Journal of Information Assurance and Security.
ISSN 1554-1010 Volume 13 (2018) pp. 118-124

Securing Democracy: A Comparative Look at Modern and Future US Voting Systems Through the Lens of the CIA Triad

Luke Hoffman[1], and Nima Zahadat[2]

[1]College of Public Affairs, University of Baltimore
1420 N Charles St., Baltimore, MD, USA
luke.hoffman@ubalt.edu

[2]College of Public Affairs, University of Baltimore
1420 N Charles St., Baltimore, MD, USA
nzahadat@ubalt.edu

Abstract: As supported by mounting evidence and testimony from top US national security officials, American elections are under siege. Included in these threats are direct attacks to voting infrastructure. It is clear that these threats must be taken seriously and aggressively mitigated. This paper will serve to analyze the current methodology of American voting infrastructure and identify security flaws within it. It will then compare those security issues with potential issues associated with an internet voting system. The CIA triad will be used to evaluate an internet voting infrastructure in comparison to the current system. Security and cryptography recommendations will be made to demonstrate that obstacles to internet voting could be overcome with enough research. The paper will also assess the role of national and state governments in securing elections and provide recommendations on what critical steps must be taken.

Keywords: Cryptography, Voting, Elections, Estonia, DRE, Internet Voting, Critical Infrastructure, Security

I. Introduction: Threat Analysis

Maintaining integrity in elections is a cornerstone to any true democracy. This long held fact led the United Nations to include "genuine elections" to its Universal Declaration of Human Rights, alongside other basic human rights such as freedom from slavery and torture [1]. The success or failure of a democracy rests largely on a nation's ability to maintain free and fair elections. This requires constant efforts to ensure that elections have adequate security, or risk watching a democracy crumble. In the United States, this risk has been heightened in recent years from state and non-state actors attempting to interfere in US elections.

Evidence of this heightened risk comes from abundant testimony of US national security officials. To quote one of many such officials, Samuel Liles, DHS Cyber Analysis Division Acting Director, testified regarding the 2016 election cycle that "We determined that internet connected election related networks in 21 states were potentially targeted by Russian government cyber hackers." Liles went on to testify that "A small number of the networks were successfully exploited" [2]. This shows not only that a foreign adversary was attempting to hack US election infrastructure, but that they were successful to an extent. This testimony is concerning, but what is more concerning is that these threats are likely only to expand. Dan Coates, Director of National Intelligence testified that Russia "Will pursue even more aggressive cyber attacks with the intent of degrading our democratic values" Coates also testified that "Disruptive cyber operations will continue against the United States…using elections as opportunities to undermine democracy." [3]. The testimony from Liles and Coats, as well as many other officials, make clear that American democracy faces a real threat today and into the future. With national elections occurring every two years, this threat is one that must be taken seriously and aggressively mitigated.

This paper will highlight vulnerabilities commonly associated with the current voting system. Additionally, because cyber threats are likely to persist into the future, Internet voting protocols are examined and compared to the current system. Recommendations will also be made on how to best mitigate the risks associated with both types.

II. DRE: The Current System

As mandated by the US Constitution, every state has a different way of conducting elections, so there is no uniform voting system in the US. There are many different mechanisms of casting and tabulating votes, however this paper will mainly discuss one type. This paper will focus on Direct Recording Equipment (DRE) as the modern voting machine. Lawrence Norden of the Brennan Center for Justice explains that "The defining characteristic of DRE machines is that votes are captured electronically and stored in that form" [4]. This is different from any other US voting machine because the process can be conducted 100% electronically, and often does not have any paper or non-electronic

component. DRE's are used extensively throughout the US, showing up in 28 of the 50 states [5]. They are also the most technologically reliant, making them more relevant to the topic of information security.

DRE's are manufactured by many different companies but generally all work in a similar fashion. Therefore, vulnerabilities and threat vectors that occur on one are often applicable to other DRE machines. Because of this, this paper will only analyze the technical aspects and vulnerabilities of one DRE. An analysis of data made available by the Verified Voting Project was used to select which DRE to analyze. According to this data, of the 2402 counties that are expected to use DREs in the 2018 election cycle, 1031 of them, or approximately 50% use to some extent the Sequoia AVC Edge (Sequoia is now owned by Dominion). Therefore, it makes most sense for this paper to focus on the technical functions of the AVC Edge.

The AVC Edge is a touchscreen non-networked DRE where votes are stored on removable memory. Fortunately, Matt Blaze et al conducted a source code review of the AVC Edge on a contract for the California Secretary of State [6]. The review is extensive so this paper will only summarize his explanation of how the system operates. In the preparation stage, which occurs at the election headquarters, election and ballot information is configured in WinEDS, an election configuration software. Once configured, the ballot information is loaded onto removable memory called the results cartridge. This cartridge is then loaded into every Edge machine and secured with tamper evident tape. The DRE's, along with smartcard issuing machines are sent to the polling places. On election day, voters will receive a smartcard from an election official, which is configured using a smartcard activator. The voter then inserts the smartcard into a port which activates the machine to open the ballot. The voter uses the touchscreen to make his or her selections, then submits the vote. The vote is then recorded onto the results cartridge as well as an internal audit trail. The audit trail can be used to recover votes if the results cartridge is damaged or lost. At the end of election day, the results cartridges are removed from the Edge machines and transported back to election headquarters. In the vote tallying process, the results cartridges are read by the WinEDS system, where votes will be tallied and a winner declared [6].

The AVC Edge may appear to be a secure, relatively straight forward system, but Blaze and other researchers found significant vulnerabilities. Blaze identified serious security issues when it came to data integrity, cryptography, access control, and software engineering. These vulnerabilities will be discussed in depth later in the paper but to get a sense of the seriousness of the vulnerabilities, one will be highlighted in this section.

There were found to be issues in the way cryptographic keys are stored and distributed. Blaze summarizes the issue saying "Virtually all cryptographic key material in the Sequoia system is permanently hardcoded into the software source code (and is apparently identical in all hardware shipped to different jurisdictions)." This is an issue for multiple reasons. NIST Special Publication 800-57, which provides best practices for key management, discusses cryptoperiods. Cryptoperiods refer to the amount of time a key, or other cryptographic function, should be used before it is changed. There is no set advised cryptoperiod, but instead depends on how and what the key is used for. However, all keys do have a cryptoperiod and should be changed at some point. NIST explains that a sound cryptoperiod "Limits the amount of information protected by a given key that is available for cryptanalysis" and "Limits the amount of exposure if a single key is compromised" [7]. The AVC Edge violates these security best practices. The keys in the Edge machines makes no attempt at limiting the "exposure if a single key is compromised" because all keys are identical in every system. This means that if a key is discovered by a bad actor in one system, that person now has the key to every system. Additionally, because the keys are hardcoded, they are never changed. NIST advises the keys be changed when "The key's cryptoperiod may be nearing expiration [7]. Since the AVC edge never established a cryptoperiod, it is impossible for the cryptography to comply with NIST Guidelines. This is just one of the many security flaws in the AVC Edge system.

III. Internet Voting

If DRE's and other electronic voting machines are the present, then internet voting is likely to be the future. Internet voting is the process of casting votes via the internet, eliminating the need to go to a polling place. With very few exceptions, internet voting has not been implemented in the United States. However it has been implemented in Norway and Estonia. The Estonian system is the most widely analyzed, so it will serve as the example of internet voting in this paper.

First though, it is important to understand why internet voting is a project even worth undertaking. The obvious reasons for internet voting are increased accessibility, versatility, and convenience. These may seem like good but not great reasons to overhaul the voting system. However, it is important to remember that these are more than just improvements to convenience, they are improvements to democracy. Voter turnout is an important factor when evaluating a democracy. If more people are participating in voting, it is a positive sign. Internet voting would logically increase voter turnout by allowing populations that would have difficulty getting to polling stations to vote. Such populations include the disabled, citizens living overseas, voters in remote locations, or people simply too busy to vote.

Estonia has used internet voting in 3 Parliamentary elections since it's implementation (2007, 2011, and 2015). Therefore, analyzing voter turnout over the course of those elections will show if internet voting has increased turnout. According to data available from the Estonian government, voter turnout in Parliamentary elections have increased each election from 61.9% in 2007, to 63.5% in 2011, to 64.2% in 2015 [8]. While there are many factors that contribute to voter turnout, it is difficult to ignore that turnout has only risen since implementation. Also during those same elections the usage of internet voting has significantly increased. Of all ballots cast, 5.5% were cast via internet voting in 2007, then 24.3% in 2011, and 30.5% in 2015 [8]. These drastic increases show that voters are gaining more trust in the internet voting system. As a disclaimer, it is important to say that these statistics show

a correlative relationship, but not necessarily a causal one. Internet voting is simply too new to confidently say that it alone is affecting voter turnout. However, based on voter turnout and internet voting usage statistics, it would appear that the Estonian voting system has shown success and could be used as a model for other countries.

The Estonian internet voting system, in place since 2005 has been an interesting case study in the approach to online voting. Research written by J. Alex Halderman et al [9] has explained extensively the Estonian internet voting system. While his literature explains the systems in great detail, this paper will summarize his explanations of how the systems function. The voting process begins when the voter downloads the voting application onto their computer from the election administration's website. When the voter is ready to vote, he or she will launch the application and insert their government issued smart card. The smart card, also used in other government online processes, can perform authentication and digital signature functions. Once inserted, the user must enter their PIN number. The application then communicates with the Vote Forwarding Server (VFS) to authenticate the voter. In addition to the VFS authenticating the user, the user will authenticate the VFS to prevent man in the middle attacks. The VFS then sends the ballot information to the voting software. The user will make their selections and cast their ballot. The ballot, which does not contain the voters identifying information, is then encrypted. Then, an encrypted signature is added to the packet that the VFS uses to authenticate the user. Encrypting the ballot and then providing a signature creates a double envelope level of security where even if the voters identity is determined, the attacker still does not know the contents of the ballot. The VFS, after authenticating the packet will send the inforamtion to the Vote Storage Server (VSS). The VSS stores encrypted and signed packets until they are ready to be tabulated. To tabulate the votes, the VSS begins by removing the 'outer envelope' of the digital signature. All that remains is the encrypted ballot which does not contain identifying information. These encrypted ballots are then loaded onto DVDs and transported to the Vote Counting Server (VCS). The VCS is not connected to a network. The VCS contains the private key that can unencrypt the ballots and tabulate the votes.

An additional feature of the Estonian voting system is a method of verification. When the ballot is cast a QR code will then appear on the user's computer screen. The user can then scan the code with their smartphone. The smartphone will then communicate with the VFS and show the user the ballot that he/she cast. This provides verification to the user that the ballot was not adjusted between the client and VFS [9].

While the Estonian internet voting system at first glance appears to be a well thought out, secure system, researchers have identified numerous issues with it. Some issues identified by J Alex Halderman include Malware recording the PIN, malware injection into the server, operational security issues, and many more [9]. Many of these will be discussed during the analysis section of this paper. The main takeaway about the full security analysis conducted by Halderman et al is provided in his paper: "we conclude that a state-level attacker, sophisticated criminal, or dishonest insider could defeat both the technological and procedural controls in order to manipulate election outcomes" [9].

It has been established by researchers that the internet voting system is far from perfect. Additionally, a quick internet search about internet voting will pull up mostly sensationalist articles saying that internet voting is entirely insecure and should never be used. Examples of such attention-grabbing headlines include "Forget rigged polls: Internet voting is the real election threat" [10] or "Internet voting is just too hackable, say security experts" [11]. These headlines are certainly scary and are likely to turn off a lot of people to internet voting. However, the internet voting system is relatively new and is likely only improve with time. The potential advantages internet voting can bring to voting procedures and democracy are too great to shy away from. Security experts must continue to work to improve this system and to not dismiss the idea as infeasible.

IV. CIA Triad

The second portion of this paper will address what is lacking in the discussion of internet voting security. There is abundant literature discussing the vulnerabilities of DREs and internet voting. However, these systems are often analyzed independant from one another. Ultimately, it is up to governments and election officials to decide whether or not to implement internet voting. However, without a side by side comparison of the vulnerabilities, advantages, and features of both systems, that decision is likely to be ill informed. Therefore, this paper will offer a comparitive analysis of DREs and internet voting. To guide the discussion, the CIA triad, a framework widely used in information security, will be used.

The CIA Triad has long been used in information security to help evaluate and create information systems. CIA stands for confidentiality, integrity, and availability. It means that a sound information security system must protect confidentiality, integrity, and availability. If the system does a poor job at protecting those prongs, it is insufficient. These principles have appeared throughout official security standards such as FIPS 199. FIPS 199, a US government information security guidline, lists the three security objectives as confidentiality, integrity and availability [12]. In the following sections, DREs and internet voting will be assessed to see how they perform under each prong of the CIA triad. Each section will highlight common attack to the respective prong, and how each system prevents or doesn't prevent such an attack. This analysis will give decision makers a clearer picture of how the two compare from a security perspective. Additionally, recommendations will be made to enhance security using cryptography and other security principles.

A. Confidentiality

The confidentiality prong of the CIA Triad refers to the protection of information from unauthorized or unintended discloseure Threats to confidentiality can include data exfiltration, spyware, or network snooping, among others. Confidentiality is vital to an election system because of the strongly held principle of the secret ballot. A secret ballot simply means that a person's vote is not public. This is foundational to democracy and is an assurance provided in

many state constitutions. The Delaware State Constitution, for example, states that "General Assembly may by law prescribe the means, methods and instruments of voting so as best to secure secrecy and the independence of the voter" [13]. It is vital that an election system be able to adequately protect confidentiality.

An attack that has been identified to affect confidentiality in the internet voting system is spyware. Spyware is malware that will record what a user is doing on a computer. This information can then be either stored locally or more often transmitted over a network to a bad actor. Haldermann and his team of researchers identified the client, or users computer, as particularly vulnerable in the Estonian system [9]. Haldermann et al recreated the Estonian system in a lab in order to thoroughly test the system. Most research focused on attacks to integrity, several of which were successful. However Haldermann concluded that "Sophisticated attacks reman possible, however, including spyware on the voter's PC or smartphone…" [9]. This is a logical attack that exploits one of the main weaknesses of internet voting. While DREs are under relatively full control of election officials at all times, the users computers in internet voting are not. This means that the government has little means of ensuring confidentiality, or integrity for that matter, if attacks are performed at the client side.

Additionally, spyware is often a passive attack meaning it does not actively attack a computer. Instead it often simply sits on a computer collecting information and can remain undetected. This makes it different than many other more active and harmful malware. NIST SP800-83 explains that normal antivirus software may be insufficient in stopping spyware: "Unlike antivirus software, which attempts to identify many types of malware, spyware detection and removal utilities specialize in both malware and non-malware forms of spyware" [14]. This means that in order for internet voting to protect confidentiality, all users would have to have both antivirus software plus a supplemental spyware detection and removal utility. This is of course not the case in the Estonian system, and is near impossible to ensure.

While there are serious confidentiality issues with internet voting, DREs are not a perfect system either. While spyware is also a possibility on DRE machines, the election officials have more control over them and can more easily ensure proper security. One threat that is possible in the previously discussed AVC Edge machine takes advantage of the lack of strong encryption in the results cartridges. Results cartridges are the removable memory that the votes are recorded on, transported to election headquarters, and it's data is ultimately used in vote tallying. The information stored on the results cartridges are encrypted which is a good step. However, the full source code review conducted by Blaze et al determined that the encryption used in the results cartridges was insufficient.

The encryption issue revolves around poor implementation of randomization. One attempt the AVC Edge makes at encryption is the use of a pseudo-random number generator to rearrange the order in which the votes are cast. Without this rearrangement, knowledge of the order in which votes were cast (could be obtained just by observing or from watching security footage) and access to the information on the results cartridge would show how each individual voted. However, Blaze discovered that "A person who gains access to the votes stored on a Results Cartridge can determine the original order in which votes were cast" [6]. Blaze explains that this is because "the way the random number generator is used reduces the possible random sequences to just 10". While this would take some effort to obtain the results cartridge information as well as determine the order in which each person voted, an attack on this would violate confidentiality.

Whereas spyware on internet voting can only affect one computer, thus one person, at a time, this attack on DRE confidentiality would affect a large number of voters. However, when comparing DREs to internet voting, DREs do a better job of protecting confidentiality. This is helped because DREs are always under control of election officials and can better ensure that proper antivirus and spyware software is installed. Without control over the client, it is near impossible for an internet voting system to adequately defend against spyware and protect confidentiality. To improve their system though, DRE manufacturers should routinely publish source code to allow the information security community to help identify flaws. This could have prevented the encryption issue highlighted by Blaze.

B. Integrity

The integrity prong of the CIA triad refers to the protection of information against unauthorized alterations. A loss of integrity as it refers to elections would be a changing of the ballot information. This could occur at any point between when the voter makes a selection to when the votes are tabulated. The importance of integrity during elections is obvious. If bad actors can just change the votes to produce whatever outcome they want, then there is no point to holding elections in the first place. Worryingly, the AVC Edge and Estonian internet voting systems had serious flaws in their systems.

One threat to integrity in the internet voting system again occurs at the client side. After setting up a mock election environment, Halderman was able to "use malware on the client machine to silently replace the user's vote with a vote in favor of an attacker-selected candidate" [9]. To summarize the attack, the malware works silently to first log the users PIN when they first go to vote. The malware will then wait until either the voting application is closed or a set amount of time. The malware will then open a hidden session of the voting application, check to make sure the smartcard is still in the machine, enter the PIN, and cast a new ballot. The new ballot will overwrite the previously submitted vote.

This is concerning because the 2-factor authentication (smartcard and PIN) that provides much of the security of the system was able to be easily circumvented. Wide implementation of this attack would completely undermine the results of the election. This type of malware is more concerning because it is only used during short election cycles. Since elections occur on one day or a small number of days, this malware, or another like it, could be implemented as a zero day. FireEye, a respected cyber threat intelligence firm, defines a zero day as "an unknown exploit in the wild that exposes a vulnerability in software or hardware and can create complicated problems well before anyone realizes something is wrong" [15]. Well-funded state actors are one such group

that would be interested in hacking an election. They could use their resources to develop and implement a well-made zero day exploit. FireEye also explains about zero days that "it often takes not just days but months and sometimes years before a developer learns of the vulnerability that led to an attack". Zero-day exploits are especially dangerous during elections because there will not be enough time to identify and patch the issue.

The AVC Edge DRE also has a serious integrity vulnerability. The vulnerability, identified by Blaze et al, deals again with poor encryption in the results cartridges. Blaze et al states that "every one of the cryptographic algorithms used in the Sequoia system is either obsolete and known to be weak [6]. One example of outdated encryption algorithms used is the Cyclic Redundancy Check (CRC) being used as a Message Authentication Code (MAC). A MAC is defined as "A function of the message and a secret key that produces a fixed-length value that serves as the authenticator" [16]. A MAC is used to verify integrity of a message to ensure data was not altered in transit. This is important because without a properly implemented MAC protocol election officials would have no way of knowing if the results cartridges were tampered with. Blaze explains that CRC as a MAC is "appropriate only for detecting non-malicious errors; they provide no defense against intentional data tampering". Therefore, there is essentially no way to verify the integrity of the election results. The implication of this is that if anyone handling the results cartridges from the time the polls close to the time of tabulation can alter the results without detection.

The AVC Edge and Estonian voting system both have serious flaws that can impact the integrity of the election. The AVC Edge must use modern encryption standards and cease using CRC as a MAC. This is a relatively easy problem to fix. However, in the Estonian voting system, the inability of election officials to control client security can once again lead to integrity issues. Unlike the DRE issues, there is no reasonable method to ensuring malware is prevented on all clients. Therefore, even though it is flawed, the AVC Edge does a better job of protecting integrity.

C. Availability

The availability prong of the CIA triad refers to ensuring that the information can actually be accessed by the appropriate parties. Availability is important because there is no point to securing information systems if that information cannot be accessed. Of course, the best way to have perfect integrity and confidentiality is to simply unplug the servers and computers. However, this would make the availability very poor.

The most common threat to availability is a denial of service (DOS) attack. This is when a machine or group of machines flood an information system with so much information that the system cannot receive legitimate information. Both DRE and Internet voting infrastructures utilize servers to tabulate and store votes, so threats appear to be relatively similar on both. One large difference between the two systems is that in internet voting, the Vote Forwarding Server (VFS) is connected to the internet. It receives HTTPS traffic from people submitting their votes. DRE Servers are not required to be connected to the internet because ballots are transferred directly from removable media such as results cartridges. Connectivity to the internet automatically opens the door to new threats, and these threats can come from anywhere in the world.

One such DOS threat was identified by Halderman et al. The vulnerability is an attack designed to fill the log partition of the server. His paper explains that "By sending many specially crafted requests containing fields with very long names, an attacker can exhaust the server's log storage, after which it will fail to accept any new votes [9]. Halderman estimated that such an attack would fill up the log partition in about 75 minutes. When election windows are only a matter of a day or days, a loss of availability for any significant time period could be a major inconvenience.

In addition to targeting servers and other election infrastructure itself, larger scale attacks could lead to availability losses. Since both DRE and Internet voting require electricity, a major attack on critical infrastructure such as the power grid would impact availability. A power grid failure will affect DRE and internet voting in similar ways. Additionally, traditional denial of service attacks can affect the servers in both systems similarly. The major difference then is the VFS being connected to the internet. This creates an additional attack surface that is unavailable when trying to attack a DRE infrastructure. However, utilizing a well thought out web service security system, including using TLS, could mitigate the inherent risk of internet voting.

While both systems have significant vulnerabilities across all triad prongs, the DRE is still the more secure option for voting. The DRE security flaws are largely implementation issues including poor encryption standards and not rotating secret keys. These issues are fixable and could be more easily avoided by releasing source code to the information security community. The internet voting issues, however, are conceptual such as requiring internet connected servers or the inability to stop malware during client-side attacks. Even though DREs are more secure today, the security community must continue it's work in attempting to develop an adequately secure internet voting infrastructure. The potential benefits it could provide to democracy are too great to ignore.

V. Role of Government

The American system of federalism as it applies to elections creates an interesting dynamic when it comes to election security. The US Constitution provides that states have control over "The times, places and manner of holding elections" but continues to say "but the Congress may at any time by law make or alter such regulations" [17]. Because states are given most authority over elections, the final say of what voting equipment they use lies with state election officials. However, federal entities such as National Institutes of Standards and Technology (NIST), Election Assistance Commission (EAC), and Federal Elections Commission (FEC) have the significant resources needed to ensure election security. This has required a strong relationship to develop between the states and federal government.

The EAC is an instance of federal government working with state governments to help better voting security. Relevant to this paper, one function of the EAC is that it "operates a voting system testing and certification program. This program certifies, decertifies and recertifies voting system

hardware and software and accredits test laboratories" [17]. In addition to a certification program, the EAC routinely publishes the Voluntary Voting System Guidelines (VVSG). VVSG provides a "set of specifications and requirements against which voting systems can be tested to determine if the systems meet required standards" [17]. The VVSG guidelines include encryption recommendations. For example, the 2015 VVSP requires that machines transmitting data wirelessly "Cryptography used for encryption and authentication shall use NIST approved algorithms with security strength of at least 112 bits. Message Authentication Code (MAC) keys shall have a security strength of at least 112 bits" (Election Assistance Commission VVSG) [18]. These are good cryptographic recommendations and is useful in determining which systems are secure.

While this is a useful publication, its flaw is also the first word, voluntary. The EAC Certification program is also voluntary. In January 2011, EAC conducted an analysis of what states have statutes or regulations requiring compliance with federal programs such as VVSG. The study found that 20 states had no regulations requiring their voting systems meet Federal requirements. Additionally, only 13 states required federally certified election machines. The other states only required testing of machines either in or out of a federally accredited lab [18]. While it is a positive sign that there are federal resources available to states to ensure election security, most states are not taking advantage of that.

In addition to EAC, the Department of Homeland Security (DHS) is developing new programs in its newly expanded role in protecting election infrastructure. To best prioritize where resources should be focused, DHS has a list of critical infrastructures. Until recently, elections and voting were not considered critical infrastructure. However, on January 6, 2017 DHS Press Secretary Jeh Johnson announced that election infrastructure would be "designated as a subsector of the existing Government Facilities critical infrastructure sector" [19]. The press release went on to state that the designation "Enables this Department to prioritize our cybersecurity assistance to state and local election officials". However, similar to the EAC regulations, DHS made clear that the assistance is only for those who request it and that this is not a federal takeover of election systems.

While Federal programs have the financial and intellectual resources to ensure election security, they do not have the authority. This authority of course lies with state election officials. In an ideal world, all 50 states would have their own well-funded election security teams that can set standards, test and certify voting machines, and adequately address all election security concerns. Ideally, these teams would be staffed with brilliant security experts, cryptographers, engineers, and risk management experts. However, it is unreasonable to expect all 50 states to maintain such a system. However, Federal agencies such as NIST, EAC, and DHS do have those resources available to states. However, as evidenced by the lack of states that require federally certified machines, it is clear states are not taking full advantage of these systems. A boon to election security would be for the Federal government to more aggressively market their services to state governments. Also, state governments must do a better job of utilizing the expertise available to them from the Federal government.

VI. Conclusion

As the threat to US elections continues to grow, increased efforts must be made to harden the information systems used to conduct the elections. While no information system is completely secure, there are obvious steps that can be made to improve election security in the United States. Because democracy is an ideal respected across all levels of society, all stakeholders have an interest in protecting elections. Therefore, it would be beneficial to everyone to work together including DRE manufacturers, local election officials, state governments, federal governments, academia, and the information security industry. DRE manufacturers should publish source code to leverage the expertise available in academia and the information security sector. This can help prevent security flaws such as those highlighted in the AVC Edge. After all, these vulnerabilities were only discovered after a review of the source code. Additionally, all levels of government need to engage with one another to provide proper oversight of voting infrastructure. While the Federal government is limited in what it can do from an implementation standpoint, it does offer useful resources that are impossible to have at the state level. State governments must take advantage of these resources. Lastly, internet voting is an interesting concept that has been sparsely implemented globally. While it has significant vulnerabilities, which will be difficult to overcome, it is still a young system and an avenue worth exploring. The potential benefits to increased democratic participation are significant and researchers must continue to diligently work to develop a secure internet voting system. Overall, the election system in the US has flaws. However, in the face of powerful adversaries attempting to harm our election system, it is now more than ever necessary for all stakeholders to work together to combat this threat. They must do so, or risk watching American democracy erode.

References

[1] United Nations, "Universal Declaration of Human Rights," 10 December 1948. [Online]. [Accessed 10 03 2018].

[2] S. Liles, "Russian Interference in US Elections," 21 June 2017. [Online]. [Accessed 10 March 2018].

[3] D. Coats, "Global Threats and National Security," 13 February 2018. [Online]. [Accessed 10 March 2018].

[4] L. Norden, "The Machine of Democracy," 2006. [Online]. [Accessed 11 March 2018].

[5] Verified Voting, "The Verifier - Polling Place Equipment - November 2018," 2017. [Online]. [Accessed 10 March 2017].

[6] M. e. a. Blaze, "Source Code Review of the Sequoia Voting System," 20 July 2007. [Online]. Available: http://votingsystems.cdn.sos.ca.gov/oversight/ttbr/sequoia-source-public-jul26.pdf. [Accessed 10 03 2018].

[7] NIST, "NIST Special Publication 800-57," January 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r4.pdf. [Accessed 17 March 2018].

[8] Valimised.ee, "Statistics about Internet Voting in Estonia," [Online]. Available: https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia. [Accessed 17 March 2018].

[9] J. A. e. a. Halderman, "Security Analysis of the Estonian Internet Voting System," in *21st ACM Conference on Computer and Communications Security*, Scottsdale, AZ, 2014.

[10] Revealnews.org, "Forget rigged polls: Internet voting is the real election threat," 3 November 2016. [Online]. Available: https://www.revealnews.org/article/forget-rigged-polls-internet-voting-is-the-real-election-threat/. [Accessed 17 March 2018].

[11] USA Today, "Internet voting is just too hackable, say security experts," 28 January 2016. [Online]. Available: https://www.usatoday.com/story/tech/news/2016/01/28/internet-voting-not-ready-prime-time-security-risks/79456776/. [Accessed 17 March 2018].

[12] NIST, "Federal Information Processing Standards Publication," February 2004`. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf. [Accessed 18 March 2018].

[13] State of Delaware, "Article V, Elections," 1897. [Online]. Available: http://delcode.delaware.gov/constitution/constitution-06.shtml#TopOfPage. [Accessed 18 March 2018].

[14] NIST SP800-83, "SP800-83," November 2005. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-83.pdf. [Accessed 18 March 2018].

[15] FireEye, "What is a Zero-Day Exploit," 2018. [Online]. Available: https://www.fireeye.com/current-threats/what-is-a-zero-day-exploit.html#dismiss-lightbox. [Accessed 18 March 2018].

[16] W. Stallings, Cryptography and Network Security, Hoboken, NJ: Peason, 2017, p. 366.

[17] Election Assistance Commission, "System Certification Process," [Online]. Available: https://www.eac.gov/voting-equipment/system-certification-process-s/. [Accessed 18 March 2018].

[18] Virginia Department of Elections, "INTERIM REPORT ON VOTING EQUIPMENT PERFORMANCE, USAGE AND CERTIFICATION," 15 April 2015. [Online]. Available: https://www.elections.virginia.gov/WebDocs/VotingEquipReport/2.pdf. [Accessed 17 March 2018].

[19] M. e. a. Alvarez, "Internet Voting in Comparitive Perspective: The Case of Estonia," *PS: Political Science and Politics, Vol.42, No.3,* pp. 497-505, 2009.

[20] Election Assistance Commission, "2015 Vountary Voting System Guidelines," 2015. [Online]. Available: https://www.eac.gov/assets/1/28/VVSG.1.1.VOL.1.FINAL1.pdf. [Accessed 18 March 2018].

[21] J. Johnson, "Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector," 6 January 2017. [Online]. Available: https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical. [Accessed 18 March 2018].

[22] *US Constitution.*

Author Biographies

Luke Hoffman is a graduate student in the Forensic Science of High Technology Crime program at University of Baltimore. Luke has held multiple positions in national security in the Washington, DC area. Luke's professional interests include computer forensics, national security, and intelligence.

Nima Zahadat, PhD, is the director of the Forensic Science of High Technology Crime program at the University of Baltimore. Zahadat has also worked extensively with U.S. government agencies and the public and private sectors throughout the years. He has an undergraduate degree in Mathematics from George Mason, a graduate degree in Information Systems from the George Washington University, and a Ph.D. in Systems Engineering and Engineering Management from the George Washington University. Zahadat's research interests are mobile security with a focus on BYOD, information security, virtualization, data mining and information visualization and online education.