Federal Elections Standards for a Malicious Cyberspace

by Michael E. Cairo

"The right to vote should be considered sacred in our democracy."
Charles B. Rangel

Introduction

The right to vote is the most defining and important part of a functional democracy. Public faith in voting systems is absolutely crucial to a successful democracy so that citizens have a high degree of confidence that their elected leaders receive affirmative votes in a fair manner by a majority of the respective electorate, ensuring accurate representation in government. There are a plethora of Federal laws, State laws and five separate amendments to the Constitution of the United States that protect citizens' right to vote indiscriminate of race, sex, income and age. The 2016 Presidential election brought to light a new kind of threat to our democracy- malicious cyberattacks from an adversarial foreign government.

Presidential elections in the United States are vulnerable to system breaches by independent hackers or foreign state-sponsored cyber militants. This sobering reality was revealed when the Office of the Director of National Intelligence released a shocking declassified report on a joint investigation conducted by the Central Intelligence Agency (CIA), Federal Bureau of Investigation (FBI) and National Security Agency (NSA). All of these agencies asserted with high confidence that the Russian President Vladimir Putin likely ordered an influence campaign with intentions to undermine public faith in the U.S. democratic process in an aim to discredit former Secretary of State Hillary Rodham Clinton's campaign in an attempt to foster support for President Donald Trump's campaign.[1]

[1] Office of the Director of National Intelligence, Assessing Russian Activities and Intentions in Recent US Elections ii, 3, Jan. 6, 2017, https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf , (last visited April 5, 2017).

The report also stated that Russian intelligence successfully gained access to several local and state voting systems. The declassified report released to the public notes that it purposefully excludes intelligence methods and sources that would fully support these assertions in order to maintain the agencies' ability to collect critical intelligence in the future. These agencies state that Russia is responsible for these malicious activities in reference to Russian propaganda tactics deployed in former Soviet countries and in the United States, activity which supports this narrative.[1] Under the assumption that these allegations are true, the very scenario of any foreign government or any other entity having the ability to hack into our voting systems begs the question about the security of our democracy at large in the 21st century.

Through further examination into the level of vulnerability some states' voting systems, it is evident our democratic process has never been more severely at risk than it is today. 28 percent of voters live in jurisdictions that use Direct-Recording Electronic (DRE) machines to keep track of votes. The issue with this system is that there is no paper trail or other verifiable means that can record the votes cast outside of a susceptible electronic database.[2] Some DRE machines used in the 2016 election still operate on the severely outdated Windows XP operating system, security updates for which were halted in 2013, leaving them very vulnerable to cyber-attacks.[3] The current legal framework neglects to address key questions that need to be asked and answered in the event of a cyberattack on our nation's voting systems. What measures are currently in place to protect the integrity of U.S. elections? What are the national standards that states must comply with in order to ensure that their systems maintain a proper level of security? How can voters independently verify the accuracy of elections if a DRE system is compromised? Robust mandated federal cybersecurity standards must be

---

[2] Drew DeSilver, *On Election Day, most voters use electronic or optical-scan ballots*, Pew Research Center (2017), http://www.pewresearch.org/fact-tank/2016/11/08/on-election-day-most-voters-use-electronic-or-optical-scan-ballots/, (last visited Feb 1, 2017).

[3] Shanika Gunaratna, *Cybersecurity expert: One battleground state most vulnerable to voting hacks*, CBSNews.com, 2017, http://www.cbsnews.com/news/ex-nsa-expert-if-i-were-an-election-day-hacker-id-hit-pennsylvania, (last visited Feb 1, 2017).

adopted to secure our voting systems to protect the integrity of U.S. elections and the public faith in the democratic process to maintain strong national security.

Current Regulation

The federal government of the United States only has limited power in regulating how elections are conducted; a majority of the power is vested with the States and localities. Art. I, § 2 of the U.S. Constitution provides that "The House of Representatives shall be composed of Members chosen every second Year by the People of the several States." Art. I, § 4 provides that "The Times, Places and Manner of holding Elections for Senators and Representatives, shall be prescribed in each State by the Legislature thereof; but the Congress may at any time by Law make or alter such Regulations, except as to the Places of choosing Senators." And Art. I, § 8, clause 18 gives Congress the power "To make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof."

These provisions grant States and localities to determine the policies surrounding the administration of elections, however it also grants Congress the power to create or amend laws that are "necessary and proper" to ensure that elections are executed appropriately so that our leaders are duly elected. Furthermore, the Help America Vote Act of 2002 (HAVA) established the Elections Assistance Commission (EAC) that provides aid to States and localities in improving the administration of elections, and provides funds to update outdated voting systems and establish a system of testing and certification of each State's voting systems. The provisions in HAVA do not require all states to be compliant with federal testing and regulation.[4] Taking these factors into account with respect to Art. I, § 4, it is apparent that Congress is granted the authority to adopt "necessary and proper" security regulations so long as they do not interfere with the places in which representatives and senators are elected to represent. .

[4] 42 U.S.C. § 15301 (2009).

Before we examine the law surrounding the protection of votes cast in an election, let us first consider the definition of a "legal vote" as decided in Bush v. Gore.[5] This case is one of the most deeply controversial in our election system in recent history because its outcome ultimately decided who would become the President of the United States in the hotly contested 2000 election between then-Governor George W. Bush and former Vice President Al Gore. The validity of the election was called into question when it was discovered that 9,000 votes cast in Miami-Dade County failed to properly detect a vote for President. The Gore campaign was granted a recount because Section 102.168(3)(b), Florida Statutes (2000) provides that a recount could be imposed by a court of law if the "rejection of a number of legal votes sufficient to change or place in doubt the result of the election."[6] Given this interpretation of a legal vote, voting systems must not only tally the results of an election, but they must also clearly indicate the intent of each voter.

Analysis

While several provisions in Art. I of the Constitution grants States and localities power to administer and regulate elections as they see fit, Congress does have limited power to create and amend elections regulations as well. Given the recent attacks on our voting systems in the 2016 election, it is urgent and absolutely necessary that Congress establish some kind of federal standard for cybersecurity of voting systems that States and localities must comply with in order to protect the integrity of the process.

According to a study about the voting systems in place during the 2016 election conducted by Pew Research Center, 28 percent of voters live in jurisdictions that only use DRE voting systems.[7] The EAC's

[5] *Bush v. Gore*, 531 U.S. 98 (2000).
[6] Fl. Stat. 102.168(3)(b) (2011).
[7] Drew DeSilver, *On Election Day, most voters use electronic or optical-scan ballots*, Pew Research Center, Nov. 8, 2016, http://www.pewresearch.org/fact-tank/2016/11/08/on-election-day-most-voters-use-electronic-or-optical-scan-ballots/, (last visited Feb 1, 2017).

recommendations for secure voting are non- binding because of the aforementioned provisions of Art. I. In a report released by the EAC, 20 states have no federal requirements for voting standards, 10 require testing to federal standards, 13 require testing by a federally accredited laboratory, and 12 require federal certification.[8] Giving States the power to decide if they will comply with federal testing and security standards defeats the purpose of having federal standards in the first place. Reasonable minimum standards for cybersecurity are necessary in the digital age and should not be mere recommendations if the vulnerability of one state (such as Florida in 2000) could potentially affect the outcome of an entire election. These facts are especially concerning when you consider the aforementioned intelligence report revealing that Russian hackers successfully gained access to voting systems in several U.S. states and localities. An article by CBS News asserts that the FBI had discovered that as many as ten states' systems were probed or breached during this election cycle.[9] U.S. officials currently maintain that the vote counts were not compromised in the 2016 election, however, foreign actors gaining access to our election processes poses a huge threat to the success of our democratic process and could have catastrophic consequences.

States that use DRE systems (such as Pennsylvania) are especially vulnerable when you consider the fact that some of these systems still operate on the severely outdated Windows XP operating system. Windows XP is a favorite among computer hackers because its vulnerabilities are plentiful and well-documented, thus making it relatively easy to hack-- so much so, that the cybersecurity firm Carbon Black's chief security strategist Ben Johnson says if

[8] U.S. Election Assistance Commission, State Requirements and the Federal Voting System Testing and Certification Program, https://www.eac.gov/assets/1/1/State%20Requirements%20and%20the%20Federal%20Voting%20System%20Testing%20and%20Certification%20Program.pdf , (last visited April 5, 2017).

[9] Alan Diaz, *More state election databases hacked than previously thought*, CBSNews.com , Sept. 28, 2016, http://www.cbsnews.com/news/more-state-election-databases-hacked-than-previously-thought/, (last visited Feb 6, 2017).

he was a hacker, he'd target Pennsylvania specifically for that reason.[10]

In the event of a cyberattack on DRE voting systems that destroys or manipulates the vote counts in the machines' computer memory, the lack of verifiable paper ballots makes it impossible to accurately recover "legal votes" as defined in Bush v. Gore because a "clear indication of the intent of the voter" cannot possibly be determined if, for example, a hacker erases the computer's memory and replaces actual vote counts with fraudulent data. If a hacker successfully gained access to Pennsylvania's DRE databases, they could erase all the votes for a candidate stored in the computer's memory and replace it with several million votes for their opponent, for example. In this case, this outcome would be flagged as suspicious and a recount ordered. However on DRE systems, there would be nothing to back up what was initially recorded into the database. Pursuant to Art. I, § 8, cl. 18 of the Constitution, establishment of federal cybersecurity compliance standards are both necessary and proper for carrying into execution federal elections in the digital age, and the existing recommendations provided by the EAC model are no longer sufficient.

In 2016, Congressman Hank Johnson, D-Ga., introduced the Electronic Infrastructure and Security Promotion Act of 2016 (H.R.6073) that would have directed the U.S. Department of Homeland Security (DHS) to:"(1) designate voting systems used in the United States as critical infrastructure; (2) include threats of compromise, disruption, or destruction of voting systems in national planning scenarios; and (3) conduct a campaign to proactively educate local election officials about the designation of voting systems as critical infrastructure and election officials at all levels of government of voting system threats.[11]

The bill would also task the National Institute of Standards and Technology (NIST) to develop transparent and verifiable standards to ensure the

[10] Shanika Gunaratna, *Cybersecurity expert: One battleground state most vulnerable to voting hacks,* CBSNews.com, 2017, http://www.cbsnews.com/news/ex-nsa-expert-if-i-were-an-election-day-hacker-id-hit-pennsylvania, (last visited Feb 1, 2017).

[11] H.R.6073 — 114th Congress (2015-2016).

operational security of voting systems in each state, and it would amend HAVA[12] to require that each state comply with the standards developed by NIST. The bill died in committees under the 114th Congress because some opponents argued that it would create an additional layer of bureaucracy surrounding elections that they deemed unnecessary. At the time, DHS officials stated that they had no evidence of any 'credible threat' of a cyberattack.[13] Given the information about the Russian hacks we have now, additional protection is needed, whether it be designated critical infrastructure status or not. Either H.R. 6073 or similar legislation that establishes more robust cybersecurity standards at a federal level should be adopted in order to ensure the efficacy and protection of each state's' voting systems. Each state could still retain full authority to administer elections as it sees fit pursuant to Art. I, § 4 so long as it meets federal cybersecurity standards.

While this legislative attempt was a step in the right direction, the 115th Congress of the United States seemed to have taken a different approach. As of February 2017, there is legislation on the House floor entitled H.R. 634 - Elections Assistance Commission Termination Act to amend the HAVA to effectively terminate the EAC citing that the commission has outlived its purpose. "If we're looking at reducing the size of government, this is a perfect example of something that can be eliminated," said Rep. Gregg Harper (R-Miss.), the committee chairman, after the bill passed on a 6-3 vote. "We don't need fluff."[14] In a particularly volatile election year where numerous claims of voter fraud and foreign actors hacking into our voting systems, it seems as though some in Congress are considering eliminating the EAC at a time when it appears that it is needed the most.

---

[12] The Help America Vote Act of 2002, 42 U.S.C. §15541 (2002).

[13] *Summary of H.R. 6073 (114th): Election Infrastructure and Security Promotion Act of 2016* - GovTrack.us,, https://www.govtrack.us/congress/bills/114/hr6073/summary, (last visited Feb 1, 2017).

[14] Associated Press, *House Committee votes to scrap agency that helps states improve voting systems*, Feb. 7, 2017, http://www.latimes.com/politics/washington/la-na-essential-washington-updates-house-committee-votes-to-scrap-agency-1486514170-htmlstory.html, (last visited April 5, 2017).

Conclusion

The need for federal cybersecurity compliance standards for voting systems in the United States is absolutely essential to protect our democracy, and the time to act is now. The current EAC guidelines do respect the autonomy of States and localities in determining policy for executing elections as provided in Art. I of the Constitution. However, they are insufficient given the ever-present threat of data breaches in States that use DRE systems to tally votes. Congress should exercise its power granted in Art. I to impose more robust federal compliance standards to ensure that every state's voting systems are secure and that they maintain a verifiable paper trail that can be used for audit in the event of a cyberattack.[15] If the EAC is to be dismantled, the Department of Homeland Security should administratively add cybersecurity regarding federal elections to their list of sectors of critical infrastructure to ensure optimal protection and efficacy in our democratic process.

Reform is essential if we hope to maintain a properly functioning democracy, to restore a recently shaken public faith in our democratic process, and to deter any attempts by foreign adversaries such as the Russian government from interfering in or undermining confidence in our elections. Foreign influence on our elections could prove to be catastrophic for our national security if adversarial actors can successfully manipulate our election process to favor their own interests. The need for stronger cybersecurity reform to our voting system is critical to the survival of our democracy in the digital age.

[15] U.S. General Accounting Office, *The Scope of Congressional Authority in Election Administration* , March 2001, http://www.gao.gov/new.items/d01470.pdf, (last visited April 5, 2017).