machines that are no longer manufactured.[335] Some machines are at least fifteen years old and run on outdated software that is no longer supported, such as Windows XP.[336] In the November 2018 election, fourteen states did not use a voting mechanism that allowed for a voter-verified paper audit trail.[337]

Many states understand the need for more secure voting equipment but lack sufficient financial resources. Although the 2018 HAVA funds were dispersed quickly, states did not have enough time to make major improvements to their

---

327 *See* Norden & Cordova, *supra* note 110.

328 *Id.*

329 *Id.*

330 Likhitha Butchireddygari, *Many County Officials Still Lack Cybersecurity Training*, NBC NEWS (Aug. 23, 2017, 5:20 AM), https://www.nbcnews.com/politics/national-security/voting-prep-n790256.

331 *Id.*

332 *Id.*

333 SENATE INTELLIGENCE REPORT, *supra* note 13, at 46.

334 Tim Lau, *U.S. Elections Are Still Vulnerable to Foreign Hacking*, BRENNAN CTR. FOR JUST. (Jul. 18, 2019), https://www.brennancenter.org/our-work/analysis-opinion/us-elections-are-still-vulnerable-foreign-hacking.

335 Norden & Cordova, *supra* note 110.

336 *Id.*

337 Lin et al., *supra* note 51, at 22.

election systems before the 2018 midterm elections.[338] The funding has also been insufficient for states to overhaul their elections systems and replace outdated voting machines.[339] Most states recognized a need to purchase new equipment before the 2020 election, but two thirds of the state officials claimed that they lack the money to do so, even with the additional HAVA funds.[340]

Consequently, states and municipalities cannot be relied on to successfully combat foreign cyberattacks against U.S. election systems. According to Senator Ron Wyden (D-Or.),

> If there was ever a moment when Congress needed to exercise its clear constitutional authorities, this is it. America is facing a direct assault on the heart of our democracy by a determined adversary. We would not ask a local sheriff to go to war against the missiles, planes and tanks of the Russian army. We shouldn't ask a county IT employee to fight a war against the full capabilities and vast resources of Russia's cyber army. That approach failed in 2016 and it will fail again.[341]

Simply providing funding to states is also not enough. Congress must create a comprehensive plan to secure federal elections against foreign attacks.

C. Congress Must Enact a Federal Plan to Preserve the Right of All Citizens to Vote

Professor Franita Tolson has effectively described how Congress's license to enact comprehensive federal election legislation may be even greater than its Elections Clause power alone because it derives from multiple sources of authority.[342] In addition to its obligation to preserve the integrity of federal elections under the Elections Clause, Congress has a responsibility to exercise its authority under the enforcement clauses of Fourteenth and Fifteenth Amendments to protect the right of all citizens to vote.[343] Multiple sources of authority confer even broader power when Congress acts to protect constitutional rights and may provide the impetus for the Supreme Court to find a federal statute valid where it would have considered it unconstitutional under a single source of authority.[344] Therefore, notwithstanding the Supreme Court's

---

338 The EAC dispersed 96% of the HAVA funds by August 2018. Lynch, *supra* note 187, at 1999.

339 Norden & Cordova, *supra* note 110.

340 *Id.*

341 SENATE INTELLIGENCE REPORT, *supra* note 13, Minority Views of Senator Wyden, at 1.

342 Tolson, *supra* note 164, at 329.

343 *Id.* at 324.

344 *Id.* at 329. The Supreme Court has been inconsistent in its recognition of a greater scope of authority when Congress acts pursuant to multiple sources of authority. *Compare* Tennessee v. Lane, 541 U.S. 509, 516

holding in *Shelby County*, the Reconstruction Amendments provide additional power to Congress's Elections Clause authority to establish a federal system for election infrastructure.[345] With this power comes a duty for Congress to act.

Cyberattacks that disrupt the voting process and create risks that vote tallies will be manipulated infringe on the right of citizens to vote. The fundamental right to vote includes the right to be certain that one's vote matters.[346] Courts have found that plaintiffs have standing to bring Fourteenth Amendment Due Process and Equal Protection claims where they allege that certain voting methods prohibit their votes from being properly counted.[347] In *Stewart v. Blackwell*, the Sixth Circuit found that the increased probability that plaintiffs' votes would not be properly counted due to a faulty punch-card system was "neither speculative nor remote" and was therefore a justiciable claim.[348] Similarly, a Pennsylvania court found that voters had proper standing to bring a Fourteenth Amendment claim because the machines they used to vote did not allow them to know whether their votes had been cast or would be counted.[349]

A recent lawsuit brought by voters in Georgia demonstrates how voting systems that are not secure against cyberattacks infringe on voters' rights.[350] A federal court granted an injunction against using insecure DRE machines based on the merits of the plaintiffs' Fourteenth Amendment Due Process and Equal Protection claims.[351] The plaintiffs in *Curling* claimed that the state had violated their Due Process rights by placing a "substantial burden" on their fundamental right to vote and had violated their Equal Protection rights by placing "more severe burdens" on their right to vote than voters who did not have to use DRE machines.[352] The court agreed and granted plaintiff's relief in part because the

(2004) (upholding Title II of the Americans with Disabilities Act (ADA) based on "the power to enforce the [F]ourteenth [A]mendment and to regulate commerce"), *with* Bd. of Trs. v. Garrett, 531 U.S. 356, 374 (2001) (ignoring the Congress's Commerce Clause authority when invalidating the ADA in part as an improper exercise of the Fourteenth Amendment enforcement clause), *and* Shelby Cnty. v. Holder, 570 U.S. 529, 553 (2013) (giving no weight to Congress's additional authority for enacting the VRA under both the Fourteenth and the Fifteenth Amendments).

345 *See* Tolson, *supra* note 164, at 330 ("[F]ar-reaching and potentially controversial legislation can gain substantial legitimacy from the fact that Congress can draw on multiple sources of power.").

346 *See* Curling v. Kemp, 334 F. Supp. 3d 1303, 1328 (N.D. Ga. 2018).

347 *E.g.*, *id.*

348 Stewart v. Blackwell, 444 F.3d 843, 855 (6th Cir. 2006), *superseded by* Stewart v. Blackwell, 473 F.3d 692 (6th Cir. 2007).

349 Banfield v. Cortes, 922 A.2d 36, 44 (Pa. Commw. Ct. 2007).

350 *Curling*, 334 F. Supp. 3d 1303; Curling v. Raffensperger, 397 F. Supp. 3d 1334 (N.D. Ga. 2019).

351 *Curling*, 397 F. Supp. 3d at 1410.

352 *Curling*, 334 F. Supp. 3d at 1312.

state's ongoing use of an insecure voting method "pierce[d] citizens' confidence in the electoral system and the value of voting."[353]

Therefore, in some instances, voting rights advocates can protect the right to vote against insecure voting systems through litigation.[354] Federal courts may be willing to recognize that an infringement on voters' right to feel secure that their votes will count is an injury for which relief may be granted.[355] Insecure voting systems can also affect voters' ability to merely cast a ballot. Long wait times to vote—resulting from erroneous registration data or voting equipment dysfunction—may impact minority voting districts to a greater degree than predominantly white precincts.[356] And as wait times increase, voter participation drops.[357] Consequently, the Equal Protection Clause and the Fifteenth Amendment may be implicated when citizens of color are disproportionately denied the right to vote when cyberattacks disrupt voting on election day.

However, litigation is cumbersome and cannot always protect the rights of all voters or ensure the integrity of federal elections. Indeed, one impetus for the VRA in 1965 was that piecemeal litigation had failed to sustainably protect the African Americans' right to vote in most jurisdictions in the Deep South.[358] With each hard fought victory in courts, state and local governments found ways to enact new restrictions.[359] Moreover, litigation only grants relief after harm has occurred. Courts can grant prospective relief to require security measures for future election cycles.[360] But there is no sufficient remedy for the harm to voters that has already occurred after they participated in an insecure election.[361] Thus,

---

353 *Curling*, 397 F. Supp. 3d at 1411 (quoting *Curling*, 334 F. Supp. 3d at 1328).

354 *Id.* at 1410.

355 *Id.*; *see Curling*, 334 F. Supp. 3d at 1328 ("A wound or reasonably threatened wound to the integrity of a state's election system carries grave consequences beyond the results in any specific election, as it pierces citizens' confidence in the electoral system and the value of voting."). *Contra* Heindel v. Andino, 359 F. Supp. 3d 341, 357 (D.S.C. 2019) (holding that plaintiffs failed to show a clearly impending injury that was traceable to state election officials because they "merely speculate and make assumptions about whether their votes will be inaccurately counted as the result of a potential hack" (quoting Clapper v. Amnesty Int'l, 568 U.S. 398, 411 (2013))).

356 Stephanie Mencimer, *Even Without Voter ID Laws, Minority Voters Face More Hurdles to Casting Ballots*, MOTHER JONES (Nov. 3, 2014), https://www.motherjones.com/politics/2014/11/minority-voters-election-long-lines-id/; German Lopez, *Minority Voters Are Six Times More Likely as White Voters to Wait More Than an Hour to Vote*, VOX (Nov. 8, 2016, 1:30 PM), https://www.vox.com/identities/2016/11/8/13564406/voting-lines-race-2016.

357 *Lopez*, *supra* note 356.

358 South Carolina v. Katzenbach, 303 U.S. 301, 314 (1966).

359 *Id.*; ANDERSON, *supra* note 165, at 13; *see supra* Part II.A.

360 *See Curling*, 397 F. Supp. 3d at 1412.

361 *See Curling*, 334 F. Supp. 3d at 1315.

the federal government must respond comprehensively to protect voters' rights against cyberattacks from foreign actors.

In sum, Congress must act to protect U.S. election infrastructure and to combat foreign interference in federal elections. Congress has the primary obligation to safeguard the legitimacy of the federal government, to protect the fundamental right of citizens to vote, and to ensure that the election results reflect the choice of the majority of voters. And Congress has the authority to act pursuant to the Elections Clause coupled with the enforcement provisions of the Reconstruction Amendments, which provide additional power to protect the right of all citizens to vote.

IV. A PROPOSED FEDERAL PLAN TO SECURE U.S. ELECTIONS

Congress has the power under the Elections Clause to enact legislation that establishes a federal plan to which state election authorities must adhere.[362] The Elections Clause authorizes Congress to designate the manner in which federal elections are conducted in order to protect the integrity of the federal government against a threat of foreign interference.[363] After Russian cyberattacks against state and local election systems in 2016 and 2018, and the anemic, ineffective response by state election officials, the need for a uniform federal election plan is evident.[364] Therefore, Congress has the obligation to enact a national plan that creates uniform standards across all election jurisdictions to ensure that federal elections are secure and that all citizens are able to exercise their right to vote and know their votes will count.

A national plan for federal elections does not imply that the entirety of election administration should be conducted by the federal government. The decentralized approach to U.S. elections, which relies on states and localities to manage the nuts and bolts of elections, provides efficiency.[365] The cybersecurity benefit of a decentralized structure remains—it protects against the devastating impact of a single widespread cyberattack or technological breakdown.[366] But an ongoing role for states to conduct elections does not preclude implementing uniform rules and standards for federal elections. Measures to secure U.S.

---

362 *See supra* Part III.A.

363 *See id.*

364 *See supra* Part I.C.

365 *See* THE FEDERALIST NO. 59 (Alexander Hamilton) (stating that regulation of federal elections is left to local administrations because "it may be more convenient and more satisfactory").

366 Manpearl, *supra* note 71, at 182; NAS REPORT, *supra* note 11, at 119.

election infrastructure would be most effective if they are implemented at a national level.[367]

Although Congress's national plan for federal elections should be mandatory for states to follow, the Elections Clause does not grant Congress authority over state and local elections.[368] However, Congress can encourage states to follow a federal election plan for their own internal elections. First, because of logistics, efficiency, and cost, states would likely use federal election infrastructure to conduct state and local elections along with federal elections. Second, states' inability to take appropriate cybersecurity measures for their own elections provides the impetus for Congress to act under the Fourteenth and Fifteenth Amendments to protect the right of all citizens to know that their votes with count.[369] Unlike the Elections Clause, the Fourteenth and Fifteenth Amendments apply to *all* elections: federal, state, and local.[370] Third, Congress could use its Spending Clause power to condition funding for election infrastructure on a state's compliance with a federal plan for all elections conducted within the state.[371]

A national election plan should have three main components. First, it should create uniform federal standards for securing voter registration databases and for transmitting voter information to polling places so that voters can be checked-in on election day. Second, Congress should require that all states implement a secure method of voting that uses a uniform ballot design. All voters should be allowed to mark and record their selections in the manner that is least susceptible to cyberattacks: hand-marked paper ballots read by secure, state-of-the-art optical scanners. Finally, to ensure the integrity of every federal election, states must be required to submit to federal post-election audits.

---

367 *See* Mark Lanterman, *Fair Elections and Cybersecurity*, 75 BENCH & BAR MINN. 10, 10 (2018) ("[T]he sorts of measures that would most likely effect positive security outcomes are best implemented at a national level, where standardized procedures can provide a framework for ongoing improvement.").

368 U.S. CONST. art. I, § 4, cl. 1.

369 *See supra* Part III.C.

370 U.S. CONST. amend. XV, § 1 ("The right of citizens of the United States to vote shall not be denied or abridged *by the United States or by any State* . . . .") (emphasis added).

371 *See* Art. I, § 8, cl. 1 (empowering Congress to "lay and collect Taxes, Duties, Imposts, and Excises, to pay the Debts and provide for the common Defence and general Welfare of the United States"); South Dakota v. Dole, 483 U.S. 203, 207 (1987) ("[O]bjectives not thought to be within Article I's enumerated legislative fields may nevertheless be attained through the spending power and the conditional grant of federal funds.") (internal quotation marks omitted).

A. Congress Should Establish Binding Federal Standards for States to Register Voters, Maintain Secure Voter Databases, and Check-in Voters at the Polls

Voter registration databases that are maintained electronically are particularly vulnerable to manipulation by malicious cyber actors.[372] Election administrators currently rely on county or state government IT departments to secure voter registration databases.[373] A DHS analysis found that the security of voter databases varied significantly by state, and many states lacked encryption and backups for their databases.[374] Federal intelligence and cybersecurity officials have made recommendations to states and have offered to provide cybersecurity measures to protect voter registration databases.[375] But many states have demonstrated a reluctance to receive help from the federal government or to follow recommendations.[376]

Consequently, Congress must pass legislation that directs states to implement specific cybersecurity measures for voter registration databases, which include updating relevant software, creating paper back-ups, and instituting two-factor authentication for user access to the databases.[377] This action would not be novel—Congress has previously set mandatory requirements for state voter databases.[378] A federal plan should also require states to put in place standard security procedures for monitoring voter database integrity.[379] Such measures should include installing monitoring sensors on state registration systems to detect attempts to hack into the systems and reporting any identified compromises immediately to DHS.[380]

A national plan must also create standards for transmitting voter data to polling places for voter verification and check-in. Because they are electronic, e-pollbooks are vulnerable to cyberattacks, particularly if they are locally

---

372 SENATE INTELLIGENCE REPORT, *supra* note 13, at 57.

373 NAS REPORT, *supra* note 11, at 58.

374 SENATE INTELLIGENCE REPORT, *supra* note 13, at 46.

375 *Id.* at 52.

376 *See supra* Part III.B; SENATE INTELLIGENCE REPORT, *supra* note 13, at 48–49; *see also id.*, Minority Views of Senator Wyden, at 2 ("The Committee report describes a range of cybersecurity measures needed to protect voter registration databases, yet there are currently no mandatory rules that require that require states to implement even minimum security measures.").

377 SENATE INTELLIGENCE REPORT, *supra* note 13, at 57.

378 Help America Vote Act of 2002, Pub. L. No. 107-252, 116 Stat. 1666 (codified as amended at 42 U.S.C. §§ 15301-15545) (requiring "a single, uniform, official, centralized, interactive, computerized statewide voter registration list defined, maintained, and administered at the state level").

379 NAS REPORT, *supra* note 11, at 63.

380 SENATE INTELLIGENCE REPORT, *supra* note 13, at 57.

networked or connected to the internet.[381] Cyberattacks could change voter data, alter information on who has voted, or simply shut down operation of an e-pollbook through a "denial of service" attack.[382] Congress should, therefore, include national security standards for the use of e-pollbooks in its federal plan. Because e-pollbooks have advantages over paper and are easy to use, their use should not be discontinued.[383] Rather, the NAS recommends that Congress authorize and fund the National Institute of Standards and Technology to develop security standards along with verification and validation protocols for e-pollbooks.[384] In addition, each precinct should be required to maintain a paper copy of the precinct's pollbook as a back-up in the event that voter data is manipulated or access to electronic data is disrupted.[385]

B. Congress Should Mandate Uniform Paper Ballots for All Federal Elections

Voters across the country cast their ballots using methods that are subject to varying degrees of cyber risks, and many states are either unwilling or incapable of following the recommendations of cybersecurity experts.[386] Voting systems that do not provide human-readable printouts for voters to confirm their selections and do not maintain a voter-verified paper audit trail are most vulnerable to cyberattacks.[387] Experts have called for discontinuing the use of paperless DRE machines because they are vulnerable to hacking without detection and do not produce auditable paper trails.[388] Yet, in 2019, twelve states were still using paperless DRE machines in at least some jurisdictions, and four states still used them statewide.[389] Congress should pass legislation that prohibits states from using outdated, paperless voting machines and requires the use of a uniform method of voting that will provide an auditable paper trail.

The Senate Intelligence Report concluded that "[p]aper ballots and optical scanners are the least vulnerable to cyberattack."[390] The most secure and cost-effective method for voting would be to use hand-marked paper ballots in all

---

381 See *supra* Part I.B. regarding the vulnerability of e-pollbooks.

382 NAS REPORT, *supra* note 11, at 71, 86.

383 *Id.* at 72.

384 *Id.*

385 *Id.*

386 *See supra* Part III.B.

387 SENATE INTELLIGENCE REPORT, *supra* note 13, at 42.

388 See *supra* Part I.B. for a detailed description of the security flaws associated with DRE voting machines.

389 Norden & Cordova, *supra* note 110.

390 SENATE INTELLIGENCE REPORT, *supra* note 13, at 59.

federal elections.[391] Using a uniform paper ballot for federal elections that voters mark by hand would also allow states to continue and expand the use of vote-by-mail.[392] Alternatively, Congress could require and provide funding for uniform BMD machines to be used across all jurisdictions. The BMDs must produce a paper record of the voter's choices, which each voter can review before casting their ballot. However, because BMD machines are potentially vulnerable to cyberattacks, the most secure election systems use hand-marked paper ballots as the primary method for voting.[393] Moving forward, Congress should mandate that all federal elections be conducted using human-readable paper ballots that are counted either by hand or by using federally certified optical scanners.[394]

C. Congress Should Require All States to Submit to Federal Election Audits

As part of a federal election plan, Congress should require that all states submit to post-election audits. Audits require voter-verifiable paper ballots that provide a human-readable record of the voter's selections.[395] Such audits provide assurance that the outcome of any election reflects the voters' choices and is based on an accurate tabulation of the ballots cast.[396]

NAS election cybersecurity experts recommend risk-limiting audits as the most efficient and effective means to ensure the reliability of an election.[397] Risk-limiting audits examine randomly selected, individual ballots until a predetermined level of statistical assurance is reached.[398] In 2017, risk-limiting audits were piloted statewide in Colorado, and several other states plan to conduct pilots in the next few years.[399] However, rather than leaving the requirement for audits to the discretion of states, Congress should pass

---

391 *Id.*; Christopher Deluzio & Kevin Skoglund, *Guess Which Ballot Costs Less and Is More Secure—Paper or Electronic?*, PATRIOT NEWS (Aug. 20, 2019), https://www.pennlive.com/opinion/2019/08/guess-which-ballot-costs-less-and-is-more-secure-paper-or-electronic-opinion.html.

392 In 2016, Colorado, Oregon, and Washington used mail-only voting, and most ballots in California and Utah were cast by mail. NAS REPORT, *supra* note 11, at 48–50.

393 *See generally* Andrew Appel, Richard A. DeMillo & Philip B. Stark, *Ballot-Marking Devices (BMDs) Cannot Assure the Will of the Voters*, 19 ELECTION L.J. 432 (2020) (describing the vulnerability of BMD voting machines to hacking as well as risk that BMDs may not accurately record a vote as the voter had intended and arguing that the most secure method of voting is a system that uses hand-marked paper ballots).

394 NAS REPORT, *supra* note 11, at 80.

395 *Id.* at 94.

396 *Id.*

397 *Id.* at 95.

398 *Id.*

399 *Id.*

legislation to require all states to submit to federal risk-limiting audits after each federal election.

The federal government's response to ongoing Russian cyberattacks must extend beyond offers to provide resources to states.[400] To protect and defend U.S. elections, Congress must "establish mandatory nation-wide cybersecurity requirements."[401] Such requirements must designate specific measures to ensure the security of voter registration databases and pollbooks and should compel the use of uniform paper ballots and post-election audits.

CONCLUSION

The right of citizens to freely choose who will represent them is the essence of our republican form of government. The founders understood that maintaining free and fair elections is a core tenet of this nation. Therefore, they placed in the Constitution the means for Congress to have final authority to regulate federal elections when the need arises. Russian cyberattacks on state and local election systems constitute a challenge to the core values of American democracy, which require a comprehensive, uniform federal response.

To varying degrees over the past 150 years, Congress has imposed regulations on states to protect election integrity by ensuring that all citizens have the right to vote. The current threat requires an even greater response. This Comment describes a source of authority that authorizes Congress to prescribe cybersecurity measures to which states must adhere in conducting federal elections. The value implicit in the Elections Clause is that federal elections must be administered in a manner that produces a clear and legitimate outcome. Congress has the authority and an obligation under the Elections Clause to ensure the integrity of American democracy in the face of cyberattacks by a foreign adversary. Congress must exercise this power to create a comprehensive national plan for federal elections.

SUMAN MALEMPATI*

400 SENATE INTELLIGENCE REPORT, *supra* note 13, Minority Views of Senator Wyden, at 1.

401 *Id.*

* J.D. Candidate, Emory University School of Law, Class of 2021. I extend my deepest gratitude to Professor Robert Schapiro for his wisdom, guidance, and support throughout the writing process. Thank you to Natalie Baber and Connor Hees for providing insightful feedback. To the *Emory Law Journal* staff, particularly Brennan Mancil and Sam Reilly, thank you for the incredible work you have done make this Comment better and get it published.