PROTECTING THE STATES FROM ELECTORAL INVASIONS

Drew Marvel*

> Protecting systems from cyberthreats from nation-states can really only be done on a national level. It's insane we have state-level control of these systems.
>
> —Dave Aitel, former National Security Agency security scientist[1]

INTRODUCTION

Since the 2016 U.S. presidential election, the threat of foreign interference in U.S. elections has loomed large in the minds of the American public.[2] During the 2016 campaign season, Russian government-backed hackers infiltrated the networks and computers of the Democratic National Committee (DNC), the Democratic Congressional Campaign Committee (DCCC), and various campaign officials, harvesting private information and installing spyware and malware for ongoing intelligence purposes.[3] U.S. intelligence officials have indicated that, using similar tactics, the Russian hackers also targeted election systems and officials in all fifty states,[4] successfully breaching at least two of those states' election systems, Illinois and Florida.[5]

---

* JD Candidate, William & Mary Law School, 2020; BA, University of Maryland, Baltimore County, 2017. Thank you to the *William & Mary Bill of Rights Journal* staff for their edits, and a big shout out to Mike and Andrea for their support and direction early on. Many thanks to Professors Rebecca Green and Tara Grove for their encouragement and suggestions during the writing process. Finally, thanks to my Mom and Dad, my sisters Ashley and Brittany, my brothers-in-law Ben and Scottie, and Sofie, Wes and Archer for keeping me sane throughout this endeavor.

[1] Derek Hawkins, *Elections Remain Vulnerable to Hacking, Experts Say*, PROVIDENCE J. (May 26, 2018, 8:16 PM), https://www.providencejournal.com/news/20180526/elections-remain-vulnerable-to-hacking-experts-say [https://perma.cc/8JPQ-GSQQ].

[2] *See, e.g.*, Sabrina Siddiqui, *Half of Americans See Fake News as Bigger Threat than Terrorism, Study Finds*, GUARDIAN (June 7, 2019, 8:53 PM), https://www.theguardian.com/us-news/2019/jun/06/fake-news-how-misinformation-became-the-new-front-in-us-political-warfare [https://perma.cc/U3W5-8RV6].

[3] *See* 1 ROBERT S. MUELLER III, U.S. DEPT. OF JUSTICE, REPORT ON THE INVESTIGATION INTO RUSSIAN INTERFERENCE IN THE 2016 PRESIDENTIAL ELECTION 36–41 (2019) [hereinafter MUELLER REPORT].

[4] Sean Gallagher, *DHS, FBI Say Election Systems in All 50 States Were Targeted in 2016*, ARSTECHNICA (Apr. 10, 2019, 2:20 PM), https://arstechnica.com/information-technology/2019/04/dhs-fbi-say-election-systems-in-50-states-were-targeted-in-2016/ [https://perma.cc/E8WL-XUAP].

[5] *See* MUELLER REPORT, *supra* note 3, at 50–51. In July 2016, Russian hackers used a

The purpose of these hacks was not to damage or otherwise incapacitate the nation's electoral infrastructure, but rather to gather information that could be used in a larger, comprehensive, and ongoing misinformation campaign designed to undermine the public's trust in democratic and governmental institutions, influence public opinion and, ultimately, impact the election itself.[6]

The Russian campaign in 2016 was wildly successful, and the U.S. intelligence community has made it clear that the Russians have every intention of continuing these types of malign cyber-operations in future elections.[7] Although Russia may be the poster child for this type of electoral interference, U.S. officials have stated that other foreign powers have taken note of the Russian success and will likely be engaged in similar sorts of ideological warfare in the years to come.[8] This new threat has prompted ongoing discussions regarding the country's election security and state and local officials' preparedness—or rather lack thereof—to handle this growing national security issue. Many of these debates involve questions of federalism given the overlapping governmental interests and responsibilities this issue implicates: election administration, a constitutional privilege entrusted to the states; and national security, a sphere traditionally understood to fall under the federal government's domain.[9]

The Framers of the U.S. Constitution undoubtedly recognized that foreign threats would always pose a danger to the United States' continued independence, and, to that end, they debated at length to achieve the most effective and efficient allocation of governmental defense responsibilities between the states and the federal government.[10] Naturally, a document written in the late eighteenth century,

---

technique called "SQL injection" to breach the computers at the Illinois State Board of Election, allowing them to steal the personal information of about 500,000 Illinois voters. Chuck Goudie & Christine Tressel, *How the Russians Penetrated Illinois Election Computers*, ABC7 CHI. (July 19, 2018), https://abc7chicago.com/politics/how-the-russians-penetrated-illinois-election-computers/3778816/ [https://perma.cc/3RF2-BBNT]. Similarly, in 2016, Russian hackers used a technique called "spearphishing" to breach the election systems of two undisclosed counties in Florida. Patricia Mazzei, *Russians Hacked Voter Systems in 2 Florida Counties. But Which Ones?*, N.Y. TIMES (May 14, 2019), https://nyti.ms/2Q6yXTl.

[6] *See* MUELLER REPORT, *supra* note 3, at 36–50.

[7] *See* Press Release, Office of the Dir. of Nat.'l Intelligence, Joint Statement from the ODNI, DOJ, FBI and DHS: Combating Foreign Influence in U.S. Elections (Oct. 19, 2018), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2018/item/1915-joint-statement-from-the-odni-doj-fbi-and-dhs-combating-foreign-influence-in-u-s-elections [https://perma.cc/T5CP-XBRT] [hereinafter Joint Statement].

[8] *See* U.S. SENATE SELECT COMM. ON INTELLIGENCE, RUSSIAN TARGETING OF ELECTION INFRASTRUCTURE DURING THE 2016 ELECTION: SUMMARY OF INITIAL FINDINGS AND RECOMMENDATIONS (May 8, 2018), https://www.intelligence.senate.gov/sites/default/files/publications/RussRptInstlmt1.pdf [https://perma.cc/Y5LN-AZBQ] [hereinafter S. REP. SUMMARY ON RUSSIAN TARGETING].

[9] *See, e.g.*, R. SAM GARRETT, CONG. RESEARCH SERV., R45302, FEDERAL ROLE IN U.S. CAMPAIGNS AND ELECTIONS: AN OVERVIEW 1, 4–5 (2018).

[10] *See, e.g.,* THE FEDERALIST NO. 45 (James Madison).

a time when warfare was strictly understood to be a tangible threat, could not have predicted that the United States' democratic processes could be attacked without the enemy ever needing to step foot on American soil. Notwithstanding the Framers' unfamiliarity with modern day technology, they nonetheless contemplated the two governmental responsibilities foreign electoral interference directly implicates: maintaining a republican form of government in the states and defending the nation from foreign invasions. Article IV, Section 4 of the U.S. Constitution specifically entrusts the federal government with these dual obligations, proclaiming "[t]he United States *shall* guarantee to every State in this Union a Republican Form of Government, and *shall* protect each of them against Invasion."[11] Based on the plain text and underlying rationale of these provisions, it is clear that if alive today, the Framers would consider defending the states against foreign electoral interference as an obligatory duty falling squarely on the federal government's shoulders.

This Note takes the position that foreign election interference and hacking attempts should be understood as an "invasion" within the scope of Article IV, Section 4. This "invasion" poses an acute and unique risk to the states' "Republican Form[s] of Government"[12] such that the federal government has a constitutional duty to defend against it. It is important to note that the argument here does not posit an affirmative, judicially enforceable obligation on the federal government to act. Rather, "duty" should be understood as a judicially cognizable constitutional basis that further justifies greater federal involvement in and support of election security and administration.[13] Nor does this Note advocate for a sweeping, pre-emptive, one-size-fits-all federal legislative or regulatory framework for election administration. Such action would not only completely divest state and local jurisdictions of a constitutionally vested power, but would also likely create more problems than it would purportedly solve. Historically, the states have always fiercely resisted attempts by the federal government to interpose itself into the states' administration of elections, and the prospect of a complete federal takeover would in all likelihood make implementation near impossible.[14] Instead, this Note advocates for the federal government to take a more proactive role in assisting states and localities to fund and secure their election systems generally, and further articulates why such action would be both consistent with the Framers' intentions and beneficial to the nation's national security as a whole.

Part I provides a general overview of the current state of election administration and security in the U.S. It also discusses how systematic problems with funding,

---

[11] U.S. CONST. art. IV, § 4 (emphasis added).

[12] *Id.*

[13] *See generally, e.g.*, Gillian E. Metzger, *The Constitutional Duty to Supervise*, 124 YALE L.J. 1836 (2015).

[14] *See generally* Alan Greenblatt, *State Election Officials Fear Feds Are Making Security Worse*, GOVERNING (July 12, 2017, 5:00 PM), https://www.governing.com/topics/politics/gov-elections-states-federalism-trump.html [https://perma.cc/XYT3-WUJU].

varying cybersecurity standards and expertise, and inconsistent sharing and reporting of information can be exploited and exacerbated in the context of foreign interference attempts. Part II then briefly discusses how the federal Elections Clause provides the constitutional authority for the national government to legislate and regulate election administration, as well as highlighting federal legislation that already exists in this area. Finally, Part III examines the challenges involved in applying existing international law to non-damaging cyber-operations like the Russian election hacks and attempts to characterize them through comparison to the 2014 Sony hack. It also analyzes the Framers' intent and rationale for their inclusion of Article IV, Section 4 and how its text and structure command the importance with which they viewed the provision's obligations.

I. THE SWISS CHEESE OF ELECTION SECURITY INFRASTRUCTURE

The U.S. Constitution places the primary responsibility for holding and administering elections with the states, thereby making the nation's election systems decentralized by default.[15] Most states have further delegated many election administration responsibilities to local jurisdictions, creating a "*hyper*federalized"[16] electoral infrastructure comprised of thousands of independent systems.[17] Many security experts have lauded the heavily decentralized model as an effective security mechanism.[18] The "disjointed nature" of American elections means that for a hostile actor to infiltrate and manipulate elections on a wide scale, they would need to breach a multitude of systems successfully, each with its own unique security measures to overcome.[19] The decentralized system acts as a failsafe of sorts, containing any would-be successful hacker's access to only those systems compromised.[20]

This model, however, is a double-edged sword because the aspects that make it more secure also make it more difficult to defend against security threats, to respond to security breaches, and to assess the nation's systems as a whole.[21] States and counties vary widely in the types of hardware, software, and accompanying

---

[15] *See* U.S. CONST. art. I, § 4, cl. 1 ("The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations . . . .").

[16] ALEC C. EWALD, THE WAY WE VOTE: THE LOCAL DIMENSION OF AMERICAN SUFFRAGE 3 (2009).

[17] *See* Chris Good, *When it Comes to Election Cybersecurity, Decentralized System is Viewed as Both Blessing and Curse*, ABC NEWS (Oct. 31, 2018, 1:20 PM), https://abcnews.go.com/Politics/election-cybersecurity-decentralized-system-viewed-blessing-curse/story?id=58877082 [https://perma.cc/X59B-S89P] (stating that "elections [are] overseen by about 10,000 different voting jurisdictions across the 50 states.").

[18] *See id.*

[19] *See id.*

[20] *See id.*

[21] *See id.*

cybersecurity standards they require for their voting machines, voter registration systems, pollbooks, post-election vote tabulation, recording, and certification processes,[22] and in the overall regulation of private vendors they employ to provide these functions.[23] The lack of consistent federal funding for election technology upgrades and cybersecurity training leaves the under-resourced states and counties on their own to defend themselves against hostile cyber-attacks, a task too great for many of them.[24] The current system produces a "Swiss cheese" of electoral infrastructure with thousands of potentially vulnerable entry points for hostile actors to target and exploit to the detriment of the entire nation.[25]

A. Funding

There exists today a vast disparity among jurisdictions in the capability to fund improvements for voting machine technology[26]—meaning both the physical machines voters actually use to cast their votes and the software on which those machines run. The modern trend in election administration funding can be traced back to the Help America Vote Act of 2002 (HAVA),[27] which was passed in the

---

[22] *See* Alan Greenblatt, *States Face Challenges on the Road to Better Election Security*, GOV'T TECH. (July 19, 2018), http://www.govtech.com/security/States-Face-Challenges-on-the-Road-to-Better-Election-Security.html [https://perma.cc/S5A8-9CGS]; Lily Hay Newman, *Election Security Is Still Hurting at Every Level*, WIRED (June 6, 2019, 12:01 AM), https://wired.com/story/election-security-2020/ [https://perma.cc/84Q9-KAU7]. *See generally* Danielle Root et al., *Election Security in All 50 States*, CTR. FOR AM. PROGRESS (Feb. 12, 2018, 12:01 AM), https://www.americanprogress.org/issues/democracy/reports/2018/02/12/446336/election-security-50-states/ [https://perma.cc/788K-E47R] (detailing levels of election security in the fifty states).

[23] *See* Greenblatt, *supra* note 22 ("No matter how many steps government officials take to improve their own security efforts, they face potential exposure if they're using vendors whose efforts are more lax.").

[24] On June 18, 2019, a group of twenty-two bipartisan state Attorneys General signed onto a joint letter to Senate leadership imploring Congress to provide more assistance to secure their election systems. The Attorneys General called for increased funding, more cybersecurity training, and federal legislation specifically aimed at bolstering election security, stating "[o]ur state and local election officials are on the front-lines of the fight to protect our election infrastructure, but they lack the resources necessary to combat a sophisticated foreign adversary like Russia." Letter from Keith Ellison, Minn. Att'y Gen., to Chairs of S. Comm. on Appropriations and S. Comm. on Rules and Administration (June 18, 2019), http://www.ag.state.mn.us/Office/Communications/2019/Documents/ElectionSecurityLetter.pdf [https://perma.cc/9KBW-DV4D] [hereinafter Att'ys Gen. Letter to S. Comms.].

[25] Shannon Vavra, *There's More Than One Way to Hack an Election*, AXIOS (July 3, 2018), https://www.axios.com/be-smart-there-is-more-than-one-way-to-hack-an-election-1529424861-1e0c75d9-32b8-4a85-98b3-47d5a853fdeb.html [https://perma.cc/DAH9-QZFJ].

[26] *See* Newman, *supra* note 22.

[27] Pub. L. No. 107-252, 116 Stat. 1666 (codified in scattered sections of 5, 10, 36, 42, and 52 U.S.C. (2012)).

wake of *Bush v. Gore*[28] and its controversy surrounding Florida's punch-card ballots in the 2000 presidential election.[29] Through HAVA, Congress offered states approximately $3.9 billion in federal funds to assist in the administration of federal elections and to upgrade their aging voting equipment with the latest technology in an effort to improve ballot "accuracy and accessibility."[30] With the exception of setting requirements for the types of voting machines that could be acquired, Congress left the states with considerable discretion as to how they could spend their HAVA funds.[31] Congress gave the states four years to spend their HAVA money, after which point any excess funds were to be returned to the federal government.[32] With minimal direction from the federal government and limited time to spend the funds, most states made the short-sighted decision to outright purchase the latest voting machine technology of that time.[33]

Unfortunately, HAVA's one-time, time-pressured grant of funds to the states has had the unintended effect of leaving jurisdictions stuck with their now outdated voting machines purchased with HAVA funds.[34] The few private manufacturers of HAVA compliant voting machines incurred an economic windfall in the form of state procurements which fueled a monopolization of the nearly "$300-million-a-year" industry.[35] Today, eighty percent of the nation's voting machines are under the control of three companies,[36] and the average cost of recent machines falls "between $2,500 and $3,000 each."[37] According to the National Conference of State Legislatures, local "election boards should budget for one machine per every 250 to 300 registered voters,"[38] and the Brennan Center for Justice has estimated that the cost of replacing all of the nation's existing machines would exceed $1 billion.[39]

---

[28] 531 U.S. 98 (2000).

[29] Karyn L. Bass, *Are We Really Over the Hill Yet? The Voting Rights Act at Forty Years: Actual and Constructive Disenfranchisement in the Wake of Election 2000 and* Bush v. Gore, 54 DEPAUL L. REV. 111, 111–14, 153 n.294 (2004).

[30] Brandon Fail, Comment, *HAVA's Unintended Consequences: A Lesson for Next Time*, 116 YALE L.J. 493, 493 n.4, 495 (2006); Kim Zetter, *The Crisis of Election Security*, N.Y. TIMES MAG. (Sept. 26, 2018), https://nyti.ms/2N3hoAh.

[31] *See* Fail, *supra* note 30, at 495–96; Zetter, *supra* note 30.

[32] *See* Help America Vote Act § 102(a)(3)(A)–(B), (d)(1).

[33] Fail, *supra* note 30, at 496–97.

[34] *See id.* at 494.

[35] *See* Zetter, *supra* note 30.

[36] *Id.*

[37] Sarah Breitenbach, *Aging Voting Machines Cost Local, State Governments*, PEW CHARITABLE TRS. (Mar. 2, 2016), https://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2016/03/02/aging-voting-machines-cost-local-state-governments [https://perma.cc/4D6K-9F2Z].

[38] *Id.*

[39] LAWRENCE NORDEN & CHRISTOPHER FAMIGHETTI, BRENNAN CTR. FOR JUSTICE, AMERICA'S VOTING MACHINES AT RISK 17 (2015), https://www.brennancenter.org/publication/americas-voting-machines-risk [https://perma.cc/9N8R-C2FM].

The average lifespan of voting machines is estimated at around ten years, at which point the likelihood of malfunctions and problems with the machines' systems increases.[40] Although experts say the lifespan of voting machines could be extended somewhat with proper maintenance, jurisdictions in forty-three states are using machines that are no longer manufactured, thereby making it increasingly difficult for those areas' election officials to find replacement parts and technicians.[41] Despite the technological risks, jurisdictions in forty-one states used machines purchased more than ten years ago in the 2018 mid-term elections.[42] This prevalence of outdated voting machines is in no way caused by ignorant or dismissive election officials, but rather by the fiscal realities that these state and local jurisdictions face. Officials in thirty-three states have indicated a need to purchase new election machines before 2020, however a majority of those officials have stated that they lack the adequate funding to do so.[43]

The intense decentralization of election administration further complicates this issue, as states vary in their allocation of the funds for election machines and systems. Just under half of the states have in place a "uniform voting system" wherein all voting equipment is purchased and funded at the state level.[44] Such a financing structure posed a viable option back when HAVA funds were readily available, but the dearth of federal funding in the years since HAVA's passage has left many of these states unable to provide the requisite funds now needed to replace outdated equipment.[45] A handful of states split the financial burden; they pay for a portion of their voting equipment with state funds and require counties and local jurisdictions provide the remainder.[46] Finally, some states leave the costs entirely up to local jurisdictions and only provide state funding in the rare instances where newly enacted state laws require certain upgrades to machines.[47]

---

[40] *Id.* at 8.

[41] *Id.* at 9. The Brennan Center for Justice found that nine states are exclusively using discontinued voting machines and thirty-four states are using discontinued voting machines in one or more jurisdictions. LAWRENCE NORDEN & WILFRED U. CODRINGTON, BRENNAN CTR. FOR JUSTICE, AMERICA'S VOTING MACHINES AT RISK—AN UPDATE n.17 (Mar. 8, 2018), https://www.brennancenter.org/analysis/americas-voting-machines-risk-an-update [https://perma.cc/FE2T-GRCY].

[42] NORDEN & CODRINGTON, *supra* note 41.

[43] Wilfred Codrington III & Iris Zhang, *Secure the Vote, Secure Our Democracy*, U.S. NEWS & WORLD REP (Feb. 23, 2018, 2:30 PM), https://www.usnews.com/opinion/thomas-jefferson-street/articles/2018-02-23/congress-must-act-to-upgrade-and-secure-our-voting-machines-before-midterms [https://perma.cc/9MF8-MGWL]; *see also* NORDEN & FAMIGHETTI, *supra* note 39, at 18.

[44] NAT'L CONFERENCE OF STATE LEGISLATURES, THE PRICE OF DEMOCRACY: SPLITTING THE BILL FOR ELECTIONS 12–13 (Feb. 14, 2018), http://www.ncsl.org/research/elections-and-campaigns/the-price-of-democracy-splitting-the-bill-for-elections.aspx [https://perma.cc/TE4G-R84P].

[45] *See id.*

[46] *Id.* at 13.

[47] *Id.*

Lacking adequate funding, those state and local jurisdictions with less financial resources at their disposal are unable to purchase the costly—yet needed—upgrades and maintenance to their election systems. More often, those jurisdictions are forced to divert their limited supply of funds to higher priority items and governmental functions such as infrastructure.[48] These inequities fall disproportionately on less affluent jurisdictions.[49] As such, the voters in these jurisdictions are more prone to voting machine malfunctions, problems on election day, and generally more susceptible to security breaches—flaws which erode the public's confidence in the democratic system.[50]

In March 2018, Congress used HAVA's appropriation authority to allocate an additional $380 million to the states and territories[51] for the purpose of bolstering their election security systems in response to the foreign interference attempts to the 2016 presidential election.[52] Representing the largest batch of federal funding for election infrastructure in over a decade,[53] it took until July 16, 2018, for the entire amount to be requested and distributed to state officials.[54] There can be no doubt that this financial assistance delivered much needed aid to the fiscally strapped state election officials, but many states say that their allocation was not sufficient to make all of the improvements and expenditures necessary to update and secure their election machines and systems statewide.[55]

Although the 2018 federal funds were restricted to certain permitted uses such as replacing outdated voting machines, implementing a post-election audit process, upgrading computer systems to address vulnerabilities, and cybersecurity training for election officials, the specific uses of the funds are once again left to the individual states' discretion.[56] Unfortunately, because most states need to make improvements

---

[48] *See* NORDEN & FAMIGHETTI, *supra* note 39, at 18–19.

[49] *See id.* at 19.

[50] *See id.* at 6–7, 12, 16, 19.

[51] *See* Consolidated Appropriations Act of 2018, Pub. L. No. 115-141, 132 Stat. 348, 561–62 (2018).

[52] *See* SAMUELE DOMINIONI, ITALIAN INST. FOR INT'L POLITICAL STUDIES, PROTECTING ELECTORAL INTEGRITY IN CYBERSPACE: THE U.S. MID-TERM ELECTION IN 2018, at 4 (2018).

[53] Miles Parks, *Bureaucracy and Politics Slow Election Security Funding to States*, NPR (June 18, 2018, 7:28 AM), https://www.npr.org/2018/06/18/617874348/bureaucracy-and-politics-slow-election-security-funding-to-states [https://perma.cc/738Z-Z2B8].

[54] Press Release, U.S. Election Assistance Comm'n, U.S. Election Assistance Commission Announces All Eligible States & Territories Have Requested HAVA Funds, U.S. EAC (July 16, 2018), https://www.eac.gov/news/2018/07/16/us-election-assistance-commission-announces-all-eligible-states-and-territories-have-requested-hava-funds/ [https://perma.cc/BW9Q-3C3X] [hereinafter EAC Press Release].

[55] *See* Eric Geller, *States Slow to Prepare for Hacking Threats*, POLITICO (July 18, 2018, 5:04 AM), https://www.politico.com/story/2018/07/18/hackers-states-elections-upgrades-729054 [https://perma.cc/A25Z-35K2]. Officials in Indiana, Kansas, Nebraska and Texas have all indicated that this most recent round of federal funding was not enough to overhaul their statewide election systems. *Id.*; *see also* Att'ys Gen. Letter to S. Comms., *supra* note 24.

[56] *See* Erin Kelly, *States Will Get at Least $3 Million Each to Improve Election Security*

in many or even all of these areas, the discretionary investments that states choose to make with their limited resources may not go towards addressing the most pressing issues or vulnerabilities in their election systems.[57] For example, of the five states which rely solely on paperless, electronic voting machines—considered by cybersecurity experts to be a top vulnerability in election security—*none* plan on using the funds to purchase new, more secure voting equipment like those with paper ballot trails.[58] Simply being awarded federal funding does not signify a remedy to a state's problems either, as the issue of election security and the disbursement of federal funds in some jurisdictions has been stalled by intrastate political squabbles.[59]

B. Cybersecurity

Nearly every step in the electoral process is now done, at least partially, through digital means—making voter registration databases, pollbooks used to check in voters on election day, voting machine software, vote tabulation software, and the final verification and online reporting of election results all potential targets for hackers.[60] Much like with funding, the heavily decentralized system means that state and local jurisdictions vary widely in the minimum cybersecurity standards and requirements imposed on their election machines, election systems, and the vendors who provide them.[61] As the 2018 mid-term elections have demonstrated, the threat of interference from hostile foreign actors, beyond just Russia, continues to loom over the U.S. democratic process,[62] and the overwhelming consensus of cybersecurity experts is that state election systems remain vulnerable.[63] Though reluctant at first, state and

---

Under Spending Deal, USA TODAY (Mar. 22, 2018, 2:09 PM), https://www.usatoday.com/story/news/politics/2018/03/22/states-get-least-3-million-each-improve-election-security-under-spending-deal/449562002/ [https://perma.cc/QF9W-STJU].

[57] *See* Geller, *supra* note 55.

[58] *Id.*

[59] *See* Parks, *supra* note 53.

[60] *See* Scott J. Shackelford et al., *Making Democracy Harder to Hack*, 50 U. MICH. J.L. REFORM 629, 636 (2017). *See generally* Derek Hawkins, *The Cybersecurity 202: We Surveyed 100 Security Experts. Almost All Said State Election Systems Were Vulnerable*, WASH. POST (May 21, 2018), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/05/21/the-cybersecurity-202-we-surveyed-100-security-experts-almost-all-said-state-election-systems-were-vulnerable/5b0189b030fb0425887995e2/ [https://perma.cc/YCH5-ZSPP] (surveying voter systems and their weaknesses throughout the country).

[61] *See Voting System Standards, Testing and Certification*, NAT'L CONFERENCE OF STATE LEGISLATURES (Aug. 6, 2018), http://www.ncsl.org/research/elections-and-campaigns/voting-system-standards-testing-and-certification.aspx [https://perma.cc/9786-QAKE] [hereinafter *Standards, Testing & Certification*].

[62] *See* Dan Patterson, *These Are the Hackers Targeting the Midterm Election*, CBS NEWS (Oct. 10, 2018, 10:50 AM), https://www.cbsnews.com/news/these-are-the-hackers-targeting-the-midterm-election/ [https://perma.cc/CY6M-ERN2]; *see also* Joint Statement, *supra* note 7.

[63] *See* Hawkins, *supra* note 60.

local election officials are increasingly taking note of the serious danger facing them;[64] some experts, however, believe "the magnitude of the threats from state-sponsored adversaries is too great for states to deal with alone."[65]

1. Voting Machines

As the nation's voting machines remain in service beyond their lifespans, they become not only more prone to malfunctioning,[66] but also more susceptible to cyber-attacks.[67] Many older voting machines, including those purchased with the original HAVA grants, run on outdated and unsupported software like Windows 2000 that, in addition to no longer receiving security patches,[68] is itself more vulnerable to the latest forms of hacking.[69] Notwithstanding the fact that voting machines are supposed to be disconnected from the internet, in order to load software and ballot definitions the machines need to connect with an election management computer, which *can* be connected to the internet.[70] Through this proxy, a hacker could potentially corrupt a single voting machine that, because voting machines connect locally and exchange information through memory cards, could then allow an experienced nation-state actor to corrupt an entire jurisdiction's machines.[71]

Although the likelihood of such an intricate and sophisticated hacking attempt actually occurring, let alone succeeding, might seem remote, there is ample evidence of states failing to address—or even identify—far less complex vulnerabilities in their voting machines' security that would be much easier to exploit.[72] For instance, in 2014, the Virginia State Board of Elections learned that twenty percent of their precincts' voting machines were in fact equipped with wireless network capabilities to allow ballot programming and voter data to be transmitted between machines.[73]

---

[64] *See* Miles Parks, *Will Your Vote Be Vulnerable on Election Day?*, NPR (May 8, 2018, 5:00 AM), https://www.npr.org/2018/05/08/599452050/the-u-s-voting-system-remains-vulnerable-6-months-before-election-day-what-now [https://perma.cc/QF4C-VCWE].

[65] Hawkins, *supra* note 60.

[66] NORDEN & FAMIGHETTI, *supra* note 39, at 12.

[67] *Voting System Security and Reliability Risks*, BRENNAN CTR. FOR JUSTICE (Aug. 30, 2016), https://www.brennancenter.org/analysis/fact-sheet-voting-system-security-and-reliability-risks [https://perma.cc/US4T-6379].

[68] NORDEN & CODRINGTON, *supra* note 41.

[69] *See* Alex Hern, *WannaCry Attacks Prompt Microsoft to Release Windows Updates for Older Versions*, GUARDIAN (June 14, 2017, 7:26 AM), https://www.theguardian.com/technology/2017/jun/14/wannacry-attacks-prompt-microsoft-to-release-updates-for-older-windows-versions [https://perma.cc/AKH5-RRXV].

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

[71] *See id.*

[72] *See* Newman, *supra* note 22.

[73] *See* Pam Fessler, *Vulnerable Voting Machine Raises Questions About Election Security*,

The machine's network capabilities were discovered *on Election Day* and only after one county's poll workers became concerned when their machines repeatedly crashed.[74] State auditors investigating the machines eventually learned that *anyone* nearby could easily access the voting machines' network with their smartphones—the password was "abcde"—offering access to see and edit the lists of candidates available, the number actual votes cast, and the final totals recorded, among other things.[75]

The most effective security measure against older voting machines being hacked is the creation of a paper ballot trail recording the voter's choices that can later be used to verify the accuracy of the votes entered and recorded on the machine's computer.[76] And yet, despite years of federal officials and cybersecurity experts advising otherwise,[77] in the 2018 election, thirteen states used paperless electronic voting machines as their primary voting equipment in at least some of their local jurisdictions.[78] Five of those states continue to use paperless voting machines in *all* of their state polling locations.[79] The principle utility of having paper ballots to supplement electronic voting machines is that it allows officials to conduct post-election audits of machines to verify the accuracy of the software-generated final vote tally.[80] Specifically, "risk limiting audits," a process which uses statistical models to consistently provide a high level of confidence in final tabulation results, is considered by experts to be the "'gold standard' of post-election audits"[81] and has been specifically recommended by the Senate Intelligence Committee.[82] Once again, contrary to expert opinion and congress's recommendation, only three states require risk limiting audits for their voting equipment.[83] Without paper ballots to conduct these audits regularly, it is possible that hacking attempts or errors in the voting machine's software will go unnoticed by state and local election officials.[84] As America's voting machines continue to age and the prevalence of machine malfunctions rises,[85] these audits become

---

NPR (Apr. 16, 2015, 5:03 AM), https://www.npr.org/sections/itsallpolitics/2015/04/16/399986331/hacked-touchscreen-voting-machine-raises-questions-about-election-security [https://perma.cc/UUE6-QWQJ].

[74] *Id.*

[75] *Id.*

[76] *See* NORDEN & CODRINGTON, *supra* note 41.

[77] *See* Zaid Jilani, *Amid Election Security Worries, Suddenly Paper Ballots Are Making a Comeback*, INTERCEPT (Feb. 18, 2018, 6:56 AM), https://theintercept.com/2018/02/18/paper-ballots-amidst-election-security-worries-suddenly-paper-ballots-are-making-a-comeback/ [https://perma.cc/GV7H-GJ99].

[78] NORDEN & CODRINGTON, *supra* note 41.

[79] *Id.*

[80] *Id.*

[81] *Id.*

[82] *See* S. REP. SUMMARY ON RUSSIAN TARGETING, *supra* note 8.

[83] NORDEN & CODRINGTON, *supra* note 41.

[84] *Id.*

[85] NORDEN & FAMIGHETTI, *supra* note 39, at 12.

only more imperative as even small instances of malfunction, whether external or internal in origin, can change the outcome of a race.[86]

Demonstrative of the issues that the absence of a paper trail can cause is the 2006 election in Florida's 13th Congressional district, where fifteen percent of the ballots cast in said district did not register a vote in that race—one of the most vehemently contested races that year.[87] It is highly unlikely that roughly 18,000 voters chose not to record a vote in only that race, given the statistical significance of under votes in the affected area was nearly thirteen percent higher than in other counties.[88] Unfortunately, due to the absence of paper ballots to verify the final electronic vote tabulation, it will remain unknown whether the undervotes were in fact an accurate reflection of the 18,000 voters' preferences or were instead the result of a software malfunction with the machines themselves.[89] Out of more than 238,000 votes in that district, the winner of that race won by a margin of only 369 votes.[90]

2. Voter Registration Databases & Election Websites

Considered by many experts to be the most vulnerable targets for hackers are voter registration systems and databases.[91] Although not directly tied to the votes cast or to the election results, these systems tell election officials who can vote, identify registered voters and are overall crucial to an efficient operation on election day.[92] HAVA required states to create and maintain computerized voter registration lists,[93] and so these "back end" systems used by states and counties are almost entirely digital and connected to the internet, either directly or indirectly.[94] HAVA also required states to "provide adequate technological security measures to prevent the unauthorized access to the computerized list[s]," but it did not require the EAC to develop specific technological and security standards for those systems.[95] Therefore, it was left to state and local jurisdictions to develop sufficient security measures for protecting their databases, many of whom have further delegated these responsibilities to private vendors. Unfortunately, many states and their affiliated private vendors

---

[86] *See* Root et al., *supra* note 22.

[87] *See* David Jefferson, *What Happened in Sarasota County?*, THE BRIDGE, Summer 2007, at 17.

[88] *Id.* at 18–19.

[89] *See id.* at 17.

[90] *Id.*

[91] *See* Hawkins, *supra* note 60; Parks, *supra* note 64.

[92] *See* LAWRENCE NORDEN & IAN VANDEWALKER, BRENNAN CTR. FOR JUSTICE, SECURING ELECTIONS FROM FOREIGN INTERFERENCE 14 (June 29, 2017), https://www.brennancenter.org/sites/default/files/publications/Securing_Elections_From_Foreign_Interference.pdf [https://perma.cc/6MPZ-Y6SD].

[93] Help America Vote Act of 2002, Pub. L. No. 107-252, § 303(a)(1)(A), 116 Stat. 1666, 1708 (codified at 52 U.S.C. § 21083(a)(1)(A) (2012)).

[94] *See* Hawkins, *supra* note 60.

[95] Help America Vote Act § 303(a)(3) (codified at 52 U.S.C. § 21083(a)(3) (2012)).

have failed to adequately secure their systems—leaving the door open for hostile foreign actors to take advantage.[96]

In 2016, the Russian military-backed hackers successfully infiltrated Illinois's statewide voter registration system, giving them access to Illinois voter files for *nearly three weeks* before they were detected after trying to alter or delete records in the database.[97] Although not confirmed, it is believed that Illinois is the unnamed state mentioned in an indictment filed by Special Counsel Robert Mueller as part of his investigation into the 2016 election interference[98] that alleged hackers were able to steal information including names, addresses, partial Social Security numbers, and driver's license numbers of 500,000 voters.[99]

This danger is not reserved to the state level nor is it unique to hostile foreign actors. In Arizona, hackers were successfully able to install malware on a county election official's computer when he opened a fraudulent email attachment.[100] Through that computer the hackers were able to obtain the county official's username and password which could then be used to access the county voting registration system.[101] Initially, the hackers in Arizona were widely believed to be a part of the Russian interference campaign;[102] however, it was later discovered that these hackers were not state-sponsored actors, but criminal actors nonetheless.[103]

Voter registration databases are not the only vulnerable targets in the nation's election infrastructure. Many states' election websites also lack sufficient cybersecurity measures to ward off threats from far less sophisticated actors than a hostile nation-state.[104] State election websites are the public's window into the election and the official source of the election's results. Therefore, a successful attack on these sites

---

[96] *See* NORDEN & VANDEWALKER, *supra* note 92, at 15.

[97] *Id.* at 15.

[98] Indictment at 26, United States v. Netyksho, No. 1:18-cr-00215-ABJ (D.C. Cir. July 13, 2018), ECF No. 1.

[99] *See id.*; Martin Matishak, *What We Know About Russia's Election Hacking*, POLITICO (July 18, 2018, 8:54 PM), https://www.politico.com/story/2018/07/18/russia-election-hacking-trump-putin-698087 [https://perma.cc/E768-T55A].

[100] NORDEN & VANDEWALKER, *supra* note 92, at 15.

[101] *Id.*

[102] *See* Sari Horwitz et al., *DHS Tells States About Russian Hacking During 2016 Election*, WASH. POST (Sept. 22, 2017), https://www.washingtonpost.com/world/national-security/dhs-tells-states-about-russian-hacking-during-2016-election/2017/09/22/fd263a2c-9fe2-11e7-8ea1-ed975285475e_story.html [https://perma.cc/LR8V-UD4L].

[103] Dustin Volz, *Arizona Election Database Targeted in 2016 by Criminals, Not Russia: Source*, REUTERS (Apr. 8, 2018, 7:42 PM), https://www.reuters.com/article/us-usa-cyber-election/arizona-election-database-targeted-in-2016-by-criminals-not-russia-source-idUSKBN1HF11F [https://perma.cc/TAY5-XBGN].

[104] *See* Jonathan Shieber, *Hacking the Websites Responsible for Election Information Is So Easy an 11-Year-Old Did It*, TECHCRUNCH (Aug. 12, 2018), https://techcrunch.com/2018/08/12/hacking-the-websites-responsible-for-election-information-is-so-easy-an-11-year-old-did-it/ [https://perma.cc/Q2ZK-C2CK].

could be just as damaging to voters' trust in the election as a hack on the election systems themselves.[105] At least six states had their elections websites targeted by Russian hackers leading up to the 2016 presidential election.[106] In Tennessee, hackers successfully breached the State's election website at the time the site was supposed to begin posting election results, ultimately requiring officials to shut down the site for repair, preventing voters from seeing the races' outcomes.[107]

Demonstrative of state and local election officials' lack of expertise and resources to face cybersecurity threats is that most state officials were entirely unaware of the Russian hacking attempts on their systems for nearly a year.[108] All fifty states had to rely on the federal Department of Homeland Security to notify them if they were involved in the string of cyber-attacks,[109] and even after notification, the scope of information divulged to state officials and their ability to share those details with others remain limited.[110] The reality is that the majority of state and local election officials lack the resources to prepare for, identify, and respond to cybersecurity threats.[111] When considered in the context of cyber-attacks organized and supported by a sophisticated foreign intelligence operation like Russia's, the logical conclusion is that, as one former National Security Agency security scientist stated, "[p]rotecting systems from cyberthreats from nation-states can really only be done on a national level. It's insane we have state-level control of these systems."[112]

II. FEDERAL AUTHORITY TO REGULATE ELECTION ADMINISTRATION & SECURITY

Undoubtedly, Congress has the constitutional authority to adopt a more involved and stringent regulatory stance towards assisting and overseeing state election administration. Article I, Section 4, Clause 1 of the U.S. Constitution, popularly known

---

[105] *See* Miles Parks, *6 States Hit Harder by Cyberattacks than Previously Known, New Report Reveals*, NPR (May 10, 2018, 2:51 PM), https://www.npr.org/2018/05/10/609744800/six-states-hit-harder-by-cyberattacks-than-previously-known-new-report-reveals [https://perma.cc/A2PL-UNDD].

[106] S. REP. SUMMARY ON RUSSIAN TARGETING, *supra* note 8, at 3.

[107] Miles Parks, *Not Just Ballots: Tennessee Hack Shows Election Websites Are Vulnerable, Too*, NPR (May 17, 2018, 4:56 AM), https://www.npr.org/2018/05/17/611869599/not-just-ballots-tennessee-hack-shows-election-websites-are-vulnerable-too [https://perma.cc/F8UP-S45M].

[108] *See* Horwitz et al., *supra* note 102.

[109] *See id.*

[110] *See* Gary Fineout, *Russians Hacked 2 Florida Voting Systems; FBI and Desantis Refuse to Release Details*, POLITICO (May 14, 2019, 1:32 PM), https://www.politico.com/states/florida/story/2019/05/14/russians-hacked-2-florida-voting-systems-fbi-and-desantis-refuse-to-release-details-1015772 [https://perma.cc/79TM-79DC] (reporting that the FBI required the governor of Florida to sign a nondisclosure agreement regarding the extent and targets of Russian hacking operations against the state).

[111] *See* Likhitha Butchireddygari, *Many County Election Officials Still Lack Cybersecurity Training*, NBC NEWS (Aug. 23, 2017, 5:20 AM), https://www.nbcnews.com/politics/national-security/voting-prep-n790256 [https://perma.cc/PX8W-RCJE]; Hawkins, *supra* note 60.

[112] Hawkins, *supra* note 60.

as the Elections Clause, initially vests in the state legislatures the responsibility to prescribe laws regulating the "Times, Places and Manner" of federal elections.[113] However, the Elections Clause also explicitly reserves to Congress the right to "make or alter such Regulations"[114] at any time, with it being "well settled" that state laws concerning the mechanics of federal elections are operative only so far as Congress has declined to pre-empt them with their own regulatory scheme.[115] Indeed, Congress has successfully invoked this authority to enact pre-emptory election laws and regulations dealing with voter registration,[116] absentee ballots,[117] campaign finance,[118] and voting rights protections.[119] In each of these instances, the Court has held these laws to be valid exercises of Congress's authority under the Elections Clause and that such laws control over a conflicting state law.[120]

The idea of the federal government becoming more involved in the funding and oversight of matters relating to election administration is by no means far-fetched, given that Congress has already interposed itself into this area. In 1993, Congress enacted the National Voter Registration Act (NVRA)[121] which was designed to simplify and improve the voter registration process by shifting many of the burdens of registration from the citizens to the states themselves.[122] The NVRA required states to provide prospective voters with, at minimum, three different opportunities to register using federally created registration forms,[123] established procedural safeguards to govern states' maintenance of their voter registration lists,[124] and provided

---

[113] U.S. CONST. art. I, § 4, cl. 1.

[114] *Id.*

[115] Foster v. Love, 522 U.S. 67, 69 (1997); *see also* U.S. Term Limits, Inc. v. Thornton, 514 U.S. 779, 832–33 (1995); Roudebush v. Hartke, 405 U.S. 15, 24 (1972).

[116] *See* National Voter Registration Act of 1993, Pub. L. No. 103-31, 107 Stat. 77 (1993).

[117] *See* Uniformed and Overseas Citizens Absentee Voting Act, Pub. L. No. 99-410, 100 Stat. 924 (1986).

[118] *See* Bipartisan Campaign Reform Act of 2002, Pub. L. No. 107-155, 116 Stat. 81 (2002).

[119] *See* Voting Rights Act of 1965, Pub. L. No. 89-110, 79 Stat. 437 (1965).

[120] *See* Arizona v. Inter Tribal Council of Ariz., Inc., 570 U.S. 1 (2013) (holding the National Voter Registration Act of 1993 to be a valid exercise of Congress's authority under the Elections Clause that mandated Arizona to use the federal voter registration form); McConnell v. FEC, 540 U.S. 93 (2003) (holding the campaign contribution provisions of the Bipartisan Campaign Reform Act of 2002 to be a valid exercise of Congress's authority under the Elections Clause regardless of its prohibitory effect on conflicting state laws).

[121] National Voter Registration Act of 1993 (NVRA), Pub. L. No. 103-31, 107 Stat. 77 (codified as amended at 52 U.S.C.A. §§ 20501–20511 (2012 & Supp. II 2015)).

[122] *See generally* Kevin K. Green, Note, *A Vote Properly Cast? The Constitutionality of the National Voter Registration Act of 1993*, 22 J. LEGIS. 45 (1996) (discussing the history and implications of the NVRA).

[123] 52 U.S.C.A. §§ 20503–20508 (requiring states to allow prospective voters the opportunity to register to vote for federal elections at the time they apply for a driver's license, in person, or by mail).

[124] *Id.* § 20507.

for civil enforcement of the Act's provisions.[125] As a response to the *Bush v. Gore* controversy, Congress enacted the Help America Vote Act (HAVA) in 2002, a comprehensive statutory framework designed to fund, update, and reform the nation's election administration processes.[126] Among HAVA's mandates were that states use the federal funds to implement and maintain computerized statewide voter registration lists[127] and, most importantly for the purposes of this argument, that states upgrade their voting systems, technology and software that voters use in conformance with various federal requirements.[128]

The Court's approval of laws like the NVRA and HAVA have made clear that the federal government has a valid interest in the proper administration of federal elections, however the current system creates significant obstacles to federal efforts to secure future elections from foreign interference. As the primary administrators of elections, states are under no obligation to monitor and report cyber-attacks or issues in their election systems to the federal government.[129] Both Congress and the executive agencies depend on states to voluntarily provide information on matters of election security, and due to the complexities of cyber-forensic analysis in which many state officials lack sufficient training, there is a real possibility that states have or could fail to identify evidence of cyber-attacks, whether attempted or successful.[130] This overdependence on states to self-report failures in their own systems impedes efforts to ascertain a comprehensive and accurate estimate of the nation's election infrastructure security.[131] Federal officials' concern that states may choose not to inform them upon discovery of security breaches or vulnerabilities is not unwarranted,[132] and that fear in turn has a chilling effect on the willingness of federal agencies to share information they have received with Congress and the public.[133]

In addition to providing funding to the states, HAVA created the Election Assistance Commission (EAC), an independent, bipartisan federal agency dedicated

---

[125] *Id.* §§ 20510–20511.

[126] *See* Help America Vote Act of 2002, Pub. L. No. 107-252, 116 Stat. 1666 (codified in scattered sections of 5, 10, 36, 42, and 52 U.S.C. (2012)).

[127] *Id.* § 303(a)(1), 116 Stat. at 1708–09 (recodified at 52 U.S.C. § 21082(a)).

[128] *Id.* § 303(a), 116 Stat. at 1704–05 (recodified at 52 U.S.C. § 21081).

[129] *See Election Security: Hearing Before the S. Select Comm. on Intelligence*, 115th Cong. 10 (Mar. 21, 2018) (statement of Kirstjen Nielsen, Sec.'y, Dept. of Homeland Sec.) [hereinafter *S. Hearing on Election Security*].

[130] *See id.* at 26; S. REP. SUMMARY ON RUSSIAN TARGETING, *supra* note 8.

[131] *See S. Hearing on Election Security*, *supra* note 129, at 28–29; S. REP. SUMMARY ON RUSSIAN TARGETING, *supra* note 8.

[132] Gary Fineout, *Reports of Election Site Hacking Rankle Florida Officials*, ASSOCIATED PRESS (Aug. 13, 2018), https://www.apnews.com/e298a5e7f25847dda4b67ea1b49d0189 [https://perma.cc/6URT-ZS58]; Nathaniel Herz, *Hackers Broke Partway into Alaska's Election System in 2016. Officials Say No Damage Was Done*, ANCHORAGE DAILY NEWS (May 7, 2018), https://www.adn.com/politics/2018/05/07/hackers-broke-partway-into-alaskas-election-system-in-2016-officials-say-no-damage-was-done/#_ [https://perma.cc/QRG3-Z569].

[133] *S. Hearing on Election Security*, *supra* note 129, at 26.

to establishing election security and technology standards and providing assistance to the states.[134] The EAC promulgates Voluntary Voting System Guidelines (VVSG) outlining specifications to test state voting systems for security, functionality, privacy, usability, and accessibility.[135] Additionally, voting systems and machines can be tested through a federally accredited Voting Systems Test Laboratory (VSTL) to certify that they comply with the various federal standards promulgated by the EAC.[136] Hindering the EAC's ability to bolster election security is the fact that, due to the states' primary role in election administration, the EAC's standards and certifications are entirely voluntary.[137] States, and in some jurisdictions, counties, ultimately set the standards for their voting equipment and often these state and local jurisdictions' requirements fall below the level that cybersecurity experts recommend.[138]

Currently, thirty-eight states and Washington D.C. use some aspect of the federal testing and certification program in addition to state-specific testing and certification of systems.[139] Nine states and Washington D.C. require testing to federal standards, seventeen states require testing by a federally accredited lab, and twelve states require full federal certification for their voting systems.[140] This leaves eight states with no federal testing or certification requirements for their voting machines.[141] Even more disconcerting is the fact that many of the voting machines currently in use that were purchased with HAVA funds fail to meet even HAVA's security standards.[142] Despite HAVA mandating that security standards be promulgated delineating the permissible voting machines that could be bought with the Act's funds, those final standards were not issued until 2005 and did not take effect until 2007—well after most states had already bought their current machines due to the Act's purchasing deadlines.[143]

Further complicating nationwide election security is that even when federal cybersecurity assistance is made available, some states fail to utilize the resources despite it being in the best interest of the state. Amid a flurry of reports detailing state-sponsored cyber-attacks aimed at election systems and political parties in the months leading up to the 2016 election, the Department of Homeland Security

---

[134] The EAC is an "independent bipartisan commission charged with developing guidance to meet HAVA requirements, adopting voluntary voting system guidelines, and serving as a national clearinghouse of information on election administration. The EAC also accredits testing laboratories and certifies voting systems, as well as audits the use of HAVA funds." U.S. ELECTION ASSISTANCE COMM'N, ABOUT THE EAC, https://www.eac.gov/about-the-us eac/ [https://perma.cc/69JK-N7P7].

[135] *See Standards, Testing & Certification*, *supra* note 61.

[136] *See id.*

[137] *See id.*

[138] *See* Hawkins, *supra* note 60; Root et al., *supra* note 22.

[139] *Standards, Testing & Certification*, *supra* note 61.

[140] *Id.*

[141] *Id.*

[142] *See* Zetter, *supra* note 30.

[143] *Id.*

offered states free assistance to help examine and bolster their cybersecurity defenses.[144] This offer to state and local officials included a variety of "cyber hygiene" scans and on-site inspections aimed at assessing vulnerabilities in voter registration and election systems.[145] Nevertheless, eleven states rejected the offer fearing a potential "federal takeover of elections," notwithstanding the explicit assurances from DHS that the services would bring no form of regulation or binding mandates.[146]

One of those states to reject federal election security assistance was Georgia,[147] which, despite having experienced multiple breaches of state systems containing voter records,[148] repeated its denial of federal assistance in the months leading up to the 2018 mid-term elections.[149] As it would turn out, only months after proclaiming the sufficiency of the state's election security measures, Georgia's Secretary of State Brian Kemp would allege that the state's election systems were again breached—this time by his opponent in the gubernatorial race.[150]

The NVRA and HAVA remain in force today and, although sparsely used, can serve as the conduit through which the federal government, in conjunction with the Election Assistance Commission, can easily appropriate and disburse federal funding to assist the states with election administration and establish minimal cybersecurity standards and reporting requirements.[151] The most recent round of federal funding in 2018 and the EAC's ongoing efforts in this area illustrate that the necessary mechanisms for the federal government to take a more prominent role over election security are already established. In order to ensure the nation's elections are truly secure, the federal government needs to utilize these tools in a manner that is more consistent and less discretionary, thereby relieving the states from the weighty and disproportionate burdens that combating hostile foreign actors entails.

Currently, most observers assume that the federal government's role in election administration is derived solely from the Elections Clause. Under the text's explicit command, Congress has the option to pre-empt state election laws and impose its own

---

[144] Alex Tin, *Ahead of Elections, States Reject Federal Help to Combat Hackers*, CBS NEWS (Oct. 28, 2016, 5:01 PM), https://www.cbsnews.com/news/ahead-of-elections-states-reject-federal-help-to-combat-hackers/ [https://perma.cc/M3T5-P48V].

[145] *Id.*

[146] *Id.*

[147] *Id.*

[148] Kristina Torres, *As Many as 7.5 Million Voter Records Involved in Georgia Data Breach*, ATLANTA JOURNAL-CONSTITUTION (Mar. 3, 2017), https://www.ajc.com/news/state--regional-govt--politics/many-million-voter-records-involved-georgia-data-breach/rU2bMMc3tzGkuPvmbjlkgJ/ [https://perma.cc/44CU-JTJ2].

[149] Johnny Kauffman, *Election Security Becomes a Political Issue in Georgia Governor's Race*, NPR (Aug. 12, 2018, 5:00 AM), https://www.npr.org/2018/08/12/637163104/election-security-becomes-a-political-issue-in-georgia-governors-race [https://perma.cc/3QT2-78CU].

[150] Richard Fausset & Alan Blinder, *Brian Kemp's Office, Without Citing Evidence, Investigates Georgia Democrats Over Alleged 'Hack*,*'* N.Y. TIMES (Nov. 4, 2018), https://nyti.ms/2yRYw2Z.

[151] *See* EAC Press Release, *supra* note 54; Kelly, *supra* note 56.

requirements or procedures for federal election administration if it so desires. Beyond this discretionary constitutional prerogative, however, there lies another provision in the Constitution whose commands are not optional but rather are obligatory. In a time where hostile foreign powers are attempting to intrude upon and interfere in the country's most fundamental and sovereign activities, an oft-forgotten clause in the Constitution not only permits Congress to act for the nation's defense, but it requires it to do so.

III. CONSTITUTIONAL DUTY TO PROTECT STATE ELECTION SYSTEMS FROM CYBER-INVASION

Article IV, Section 4 of the U.S. Constitution states in part: "The United States shall guarantee to every State in this Union a Republican Form of Government, and *shall protect each of them against Invasion* . . . ."[152] These two clauses, commonly referred to as the Guarantee Clause and the Protection Clause, respectively, impose two distinct yet interrelated obligations on the federal government—to ensure that every state will have a republican government and to protect every state from threats of invasion.[153] Ongoing attempts by foreign actors to attack and interfere in the U.S. electoral process are unique in that they implicate and pose a direct threat to both of these constitutional guarantees. Election systems are the vehicles through which the states conduct and maintain their republican forms of government.[154] When a hostile foreign actor launches a cyber-attack on state electoral systems and infrastructure, it should be recognized for what it is—a direct intrusion into one of the most crucial spheres of state sovereignty and an attack on the states themselves. The states in the Union are on the front lines in a new era of warfare in which cyberspace is the battlefield, and by leaving the states to fend for themselves, the federal government is failing to meet its constitutional duties under the Guarantee and Protection Clauses.

A. Cyber-"Invasion"

Undoubtedly, when the Framers originally used the term "invasion" in the Protection Clause they were speaking about a foreign power's physical intrusion into a state's geographical territory.[155] It is only natural that the Framers' conception of the term would reflect the technology and modes of warfare that existed in the 18th

---

[152] U.S. CONST. art. IV, § 4 (emphasis added).

[153] Jason Mazzone, *The Security Constitution*, 53 UCLA L. REV. 29, 55–56 (2005).

[154] *See, e.g.*, THE FEDERALIST NO. 68, at 459 (Alexander Hamilton) (Jacob E. Cooke ed., 1961). Concerning the election of a president, Hamilton wrote: "Nothing has to be more desired than that every practicable obstacle should be opposed to cabal, intrigue, and corruption. These most deadly adversaries of republican government might naturally have been expected to make their approaches from more than one quarter, but chiefly in the desire in foreign powers to gain an improper ascendant in our councils." *Id.*

[155] *See* Mazzone, *supra* note 153, at 55.

century. However, the world has experienced monumental advances in technology since then that even the Framers could not have foreseen, and those developments have completely transformed the traditional notions of warfare and state sovereignty. Both the U.S. and the international community continue to struggle with how best to characterize, prepare for, and respond to foreign cyber threats.[156] Despite this uncertainty, in recent years, there has emerged some general consensus as to the role of cyberspace within the international community and the authority that sovereign states possess over their own cyber domains.[157] As the following principles will suggest, a modern interpretation of the term "invasion" as it is used in Article IV, Section 4 should be understood to include cyber-attacks and intrusions into the United States' election systems and infrastructure.

First, states retain full sovereignty over the cyberspaces and cyber infrastructures that are located within their territory, thereby enjoying the same rights of self-defense as that of the air, land, and sea.[158] This fundamental notion of cyber sovereignty and the application of international legal principles to cyberspace has been fully recognized by the United Nations,[159] NATO,[160] and the United States government.[161] Beyond the right to act in self-defense, the modern conception of state sovereignty is fundamental within the international community and consequently is understood to encompass a much broader penumbra of rights and obligations. As stated by the International Court of Justice in 1986, "[b]etween independent States, respect for territorial sovereignty is an essential foundation of international relations."[162] In international relations, sovereignty signifies independence, and "[i]ndependence in regard to a portion of the globe is the right to exercise therein, to the exclusion of any other State, the functions of a State."[163]

Cyber-operations against another state's infrastructure could constitute a violation of the target state's sovereignty, regardless of whether that infrastructure is

---

[156] *See* THE WHITE HOUSE, U.S. NAT'L SEC. STRATEGY 12–13 (2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf [https://perma.cc/GK9S-FZHB]; Catherine Lotrionte, *State Sovereignty & Self-Defense in Cyberspace: A Normative Framework for Balancing Legal Rights*, 26 EMORY INT'L L. REV. 825, 828 (2012).

[157] *See* Lotrionte, *supra* note 156, at 831.

[158] *See id.* at 829.

[159] *See* Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. & Telecomms. in the Context of Int'l Sec., 70th Sess., at 12–13, U.N. Doc. A/70/174 (2015). Established pursuant to paragraph 4 of General Assembly Resolution 68/243; *see also* Lotrionte, *supra* note 156, at 828.

[160] *See* TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE 23–29 (Michael N. Schmitt ed. 2013) [hereinafter TALLINN MANUAL].

[161] *See generally* THE WHITE HOUSE, NAT'L CYBER STRATEGY (2018), https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf [https://perma.cc/7CAS-3E4L].

[162] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 202 (June 27).

[163] Island of Palmas (Neth. v. U.S.), 2 R.I.A.A. 829, 838 (Perm. Ct. Arb. 1928).

physical or cyber in nature.[164] Additionally, a cyber-operation could constitute an "intervention," a "use of force," or an "armed attack" depending on its purpose, target, and severity.[165] In a report on the international law of cyber warfare, NATO made clear its view that cyber-attacks which result in damage undoubtedly violate the target state's sovereignty.[166] However, in that same report, NATO was unable to reach a conclusion as to whether strictly non-damaging cyber-attacks, such as the installation of malware for monitoring purposes, would constitute a violation of state sovereignty.[167] The fact that the 2016 cyber-attacks were primarily aimed at infiltrating and installing malware on various state election systems for intelligence purposes makes classifying them within the still developing international legal framework difficult. Nevertheless, when one looks beyond solely the means employed in the election related hacking attempts and considers their purpose, scope, and impact as a whole, it is entirely reasonable to conclude that they and any future attacks of a similar nature constitute a violation of the United States' sovereignty.

In 2017, the Department of Homeland Security classified U.S. voter registration and voting systems as "critical infrastructure."[168] This designation reflects the vitally important role that electoral infrastructure plays in the country's security and, despite carrying no regulatory authority in itself, rightfully positions the federal government to take a more proactive stance in their protection.[169] This heightened role was reaffirmed in a May 2017 executive order stating that it is the executive branch's policy "to use its authorities and capabilities to support the cybersecurity risk management efforts of the owners and operators of the Nation's critical infrastructure," to guard the nation's internet against "disruption, fraud and theft," to "deter[ ] adversaries," and to "better protect[ ] the American people from cyber threats."[170]

The nation's election systems exist fully within the United States' territorial boundaries and, as such, the U.S. has the sovereign authority to protect and restrict them from being accessed by individuals outside the nation's borders.[171] The fact that

---

[164] *See* TALLINN MANUAL, *supra* note 160, at 25.

[165] *See* Nicar. v. U.S., 1986 I.C.J. ¶ 195; *see also* TALLINN MANUAL, *supra* note 160, at 16–17.

[166] TALLINN MANUAL, *supra* note 160, at 16.

[167] *See id.*

[168] Press Release, Jeh Johnson, Secretary, Dep't. of Homeland Sec., 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 [https://perma.cc/2CWP-2GJJ]. Critical Infrastructure designations are given to "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Critical Infrastructures Protection Act of 2001, Pub. L. No. 107-56, § 1016(e0, 115 Stat. 272, 400 (recodified at 42 U.S.C. § 5195c(e) (2012)).

[169] *See* Manpearl, *supra* note 70, at 183–87.

[170] Exec. Order No. 13800, 82 Fed. Reg. 22391 (May 11, 2017).

[171] *See id.*

some states' election systems are operated or controlled by private vendors has no bearing on this determination, as state sovereignty protects cyber infrastructure belonging to the government and private entities alike.[172] Similarly, while traditional violations of sovereignty were seen as limited to actions undertaken by, or attributable to, state actors, the modern view is that even cyber-operations conducted by non-state actors may also violate a state's territorial sovereignty.[173] According to the International Law Commission Articles on Responsibility of States for Intentionally Wrongful Acts of 2001, "[t]he conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct."[174]

Illustrative of the complexities and dangers that state-sponsored cyber-attacks pose to existing notions of warfare, state sovereignty, and international law is the 2014 hacking of Sony Pictures Entertainment Inc. (Sony), which the FBI concluded to have been orchestrated by the North Korean government.[175] Angered by the U.S.-based entertainment company's production and upcoming release of the film *The Interview*, a comedy based around a fictitious plot to assassinate North Korean leader Kim Jong Un, the North Korean government made clear to the U.S. and the international community that they viewed the film as nothing short of "undisguised sponsor[ing] of terrorism" and an "act of war" for which unspecified countermeasures would be taken if the U.S. government did not intervene to shut down the film.[176]

In the months following these unsuccessful attempts at intimidation, a then-unidentified group calling themselves the "Guardians of Peace" (GOP) launched a series of sophisticated cyber-attacks targeting Sony's internal networks, information, and files.[177] The hackers were successfully able to obtain an "insane" amount of Sony's internal corporate information, ranging from unpublished scripts, detailed financial data on all of Sony's recent films, confidential release dates, and even entire films that were not yet released.[178] The data stolen not only contained massive

---

[172] *Id.*

[173] *Id.* at 18; *see also* Lotrionte, *supra* note 156, at 831.

[174] G.A. Res. 56/83, annex, Responsibility of States for Internationally Wrongful Acts, art. 8 (Dec. 12, 2001).

[175] *See* Mike Levine & Kaelyn Forde, *DOJ Announces Charges Against North Korean Hacker for Sony, Wannacry Cyber Attacks*, ABC NEWS (Sept. 6, 2018, 2:21 PM), https://abcnews.go.com/us/doj-announce-charges-north-koreans-sony-hack-wannacry/story?id=57643239 [https://perma.cc/8KDR-J39Y]. *See generally* Clare Sullivan, *The 2014 Sony Hack and the Role of International Law*, 8 J. NAT'L SEC. L. & POL'Y 437 (2016).

[176] *See* Gary Leupp, *A Chronology of the Sony Hacking Incident*, COUNTERPUNCH (Dec. 29, 2014, 9:53 AM), http://www.counterpunch.org/2014/12/29/a-chronology-of-the-Sony-hacking-incident [https://perma.cc/Q4P7-2MFV].

[177] *Id.*

[178] Mark Seal, *An Exclusive Look at Sony's Hacking Saga*, VANITY FAIR (Feb. 4, 2015), http://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg [https://perma.cc/D8JG-7R94].

amounts of proprietary information, but also large quantities of employees and their families' personal and financial data including personal bank accounts, email addresses, phone numbers, passwords, birth dates, social security numbers, medical histories, salaries, and even passports and visas.[179] The hackers took all of this private data and posted it to publicly accessible file sharing websites, all the while contacting Sony employees and officials warning them to cancel the "movie of terrorism['s]" planned release or face further consequences.[180]

Subsequent to the data dump and accompanying threats, Sony cancelled its planned release of *The Interview*, after which the hackers again contacted Sony—this time to praise what they called a "very wise decision."[181] Throughout these events, North Korea repeatedly denied its involvement but nonetheless praised the operation, calling it a "righteous deed."[182] Contrary to their denials, the FBI ultimately concluded that the North Korean government was in fact responsible for the operation, stating that the attack was "intended to inflict significant harm on a U.S. business and suppress the right of American citizens to express themselves."[183] Then President Obama, whose office had already labeled the matter "a serious national security issue," publicly endorsed the FBI's conclusion that North Korea was responsible and criticized Sony for not going forward with the movie's planned release.[184] In the end, Sony did release *The Interview* as originally scheduled, albeit in a limited screening in select theaters only.[185]

The similarities between the 2014 Sony hack and the 2016 election hacks are striking, and the international and domestic reactions to the former are helpful in understanding and characterizing the latter. Indeed, each involves cyber-operations launched by non-state actors but who were largely believed to have been supported, if not directed, by hostile foreign powers.[186] These cyber-attacks were not done to cause physical damage or injury to people, objects, or infrastructure in the traditional, tangible sense of offensive warfare.[187] Rather, their goal was intangible and ideologically motivated—to target U.S. companies and citizens and obtain private information that could be weaponized to disrupt constitutionally protected rights and interfere in sovereign processes for political gain.[188]

---

[179] Sullivan, *supra* note 175, at 440.

[180] David Robb, *Sony Hack: A Timeline*, DEADLINE (Dec. 22, 2014, 1:25 PM), http://deadline.com/2014/12/sony-hack-timeline-any-pascal-the-interviewnorth-korea-1201325501 [https://perma.cc/VKS9-ZMZT].

[181] *Id.*

[182] *Id.*

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] *See* Patterson, *supra* note 62; Robb, *supra* note 180.

[187] Sullivan, *supra* note 175, at 451.

[188] *Id.* at 446, 456–57.

The 2014 Sony hack raised considerable debate in the international community over the sufficiency of existing laws governing cyberwarfare because it demonstrated the "increasingly important dual role of information as both a target and a highly effective weapon capable of causing considerable damage."[189] Commentators remarked how the controlling weight given to cyber-attacks' *physical* consequences under current international law impedes the ability of states like the U.S. to respond to these sorts of intangible yet still highly damaging state-sponsored operations.[190] Nonetheless, under the prevailing norms and understanding of international law at that time, it is hard to argue that the Sony hack constituted a "cyber use of force" or "cyber intervention," each for its own specific reason respectively.[191] First, the cyber-operation lacked the sort of physical consequences and tangible injuries that is characteristic of a use of force in international law.[192] Second, the target of the hack was aimed primarily at the operations of a single private company to influence or harm their business.[193] This result seemingly falls short of the International Court of Justice's conception of intervention as interference in a state's "political, economic, social and cultural system, and the formulation of foreign policy."[194]

In comparison to the Sony hack, designating the 2016 election interference hacks as, at least, an intervention under international law is much more palatable. Whereas the Sony hack was (relatively) contained to the data and information of a single private company, the 2016 hacks targeted a wide array of private companies, government entities, and private citizens—all of whom were intimately connected to the United States' electoral processes.[195] Whereas the Sony hack's ultimate goal was to coerce a privately owned business into making a certain commercial decision,[196] the 2016 hacks had a much grander design: a comprehensive and ongoing misinformation campaign designed to influence American public opinion and U.S. democratic processes.[197] Such a campaign clearly and explicitly intends to interfere with the United States' sovereign right to self-determine its own "political, economic, social," cultural, and foreign policies—the exact definition of "intervention" articulated by the International Court of Justice.[198]

---

[189] *Id.* at 446.

[190] Michael Schmitt, *International Law and Cyber Attacks: Sony v. North Korea*, JUST SEC. (Dec. 17, 2014), https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea [https://perma.cc/EE4R-53FQ].

[191] *Id.*

[192] *Id.*

[193] *Id.*

[194] Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, ¶ 205 (June 27).

[195] *See* Eric Lipton et al., *The Perfect Weapon: How Russian Cyberpower Invaded the U.S.*, N.Y. TIMES (Dec. 13, 2016), https://nyti.ms/2hBJis3.

[196] *See* Robb, *supra* note 180.

[197] *See* Lipton et al., *supra* note 195.

[198] Nicar. v. U.S., 1986 I.C.J. ¶ 205.

B. Framers' Intent

Undoubtedly, the term "invasion" as originally used in the Protection Clause was speaking of some sort of physical intrusion into a states' territorial boundaries.[199] The Framers never could have imagined a world in which a hostile foreign nation could wreak untold havoc on the nation's physical infrastructure and democratic institutions without ever having stepped foot onto United States soil.[200] Despite this, examining the Framers' underlying rationale for their adoption of the Protection Clause through the lens of modern warfare and threats illustrates how these types of cyber intrusions implicate the same concerns as Article IV, Section 4 was intended to address some 300 years ago.

Having only narrowly won their independence in the Revolutionary War and being certain that more threats would arise down the road, maintaining the security of the fledgling United States was a principal concern for the Framers at the 1787 Constitutional Convention.[201] Over the course of the Revolutionary War, key failures in the Articles of Confederation concerning the federal government's power to defend the nation as a whole became apparent.[202] The federal government was essentially powerless to provide and act for the common defense as its authority was contingent on the voluntary acquiescence and contributions of the individual states.[203] On their own, states were either unable or unwilling to sufficiently handle security threats, a trend that James Madison believed was not borne out of a lack of concern for their security, but because sufficient security measures were "too difficult and expensive for one state to provide."[204] When the dangers existed outside of their boundaries, states were even more recalcitrant to support national security measures because they did not directly "benefit their own constituents."[205] Speaking on this issue, Alexander Hamilton wrote, "[s]tates near the seat of war, influenced by motives of self preservation, made efforts to furnish their quotas, which even exceeded their abilities, while those at a distance from danger were for the most part as remiss as the others were diligent in their exertions."[206]

States' willingness to contribute to the defense of their neighbors remained dormant until it was perceived to be in their own best interest, but the Framers knew that such an every-state-for-themselves mentality would prove disastrous for the United States' security as a whole.[207] Invasions and attacks could not be easily

---

199 *See* Mazzone, *supra* note 153, at 48–52.
200 *See* Lotrionte, *supra* note 156, at 833.
201 Mazzone, *supra* note 153, at 37, 40.
202 *Id.* at 40.
203 *Id.* at 39–40.
204 *Id.* at 46.
205 *Id.* at 39–40.
206 THE FEDERALIST NO. 22, at 138 (Alexander Hamilton) (Jacob E. Cooke ed., 1961).
207 *See* Mazzone, *supra* note 153, at 40–47.

confined to one state and would inevitably have negative spillover effects on the economies, stability, and security of nearby states and the nation overall.[208] The Framers viewed these issues as presenting a "collective-action dilemma," where no state wanted to contribute its fair share to the collective security effort of the nation, even though each state was likely to be worse off as a result.[209] The Articles of Confederation relied upon the goodwill of states to contribute to the nation's security, a reliance which Alexander Hamilton described as "ill founded and illusory."[210]

The Protection Clause was intended to remedy the collective-action dilemma, removing from states the primary responsibility of defending themselves against foreign threats and instead entrusting the federal government with the authority and obligation to do so.[211] Alexander Hamilton argued that the national government, being "representative of the whole," would "feel itself most deeply interested in the preservation of every part" and would "best understand the extent and urgency of the dangers that threaten."[212] By granting the federal government the authority to defend all of the states, it would be able to "establish uniformity and concert in the plans and measures by which the common safety is to be secured."[213] Once made "the guardian of the common safety," Hamilton continued, the scope of the federal government's power must not be restricted for allowing states to dictate what resources the federal government could deploy would lead to "weakness, disorder, an undue distribution of the burthens and calamities of war, [and] an unnecessary and intolerable increase of expence . . . ."[214]

In a Constitution that focused on security as much as it did on "governmental structures and individual rights," the Protection Clause was regarded as an essential component.[215] It reflects the Framers' view that the states cannot and should not be left to defend against hostile foreign actors through their own devices.[216] That burden should instead fall upon the federal government, which has the resources, expertise, and authority to provide the robust and uniform defenses needed to ensure the nation's security.[217] Over the last two centuries, traditional notions of warfare and threats posed by foreign actors have evolved dramatically, and yet the original rationale and purpose envisioned for the Protection Clause are as relevant and applicable as ever. The ongoing threats from foreign attacks on state election systems and overall vulnerabilities in the nation's electoral infrastructure implicate the same concerns which the Framers intended to address through the Protection Clause.

---

[208] *Id.* at 40.
[209] *Id.*
[210] THE FEDERALIST NO. 23, at 148 (Alexander Hamilton) (Jacob E. Cooke ed., 1961).
[211] *See* Mazzone, *supra* note 153, at 45.
[212] THE FEDERALIST NO. 23, *supra* note 210, at 149–50.
[213] *Id.*
[214] *Id.*
[215] Mazzone, *supra* note 153, at 59.
[216] *Id.* at 39.
[217] *Id.* at 42–47.

Hostile actors, backed by foreign intelligence and military agencies are targeting and launching highly sophisticated and organized cyber-attacks on state election systems and infrastructure with the intent to intrude and disrupt the nation's democratic institutions.[218] As it stands today, the primary responsibility to prepare, detect, and defend against these attempted cyber-intrusions falls on state and local officials who overwhelmingly lack the requisite resources, experience, and technical knowledge to defend themselves.[219] This fear that security would ultimately prove too difficult and expensive for the individual states to provide was squarely in the minds of the Framers when they adopted the Protection Clause.[220] Both James Madison[221] and Alexander Hamilton wrote at length about the dangers of leaving states to fund and provide for their own security measures, warning that doing so was "[a] project oppressive to some States, dangerous to all, and baneful to the confederacy."[222]

The Framers' concerns that states wouldn't possess the financial and experiential resources to provide for their own security have only been exacerbated in the context of election security. The nation's election systems are comprised of highly complex IT systems with "thousands of endpoints and back-end systems that hold and process large volumes of highly sensitive data," and securing them is no easy feat.[223] Unlike conventional invasions, cyber-attacks can intrude and interfere with state-run systems without ever having physically entered a state's borders, and without sufficient cybersecurity and cyber-forensics training these attacks can—and have—been carried out without state and local officials detecting them.[224] During and after the 2016 election, the states had to rely on the federal government for information because while they "understood that there was a cyber threat, [they] did not appreciate the scope, seriousness, or implications of the serious threat they were facing."[225]

The states' dependence is wholly consistent with Hamilton's characterization of the national government as the "center of information" which would "best understand the extent and urgency of the dangers that threaten."[226] The federal government's ability to act as the "center of information"[227] and to accurately assess the nation's election security is impeded, however, when states are left with discretion as to whether they will share information with them or to accept their security assistance when it is offered.[228] Hamilton foresaw this exact issue and intended for the Protection

---

[218] *See* Johnson, *supra* note 168.
[219] *See* Butchireddygari, *supra* note 111; Hawkins, *supra* note 60.
[220] *See* Mazzone, *supra* note 153, at 46.
[221] THE FEDERALIST NO. 41, at 274–75 (James Madison) (James E. Cooke ed., 1961).
[222] THE FEDERALIST NO. 25, at 158 (Alexander Hamilton) (James E. Cooke ed., 1961).
[223] Hawkins, *supra* note 60.
[224] *See* Horwitz et al., *supra* note 102.
[225] S. REP. SUMMARY ON RUSSIAN TARGETING, *supra* note 8.
[226] THE FEDERALIST NO. 23, *supra* note 210, at 149.
[227] *Id.*
[228] *See generally S. Hearing on Election Security*, *supra* note 129.

Clause to prevent it by making the scope of the national government's power to provide for the common defense clear, obligatory, and unrestricted.[229] Much of the Framers' concerns about varying levels of state security were premised on the fear that certain states with the most resources, like New York, would be the most attractive targets for invasion and therefore would be unable to meet their disproportionate burden in furnishing security.[230] Since invasions and their negative effects would be difficult to contain within a single state, "[t]he security of all would . . . be subjected to the parsimony, improvidence or inability of a part."[231]

Again, the Framers' concerns about the shortcomings of one state affecting the security of the nation can be seamlessly applied to the election security context where the outcome of a national election is often decided by a small number of states. In this context, battleground states like Pennsylvania, Florida, and Wisconsin are synonymous with the resource-rich states like New York in that they are attractive targets for foreign interference attempts and if their security measures are lacking, that could potentially affect, or at least undermine, the electoral process of the nation as a whole.[232] Many battleground states and counties within those states are known to have insufficient election security measures in place today and, due to intrastate politics and financial deficiencies, that fact is unlikely to change without being pushed by the authority of the federal government.[233]

C. Textual Support

The language and composition of the guarantees contained in Article IV, Section 4 lend additional support to expanding the common understanding of the national government's duty to defend against invasion to encompass the realm of election security. The Framers debated at length the specific terms used to articulate the contours of the obligations imposed on the federal government and the rights reserved to the states.[234] The Protection Clause and the preceding Guarantee Clause are notable in that they each impose affirmative, perpetual, and independent obligations on the national government: "The United States *shall* guarantee to every State in this Union a Republican Form of Government, and *shall* protect each of them against Invasion."[235] "Shall means must," and by assuring these two things to every

---

[229] *See* THE FEDERALIST NO. 23, *supra* note 210, at 149; Mazzone, *supra* note 153, at 44.

[230] THE FEDERALIST NO. 41, *supra* note 221, at 275. James Madison, speaking on states furnishing their own security, stated "if their single resources were equal to the task of fortifying themselves against the danger, the object to be protected would be almost consumed by the means of protecting them." *Id.* at 275–76.

[231] THE FEDERALIST NO. 25, *supra* note 222, at 158–59.

[232] *See* S. REP. SUMMARY ON RUSSIAN TARGETING, *supra* note 8.

[233] *See* Geller, *supra* note 55; Greenblatt, *supra* note 22; Parks, *supra* note 53.

[234] *See* Mazzone, *supra* note 153, at 47–53.

[235] U.S. CONST. art. IV, § 4 (emphasis added).

state without any mention of conditional prerequisites, these provisions dictate that the federal government is breaching its duty if they fail even one state.[236] In stark contrast with the Protection Clause, the language contained at the end of Section 4 regarding the national government's obligation to protect the states from domestic violence is only triggered upon "Application of the Legislature, or of the Executive."[237] The fact the Framers chose to differentiate the national government's defensive responsibilities between these two different threats shows that when dealing with invasions, the Framers viewed the national government's protective duty as constant—it must ensure every states' security whether the state wishes to acquiesce or not.[238]

The word "guarantee" itself takes on a special significance when one considers how that term was used in eighteenth century international law and treaties, shedding further light on what the Framers' understood it to mean. While the 1787 Constitution was inherently a document geared towards the collective security of the nation as a whole,[239] its structure largely respected the individual states as independent sovereigns in their own right.[240] As such, in establishing the relationships between the states themselves and between the states and the national government, the Constitution and its provisions were very likely influenced by the principles which governed international law at the time it was adopted.[241] In fact, during the formative years of the nation, "both state and federal" courts "looked to international law principles" to address constitutional issues relating to "border disputes, interstate jurisdiction . . . extradition . . . and sovereign immunity."[242] Looking to how "guarantee" was used in eighteenth century international law, it was frequently "used to signify a reciprocal promise between contracting nations to safeguard [the] rights, privileges or territories" of one another from foreign interference.[243] It also was not unusual for contracting sovereigns to guarantee the others' "adherence to and recognition of certain internal governmental arrangements,"[244] representing not "something new but rather 'a warrant and defense' of something that already exists."[245] James Madison himself spoke of the Guarantee Clause's value as guarding against "experiments" that "may be produced by the caprice of particular States, by the ambition of enterprising leaders, or by the intrigues and *influence of foreign powers*."[246]

Against this backdrop, Article IV, Section 4 can be easily read as promising to the individual sovereign states the United States as a "guarantor" of their republican

---

[236] *See* Mazzone, *supra* note 153, at 53.
[237] U.S. CONST. art. IV, § 4; *see* Mazzone, *supra* note 153, at 53.
[238] Mazzone, *supra* note 153, at 53.
[239] *See id.*
[240] *See* Ryan C. Williams, *The "Guarantee" Clause*, 132 HARV. L. REV. 602, 625 (2018).
[241] *See id.* at 624.
[242] *Id.* at 624–25.
[243] *Id.* at 615.
[244] *Id.* at 619.
[245] *Id.* at 658.
[246] THE FEDERALIST NO. 43 (James Madison) (James E. Cooke ed., 1961) (emphasis added).

government structure, bound to employ whatever means might be necessary to defend against all perceived threats.[247] This reading is further supported by the fact that Article IV, Section 4 is the only place in the Constitution which confers a certain responsibility on the "United States" itself in its collective, corporate capacity.[248] Thus, the relationship between the states and the national government created by the Guarantee Clause and the proceeding Protection Clause is that of a treaty, entitling the sovereign states to the assistance of the national government while preserving their own sovereignty and autonomy.[249]

Beyond its terminology, the composition of Article IV, Section 4 and its overall placement within the Constitution both shed further light on its purported scope for the government's duty to secure the states' security. The Guarantee and Protection Clauses are contained in Article IV, which lays out the contours of the states' relationships with the federal government and with one another.[250] Many of the Article's provisions deal with subjects long dealt with through "international treaties between sovereign nations," provisions which were primarily designed to minimize "potential sources of friction between the . . . states and to bind [them] into a more cohesive . . . union."[251] As a whole, Article IV's goal was to promote harmony and some semblance of uniformity between the states because the Framers' were concerned that issues in one state would inevitably have spillover effects on neighboring states, thus harming the nation's security as a whole.[252]

Section 4's language itself is notable in that it requires the United States to guarantee each state a "Republican Form of Government, *and shall* protect each of them against Invasion."[253] These two obligations, security and republican government, are linked, reflecting the Framers' view that a democratic government ruled by the people "is impossible to achieve and sustain without security."[254] To ensure these fundamental, coexisting elements of democracy would not be hampered by financial insufficiencies, political squabbles, or foreign interference, the Framers imposed on the national government an unqualified and unrestrained duty to maintain their existence.[255]

Election security and the rise in foreign election interference attempts are unique in that they directly implicate both of these constitutional guarantees. Elections are the engine through which the states operate and maintain their republican forms of government, and when foreign powers attempt to attack, interfere, or otherwise

---

[247] *See* Mazzone, *supra* note 153, at 53–54.
[248] Williams, *supra* note 240, at 632.
[249] *Id.* at 660–61.
[250] *See id.* at 626–27.
[251] *See id.* at 627–29.
[252] *See id.* at 629.
[253] U.S. CONST. art. IV, § 4 (emphasis added).
[254] *See* Mazzone, *supra* note 153, at 55–56.
[255] *See id.* at 91.

influence the electoral process, they are attempting to invade one of the most fundamental liberties that a sovereign state possesses: the right to self-determine its own government. If the Framers intended for the national government to independently serve as both the perpetual guarantor of the states' republican government and their unconditional defender from foreign invasions, it takes no logical hurdle to conclude that the national government cannot leave states as the primary guards against foreign interference attempts against the country's democratic processes.

CONCLUSION

Foreign interference in U.S. elections is not going anywhere, and it poses a real threat to American democracy and to the United States' national security overall. States have been constitutionally entrusted with the authority to oversee and administer elections within their jurisdictions, and such a decentralized system is undoubtedly one of the best defenses against foreign interference.[256] Separating key electoral infrastructure into thousands of independent systems inherently contains and prevents security breaches from having widespread consequences outside of the affected jurisdiction.[257] Aside from the benefits, however, the current system also has inherent flaws that foreign powers can—and have—exploited to intrude upon our elections.[258] Disparities in funding and minimum cybersecurity standards, lack of training and expertise, and the voluntary nature of reporting and sharing information between state and federal officials act as a severe impediment to the nation's ability to combat election interference.[259]

Despite having no conception of a threat such as this in the late eighteenth century, the Framers did, in a sense, include a provision applicable to the problems we face today. The Framers knew that leaving the nation's defense to the inexperienced and ill-equipped states would result in a collective security dilemma, wherein the shortcomings of one would inevitably spillover to the detriment of the whole.[260] Instead, they had the foresight to charge the national government with the duty to defend all states from foreign influences, equally.[261] Illustrative of how essential they viewed this duty to defend, the Framers placed it directly after the duty to guarantee each state a republican form of government—the critical ingredient to American democracy.[262] The Framers would be aghast to find that the national government, citing principles of federalism, is now leaving state and local officials as the principal defenders against hostile foreign powers attempting to infiltrate and

---

256 *See* U.S. CONST. art. I, § 4, cl. 1.
257 *See* Good, *supra* note 17.
258 *See* Horwitz et al., *supra* note 102.
259 *See* Butchireddygari, *supra* note 111.
260 *See* Williams, *supra* note 240, at 629.
261 *See* Mazzone, *supra* note 153, at 53.
262 *Id.* at 55.

undermine their most sacred of democratic traditions. No less than the Framers would have expected the national government to assist a state in preventing a foreign power from invading on election day to stuff the ballot box, they too would expect the federal government to lend aid when the same result is attempted through intangible means. The Constitution demands more to be done, and the federal government already possesses the necessary tools to provide more consistent federal funding, personnel training, and mandatory minimum-security requirements. In so doing, the federal government can be confident that its conduct falls squarely within the realm contemplated for it by the Framers and the Constitution.