Evaluating Mail-Based Security for Electoral Processes Using Attack Trees

Natalie Scala, nscala@towson.edu

Abstract

Since the reports of Russian interference in the 2016 United States General Election, the security of voting processes has received increased attention from both state and federal authorities. The declaration by the U.S. Department of Homeland Security in January 2017 that election systems be classified as the seventeenth component of critical infrastructure is just the beginning of a need for more secure voting processes. More recently, the COVID-19 pandemic and the 2020 U.S. General Election has placed greater emphasis specifically on mail-based voting processes for electoral systems. The objective of this research is to provide greater insight into potential threats to mail-based voting processes. Upon identifying an attack tree as an initial structure for evaluation, new threats are postulated, and an updated tree is proposed that accounts for more recent activities. Then, using an established assessment framework, the relative likelihood of each mail-based voting process attack scenario is identified. The results facilitate providing election officials and policy makers with greater knowledge of how mail-based voting system vulnerabilities develop as well as specific security measures that may be most beneficial.

Keywords: Mail-based voting, attack tree, electoral systems, threats, utility analysis

1. INTRODUCTION

The 2016 United States General Election was unprecedented, as widespread foreign interference and meddling were reported (*New York Times*, 2021). Specifically in 2019, the U.S. Senate Intelligence Committee confirmed that all 50 states were subject to some form of attack on their elections process in 2016 (Sanger & Edmonson, 2019). Such activity inherently brought increased focus to the 2020 General Election, especially given that Special Counsel Robert Mueller III testified to Congress in 2019 that interference was ongoing and continuing (Mueller, 2019). To exacerbate matters, the COVID-19 pandemic became a global crisis in March 2020; states began shutting down in-person activity, transitioning to socially distant pickups and remote working almost overnight. Questions about continuing with the elections process ensued, and many states quickly pivoted to mail-based voting methods for the primaries that were in-process during March 2020 and scheduled to continue throughout the summer. For example, after early voting began, the state of Ohio cancelled the in-person, day-of voting for their primary election the night before Election Day and shifted to an extended absentee-only, mail-based vote for two additional months. As the COVID-19 pandemic failed to abate, the need for expanded mail-based voting for the November 2020 General Election became apparent.

With the increased use of mail-based voting, an examination of the related threats to the process and mitigation for those threats is needed. Election infrastructure, such as voting systems, the associated infrastructure, and storage for ballots and equipment, are classified as critical infrastructure in the Government Facilities sector by the U.S. Department of Homeland Security. Critical elections infrastructure does not include political action committees, campaigns, or other non-government election groups (US DHS, 2020); classification as critical infrastructure reflects

the fundamental need to secure votes, including those cast by mail, to support confidence in voting as a fundamental democratic function.

To address the critical infrastructure and adversarial needs related to mail-based voting, this research involves the development of an updated attack tree that extends identified threats along with a utility-framed probabilistic analysis, based on cost and difficulty, for the relative likelihood of those threats. The goal is to examine the mail-based voting process on a holistic and comprehensive scale, identifying the highest risks and threats that must be mitigated. Mail-based voting will continue beyond COVID-19, at a minimum as an absentee process and conceivably with continued widescale use, so such an investigation has implications beyond the 2020 elections. The starting point for this research is the mail-based voting attack tree defined by the Elections Assistance Commission (EAC) and the University of South Alabama (US EAC, 2009). At the time, the assessment was considered comprehensive and exhaustive of threats to the mail-based voting process; however, a lot has changed since 2009. For instance, Colorado, Hawaii, and Utah have transitioned to all, or mostly, mail ballots to facilitate voting, joining Oregon and Washington, which had the policy before 2009; also, advances in voter access, such as ballot drop boxes, have grown.

Regardless of the COVID-19 pandemic, a fresh examination of mail-based voting threats is needed, as threat evolves with the sophistication of the adversary and advances in technology. The US EAC (2009) assessment of mail voting is just an inventory of risks and does not identify the strength or likelihood of those vulnerabilities. This research addresses that gap by not only enumerating an updated list of relevant threats but also quantifying risk and assessing if the true threat to mail-based voting is from an external adversarial actor, insider to the process, or voter error. Finally, most electoral security research is symmetric in nature, only considering the threat

of an external actor, and tends to focus on voting equipment as the problem source. Threats to a voting process, however, are asymmetric in nature, to include insiders, and may involve other factors at the source of the problem, such as voter influence, registration fraud, and so forth. This research develops a holistic threat assessment that addresses each of these concerns. To further motivate the problem, we begin with a review on electoral security threats, the mail-based voting process, and election security research since 2016.

2. PREVIOUS RESEARCH

The Help America Vote Act of 2002 made sweeping reforms to the nation's voting processes to include voting systems and voter access (US EAC, 2018). Changes to voting systems included electronic equipment and the phasing out of paper punch cards that became a point of contention during the 2000 Presidential election and *Bush v. Gore* judicial proceedings. However, literature devoted to risk and threat to electronic voting systems that have now been in use for about 20 years is incomplete and underdeveloped.

This may be attributed to the fact that multiple types of electronic voting systems exist, causing diversity in processes and implementation; two equipment examples are optical scanners and direct recording equipment (DRE). Furthermore, industry, and not academics, primarily developed and implemented these electronic systems, so scholarly documentation and models mostly do not exist. Prior to 2020, the most academic-focused and detailed work was presented in a report by the University of South Alabama and for the United States Election Assistance Commission (US EAC, 2009). Although this report includes attack trees and potential vulnerabilities, it studied dated equipment and processes. Furthermore, as previously noted, the index of threats is now incomplete as time has evolved.

More recent research by Cahn (2017) documents vulnerabilities to electronic voting systems and provides a literature review of known events and attacks that occurred in live voting systems within the United States. Specifically, they examined a number of systems, including the Sequoia AVC Advantage and the Hart InterCivic eSlate, which have been in place in various locales across the country. However, the research serves only as an inventory of known issues and threats and does not present a model that can be used to addresses the vulnerabilities and corresponding risk. In addition, many of the vulnerabilities identified in Cahn (2017) are reflected in the subsequent DEFCON Voting Village reports, which highlight successful controlled hacks of sample voting equipment (Blaze, et al., 2017; Blaze, et al., 2018; Blaze, et al., 2019).

Other research in voting includes Shackelford, et al. (2017), which outlines how countries such as South Africa, Estonia, and India approach protecting their electronic systems; Simons and Jones (2012), which discusses the potential for Internet voting in the United States; and Wolchok, et al. (2012), which presents lessons learned during an Internet voting pilot in D.C. Note that all of this research specifically focuses on the electronic systems for casting ballots, which are typically used at polling places during in-person voting. Votes cast by mail are typically done on paper and returned through the United States Postal Service or at a designated ballot return location. The literature does not address that process and does not address threats to that process, outside of US EAC (2009).

Since 2016, a series of policy papers (e.g., Center for Internet Security, 2018; Belfer Center 2018) have been released that propose best practices for states to improve security of voting systems. These papers are mostly high-level playbooks that have little research motivation. The recommendations are standard and not tailored for a specific state or polling place, and they do not address mail-based voting. As another example, RAND specifically addressed the 2020 election

in their report, considering social distancing and processes that reduce in-person contact (Kavanagh, et al., 2020). Although the report gives considerable treatment to policy concerns and state flexibility in adapting to COVID-19 restrictions and precautions, it does not address specific threats and vulnerabilities that arise from these changes.

Moreover, there is very little recent work that has comprehensively looked at the security and integrity threats arising from an increased use mail-based voting in national elections. Lee (2020) examines online, blockchain, and mail-based voting security in the context of a global pandemic, developing and applying a basic cybersecurity evaluation framework that assesses the software independence, accuracy, fairness, trustworthiness, and integrity of a secret vote. Yet, the developed cybersecurity evaluation framework only provides high-level cybersecurity judgements of voting methods and does not provide specific threat analyses. Benkler, et al. (2020) and Pennycook and Rand (2021) examine the specific mail-based voting threat of disinformation efforts to paint mail-based voting as susceptible to widespread fraud but do not investigate mail-based voting threats holistically.

3. METHODOLOGY DEVELOPMENT

3.1. Identifying an Initial Threat Structure

To analyze vulnerabilities in a process or system, an attack tree is a useful technique that is well-documented in the defense and security literature. The method involves identifying various attack avenues (branches) an external actor may take toward achieving its objectives. Using a hierarchical diagram in conjunction with a combination of A (AND), O (OR), or T (terminal) nodes, a measurement or value for each branch is evaluated to determine the likelihood of any one scenario occurring. A benefit of an attack tree is the ability to decompose complex actions into hierarchical levels, terminating at the lowest level of single actions that must be taken. This

decomposition systemically enumerates all threats, aiding in the understanding of the full scope of the problem and needed countermeasures (Goethals, et al., 2021). The methodology was first observed in the literature in the late 1990s (Schneier, 1999) and has been used extensively in studies on information systems (Saini et al., 2008; Selvi et al., 2014; Prasad and Avadhani, 2019). A full review of almost 200 examples of attack trees and graphs along with their use of visual syntax can be found in Lallie, et al. (2020).

In 2009, the U.S. Election Assistance Commission (EAC), an independent and bipartisan commission developed as part of the Help America Vote Act of 2002, sponsored an assessment of election operations performed by an interdisciplinary advisory board from the University of South Alabama (US EAC, 2009). The board utilized NIST threat definitions as a basis for developing attack scenarios for six different voting systems, one of which was the mail-based voting process. The contribution was an attack tree capturing the potential vulnerabilities from both insider and external threats, as well as threats from unintentional voter error. Attack scenarios included a breadth of activities ranging from the coercion of voters using advertisements to the registration of deceased votes through masquerade attacks. The attack tree hierarchical diagram included branches for the insider threat (1), external threat (2 and 3), and voter error (4) with a legend for the A (AND), O (OR), and T (terminal) nodes. The basic structure of the nodes for the EAC mail voting attack tree can be observed in Figure 1 and the entire original attack tree outline is provided in Appendix I.

Insert Figure 1 here.

Attack scenarios occur at the lowest levels of the attack tree hierarchy and are built from terminal nodes (denoted by circles). Terminal nodes that roll up to OR nodes (denoted by modified triangles) on the attack tree are essentially singular or unique attack scenarios; at an OR node, at

least one activity needs to occur to breach the system. At an AND node (denoted by flat-bottom half-moons), all terminal node activities must occur in order for the system to be breached; therefore, the entire set of terminal nodes extending from an AND node to the lowest level becomes an attack scenario. Following that logic and Figure 1, within the insider threat branch (1), there are 32 possible unique combinations of attack scenarios at various points in the voting process, depending on how knowledge is gathered, how access is attained, and which attack method is used. This compares to a total of 16 possible attack scenario combinations from an external threat (7 scenarios on branch 2 and 9 scenarios on branch 3), and 9 possible attacks aligned to voter error (i.e., branch 4).

3.2. Framework Assumptions

Before examining revisions to the mail-based voting process and attack tree from over a decade ago (US EAC, 2009), some assumptions should be identified and explained. Up front, it is important to note that counties or localities within the same state may have slight variations of mail-based processes for their voting systems; states, in comparison, may have more marked differences between each other. For example, the number of ballot drop-off and collection devices or locations may not be consistent between counties within the same state, and ballot instructions may have slight variations due to the number of electoral races to vote. In contrast, rules for improperly marked ballots may vary between different states, and ballot drop-off boxes are not even used in some states. The variation in rules and process is due to the separation of powers and the responsibility of elections delegated to the states. Some states choose to standardize their voting process and equipment across the state, while other states delegate process design and equipment choice to their individual counties and localities. Although processes may vary within the state, the election laws of that state are consistently upheld across counties and districts. States

that do not have a standardized process will inherently have more variety or inconsistency between counties but not necessarily a more vulnerable system. Locraft, et al. (2019) review and identify states with standardized and non-standardized processes during the 2016 U.S. General Election and conclude that non-standardized states were targeted by adversaries less frequently.

By the nature of the attack tree produced by the US EAC (2009) assessment, it can be inferred that its focus is primarily aligned to the national or statewide election; not every election at the local level will include every sub-process identified in the study. However, by updating the attack tree to account for all potential vulnerabilities that may exist, it can be fine-tuned to support modeling processes at the national, state, or local levels. In summary, the attack tree scenarios should account for all possible activities that can breach a voting system; yet not every voting process may have the same unique combinations of relevant attack scenarios. A list of assumptions to revising the mail-based voting attack tree structure includes:

i. Counties and localities have the resources needed to sufficiently perform the mail-based voting process; they are not negatively affected in terms of personnel, facilities, equipment, service support activities, or other resources.

ii. A state's process for what is defined specifically as "absentee ballot" voting is a subset of the mail-based voting process. Since every absentee ballot is counted, even if it is counted days after an election, the threat of not counting these ballots is the same as not counting a mail-based ballot.

iii. Mail-based ballots are stored in a centralized secure location within a facility by means of a lock or safe combination. This includes blank ballots to be sent to voters as well as returned marked ballots. The centralized location for blank and returned ballots may not be the same geographic address, but all blank ballots as well as all returned ballots are stored together.

iv. All mail-based ballots are read at the local election office using an optical scanner device. Here, "local" is used in a generic context to identify with a town or city where authorized officials count and certify votes in that jurisdiction (NIST, 2020).

v. All mail-in ballots are validated at the local election's office using IT-based voter registration records which are U.S. critical infrastructure.

3.3. Investigating Attack Tree Revisions

To revise the initial US EAC (2009) attack trees for mail-based voting to include pandemic implications, threats to critical infrastructure, and the adaptive adversary, a systemic process was used. First, threats and implications discussed in local and national mainstream media were inventoried, using non-partisan news articles printed between January and August 2020 (e.g., *The Washington Post*, *The New York Times*). Then, documentation from bipartisan or non-political think tanks and organizations, along with academic centers, were used to verify the mail-based voting process and potential threats related to that process (e.g., NCSL, 2021; Kavanagh, et al., 2020; Baringer, et al., 2020). Voter instruction sheets and state-created documentation from multiple states were also reviewed (e.g., Maryland State Board of Elections, n.d.; Maryland Office of the Attorney General, n.d.; Howard County, 2020).

Finally, as a means of validation and to ensure that a holistic approach was taken to identify all potential threats, the mail-based process was discussed extensively with Board of Elections officials in the state of Maryland. A series of interviews and discussions took place during summer 2020 during which questions about attack tree branches and relevant stakeholders were presented, and the officials validated the threat or provided feedback. The officials also provided detailed notes that described the voting process and stakeholders involved in the mail-based process, from ballot request (typically an absentee form from the voter), to mailing the ballot, its subsequent

return by the voter, and to counting the ballot. Although other states may have slightly different processes, Maryland was chosen for validation and feedback because it has already been studied in the literature; the state's in-person process has received extensive treatment. Price et al. (2019) indicated 25 threats specific to polling places in Maryland, designated as cyber, physical, and insider threats; the list of those threats was adapted for mail-based voting and included in this research, considering if and how they apply to a mail-based system. Locraft, et al. (2019) proposed influence diagrams of sources of cyber, physical, and insider threat, and those sources of threat along with media reporting were used in an expertise-based brainstorm of new threats for the updated attack tree to identify potential threats. Although Locraft, et al. (2019) discuss the relative security of Maryland's process, the contribution of influence diagrams was made from a general perspective, and a non state-specific approach was taken in the brainstorm of new threats for mail-based voting. Scala, et al. (2020b) detail methods for training of poll workers; that training includes education on potential threats that may emerge at polling places. The threats in those training modules were reviewed and adapted for mail-based voting as appropriate. Finally, poll worker training manuals for Maryland were used to identify any remaining process vulnerabilities (Keene & Livingston, 2016).

In total, 30 new threats were identified to mail-based voting and are included in the updated mail-based attack tree in Figure 2; an outline of the updated attack tree can be found in Appendix II. Note, the updated tree now includes a total of 40 scenarios for insider threats (branch 1), 23 attack scenarios from external threats (branches 2 and 3), and 10 possible attacks aligned to voter error (branch 4). Table 1 enumerates the 30 new threats, with identification as insider actor, external actor, or voter human error; the assigned threat identifier number; and reference source

that detail the existence of or potential for the vulnerability. Threats denoted as ab intra are derived from expertise and the brainstorm.

Insert Figure 2 here.

Insert Table 1 here.

To incorporate these threats into the existing US EAC (2009) threat tree, an evaluation process was used. First, each threat was considered as to where it fits within the four branches of the mail voting attack tree: insider threat (branch 1), masquerade (external threat, branch 2), voting process (external threat, branch 3), or errors in system processes (voter error, branch 4). Next, to evaluate where a threat fits within a branch, three considerations were made: (i) if the threat fits in a general or node category; (ii) if anything else has to happen jointly to execute the threat; and, (iii) if the threat is terminal. Then, considering the definition of the threat, the scope of the attack, and reference support, the threat was merged into an AND node if an additional action or threat needed to occur in parallel for execution, into an OR node if it was completely related to other threats but could be executed alone, or developed into a singular terminal leaf node if it could be executed alone and was unrelated to other threats.

To illustrate this process, consider threat X_{77}, "manipulate return envelope." Ballots may be rejected for counting due to errors with their return envelopes. The errors void the vote and are often made by individuals other than the voter. Stakeholders in an internal attack include election judges, challengers, county tech personnel, support staff, and Board of Elections staff. After the voter mails their ballot, it is in the hands of any of these personnel; a nefarious insider may then manipulate it so that it will become voided. X_{77} aligns with OR node 1.5 "manipulate or discard votable ballot" and OR node 1.5.1 "delete at local election office" on the US EAC (2009) tree, as it is a singular action within this group of threats. Election officials can fail to properly stuff an

envelope, send a wrong or pre-marked ballot, misaddress the envelope, manipulate the return envelope, destroy the prepared envelope, or destroy a batch of prepared envelopes. Each of these activities can cause an error with a return envelope and a ballot to be voided.

This logical approach was taken for all threats in Table 1 when incorporating them into the existing US EAC (2009) attack tree. The updated threat tree is, therefore, reflective of existing and current threats to mail-based voting. To extend the contribution of the updated tree, an evaluation of the risk associated with all threats was developed. Such an evaluation is novel and does not exist in the literature for any attack tree related to election security, regardless of the method of voting (mail, in person, etc.).

3.4. Establishing an Evaluation Measure

To assess the likelihood of an attack scenario, an evaluation measure must first be established. Any number of attributes may be examined to produce a scoring framework, such as impact, physical cost, detectability, attack time, etc. Bagnato, et al. (2015) provide a review of different attributes for decorating attack trees and the types of processes that are most closely related to them. For a voting process, in particular, there are clearly costs to an attacker, which may come in the form of total monetary expenses to produce the effect or execute a breach. Costs may also be qualitative, in terms of the inherent risk in being captured, the magnitude of effort to create an outcome, or the technical skill and training needed to execute a breach. There are also varying levels of difficulty in executing each scenario. Finally, the success of an attack scenario is tied to the difficulty of discovering it from an information assurance perspective; given a high chance for retribution or capture, an adversary may be less likely to perform a malicious act. Du and Zhu (2013) proposed the use of a quantitative evaluation standard examining three attributes for a vehicular ad hoc network: attack cost (AC), technical difficulty (TD), and discovering

difficulty (DD). Attack cost and technical difficulty are viewed from the adversarial perspective and are, respectively, defined as the costs associated with executing an attack on the system and the skill needed for the adversary to perform the attack. Discovering difficulty reflects the skill and resources needed for the victim to realize they have been attacked or breached. Then, multi-attribute utility theory can be used to evaluate the attributes as the attacker's utility value, which then represents the relative likelihood of the execution of a terminal node on the attack tree (Du and Zhu, 2013).

A similar construct is proposed for this model but with the resulting three utility functions for AC, TD, and DD – u_1, u_2, and u_3, respectively, – defined in terms of threat-related activities in a voting process. Table 2 defines the ordinal scales for assessing the attributes; these criteria are adapted from Du and Zhu (2013) by maintaining the 1 to 5 ordinal structure but defining standards for voting systems (instead of vehicular networks). Utility assessments of each attribute are then needed for every terminal node.

Insert Table 2 here.

Assessing the threat scenarios based upon the indicated ordinal grade and accompanying standards should be explained in terms of its applicability to the voting process. In terms of relative likelihood, each of the threats in the updated attack tree discussed in Section 3.3 has some potential cost, degree of difficulty, and discoverability associated with it. Regarding the attack cost, the consequences of capture are less likely for a remote network attack from a malicious actor outside of a county or locality versus that of a direct attack on a mail voting or poll facility; hence, we would anticipate the attack cost to mirror this relationship. For an example of technical difficulty, successfully performing an act of discouraging or misinforming voters (e.g., social media influence) is assessed to be an easier task to complete by an adversary than accessing ballots, pre-

marking them, and entering the ballots into the voting pool. Finally, it is more likely that local election officials will discover problems in the ballot design or voter registration instructions rather than malware injected into a machine locally.

Using the evaluation grades in Table 2 for each utility function, the relative likelihood for each terminal node, X_j, in the attack tree is calculated using the additive weighted formula,

$P(X_j) = w_1 u_{1j} + w_2 u_{2j} + w_3 u_{3j}$, where $j \in \{1, 2, ..., n\}$, with n representing the number of terminal nodes in the tree and $w_k, k \in \{1,2,3\}$, representing the weight applied to a specific utility function. In this construct, the weights are designed to sum to one, and $u \in [0,1]$ using a scale factor to convert the ordinal scale to this range. Each attack scenario is either a single terminal node or a combination of terminal nodes depending on the OR and AND node structures on the branches of the attack tree. The scenarios, as viewed from the threat agent perspective, are assumed to be independent of one another. Accordingly, once the ith attack scenario is identified, $S_i = (X_{i1}, X_{i2}, ..., X_{iN})$, its relative likelihood may be calculated using the formula

$P(S_i) = P(X_{i1})P(X_{i2}) \cdots P(X_{iN})$ for an AND tree structure; the formula reduces to $P(S_i) = P(X_{i1})$ for the singular terminal node OR structure. It is important to note that the AND/OR combinations in this formulation are not considered as sequential conjunctive components but rather as sets; as such, calculations are not accounted for as conditional probabilities.

The resulting measurement evaluates scenarios that are high cost, very difficult to pursue, and easy to discover as being least likely to occur. Due to the subjective nature of assessing the grades for each terminal node and the scaling used, the specific value of relative likelihood provides very little interpretation with respect to the chance of a single scenario occurring.

However, an attack scenario's relative likelihood *does* provide a useful index for comparison with other scenarios; the measurement enables identification of whether attack scenarios from insiders, external actors, or voter human error are more probable. Perhaps more importantly, the relative likelihood enables comparison of the attack scenarios in terms of their relative magnitude, thus facilitating prioritization of security efforts and resources.

To calculate relative likelihood, an assessment of the utility functions $u_1, u_2,$ and u_3 need to be made for every terminal node. To achieve this, the attack cost (u_1), technical difficulty (u_2) and discovering difficulty (u_3) rubric from Table 2 are applied to the nodes. The subjective nature of the rubric can create challenges in terms of precision in assessing utility. To assuage this, the Delphi Method was used with a team of three decision makers to assess the grades for every utility function and every terminal node. The Delphi Method is an iterative process for making quantitative judgments to facilitate group decision making (Goodwin & Wright, 1998). The method allows for discourse between decision makers, including the discussion of approaches taken and potential implicit biases, without attribution. By doing so, decision makers may understand the viewpoints of others and revise or update their assessments as appropriate throughout the iterations of the exercise. Consensus can be reached rather expeditiously when the method is truly without attribution, power dynamics, and group think, along with the decision makers appropriately educated on the decision space. For further information on the method, please refer to the seminal works of Dalkey and Helmer (1963) and Helmer-Hirschberg (1967).

For this research, three decision makers first independently assessed the three utility functions for every terminal node threat. A moderator then merged all scores and assessments into a single spreadsheet so all decision makers could review the initial values without attribution.

Discussion followed regarding definition or scope of threats, key points, and approaches to the assessment and continued until consensus was achieved.

The decision makers in this work are experts in the academic study of elections security. They approached the assessment using their research knowledge, the literature, and experience from working with counties' data. Similar approaches are taken in Feng and Keller (2006), where the group decision makers were experts on decision analysis and the decision space but not necessarily the corresponding policy, and Keeney and von Winterfeldt (2011), where the decision makers were managers and researchers at a DHS University Center of Excellence. Utility assessments may be different for established nation-states with advanced skill who are external adversarial actors or recipients of attacks (i.e., the Russian Federation vs. the United States in 2016). Inclusion of state-specific data may lead to a reassessment of threat grades; in that case, the relative likelihood model can be rerun to update the utilities amongst the threat scenarios. Furthermore, to ensure that the attack tree and the assessment of grades for the utility functions are as accurate as possible, an unbiased perspective must be taken. This research provides the initial assessment and framework for assessment of risk associated with nodes on the attack tree. An empirical validation of this assessment through sensitivity analysis is discussed in Section 4.2 and is compared to security outcomes in the 2020 U.S. General Election.

4. RESULTS AND DISCUSSION

4.1. Evaluating the Updated Mail-in Voting Attack Tree

Using the updated attack tree described in Section 3.3, relative likelihoods are calculated for each of the terminal nodes. Considering equal weighting of the utility functions for this example (i.e., $u_1 = u_2 = u_3 = \frac{1}{3}$) and a scale factor of 0.2 (i.e., conversion of the five-unit ordinal

scale), the evaluation measurements shown in Table 3 are calculated. Note that the additional threats from Table 1 are shaded for reference.

Converting the terminal nodes into attack scenarios and following the updated tree structure in Figure 2, Table 4 identifies potential attack scenarios for mail-based voting, along with the corresponding calculated relative likelihood. Note that a majority of the attack scenarios are related to insider threats, with relative likelihoods generally between 0.05 and 0.08. Most external attack scenarios have very low relative likelihood and imply that external actors may not be interested or incentivized to attack mail-based voting. Finally, ten scenarios are identified concerning voter error, or 13.7% of the total possible scenarios. Figure 3 depicts histograms of the attack scenarios by branch, identifying the relative likelihood of concern as well as the vast majority of attacks having relatively low likelihood.

To further investigate the spectrum of threats, Table 5 identifies the most and least likely attack scenarios for internal and external threats as well as those pertaining to voter error.

Overall, the three threats with the highest relative likelihood are X_{15} (0.15), X_{36} (0.13), and X_{65} (0.13). $S_{13} = \{X_{15}, X_{16}, X_{17}\}$, so the relative likelihood of that scenario reduces to 0.0006 as an AND node. $S_{32} = \{X_{36}\}$ and involves the ballot being lost in the destination mailroom, which is an internal attack. This occurs when the mail ballot or envelope is misplaced or destroyed at an intermediate mailroom after delivery from the postal system. $S_{64} = \{X_{65}\}$ and occurs when the voter fails to sign their ballot correctly, which can cause a ballot not to be counted. This threat is

classified as voter error because it arises when the signature match authentication fails due to minor deviations. $S_{58} = \{X_{61}\}$, which is a debate and vote party and a form of voter persuasion. At a debate and vote event, members may invite a voter to bring their blank mail ballot. The party members then influence the voter to fill out their ballot in a favorable way to the majority. This is dangerous because it can change a voter's choice. Voters are more likely to experience suppression tactics in a group setting, which is why debate and vote parties have a higher relative likelihood of threat than other methods, such as individual coercion.

The most likely scenarios for each branch of the attack tree occur at OR nodes. Identifying these scenarios along with their relative likelihoods can enable elections officials to focus on higher relative threats, employing limited resources wisely to secure mail votes. Thus, Table 4 can be used as a prioritization for resources; scenarios with higher relative likelihood should receive priority for mitigation and resource allocation. In a complicated and evolving threat landscape, Table 4 can allow election officials to focus their attention and understand the highest return for their mitigation efforts. Mitigation recommendations for the most and least likely threat scenarios for each branch are also included in Table 5; the mitigations are informed by Abrams (2020), Ballotpedia (n.d.), Braswell (2020), Carlisle (2020), Cremer (2020), Graham (2020), Janoff (2020), and Root, et al. (2020).

When deploying resources for mitigation, elections officials should focus on both the state and the voters. Informing voters with knowledge of clear guidelines related to voting mail ballots is imperative. Examples include instructions that are sent along with ballots as well as notifications of ballot status. Both actions assist in enabling voters to cast ballots that are valid. States also play an important role in the distribution of these mail ballots and providing necessary support to the voters. Training personnel, support staff, and elections officials how to properly follow

guidelines is important for the security of the election while maintaining efficiency. An example includes training election judges how to verify signatures, which can decrease rejected ballots and potentially save officials time that would have been spent on curing votes that were otherwise not verified properly.

Other scenarios with higher-than-average relative likelihood are listed in Table 6. Although these scenarios are not the overall highest threat in a given branch, they should have the attention of election officials and policy makers. Additional resources may be allocated to mitigate against these vulnerabilities; example mitigations include instructional videos for election officials and poll workers as well as simple visual aids developed and posted to help voters. Generally, the threat mitigations in Table 5 and Table 6 could begin at the start of the mail voting process to fully secure the integrity of mail-based votes.

Insert Table 6 here.

Note that each of the scenarios in Table 5 and Table 6 are included in the original US EAC (2009) attack tree, and none of the new threats in Table 1, which have evolved over time or are related to COVID-19, identify as high concern. Such analysis reflects that the quick move to mail-based voting at a large scale due to the pandemic does not necessarily make the mail voting process less safe. Although there is a subset of eight scenarios in Table 5 and Table 6 that identify with relative likelihoods above 0.10, mitigations can be put in place to address threat, including enhanced training for insiders and awareness initiatives to identify and prevent the threats from being executed. Additionally, note that, as described in Sections 3.2 and 3.3, the analysis completed in this work reflects that of a generalized mail-based voting process; to reduce any potential bias, further scenario or state specific customized analysis may be required for markedly different mail-based voting processes and/or training protocols.

Figure 4 presents a bubble chart of each threat to mail-based voting from the updated attack tree in Appendix II. The chart depicts the adversarial attributes of technical difficulty (u_2) and attack cost (u_1) on the *x*-axis and *y*-axis, respectively, and the information assurance attribute of discovering difficulty (u_3) as the relative size of the bubble for each threat. Data is graphed to reflect a total distance of four units on each axis, transforming data so that high relative likelihood threats are in the top right of the graph and lowest relative likelihood threats are in the bottom left quadrant. Observe that almost all external threats fall on the left-hand-side of the graph, below the threshold for higher risk or threats of concern. Attacking mail-based voting is difficult for an adversary; the actions are difficult and costly with a high chance they will be detected. Furthermore, the distributed nature of mail-based voting increases the adversarial attack difficulty; an election would involve thousands of USPS mailboxes and hundreds of drop boxes. An adversary would have to infiltrate many ballot return stations and mailboxes in order to have a marked impact on mail votes. Moreover, for the insider and voter error threats of concern, mitigations can lessen the chance the threat scenario is executed, and mitigations along with the sheer volume of votes cast can lessen the impact if one of those threats were actually executed. Other observations of note in Figure 4 are that, within the scope of this analysis, insider threats are relatively easier to discover, although the attack cost may vary, and that a vast majority of the external threats are of high difficulty.

Insert Figure 4 here.

Elections personnel can be trained to identify threats as they may arise to then execute a mitigation plan; officials and insiders can also be trained to avoid becoming insider threats themselves. In summary, although there are some risks to mail-based voting, its decentralized

nature suggests that the threat at a macroscopic scale is low; mitigations at the local level can prevent threats from existing and can lessen or minimize impact if they in fact do occur.

4.2. Sensitivity Analysis

Sensitivity analysis examines the robustness of the weights (w_1, w_2, w_3) for the utility functions (u_1, u_2, u_3) to determine any potential effect on relative likelihood calculations, particularly if scenarios of interest change with potential changes in weight. The weights may be tailored to fluctuate over time due to evolving priorities of elections officials and information assurance considerations as well as due to the varying sophistication of potential external and internal actors. Also, the model's uniform weight for every utility function does not necessarily address strength of preference for each attribute (AC, TD, DD). To account for any disparities, a sensitivity analysis was performed, whereby the weights of each attribute were varied from 0 to 1, holding the other weights constant, and normalizing the sum of all weights to 1. The focus of this discussion is on the top six most likely scenarios in terms of relative likelihood, to determine how changes in weighting affected the overall standing of these scenarios.

For attack cost (AC), S_{64} (voter error) remains the most likely threat unless the weight of AC shifts to 0.5; in that case, S_7 (insider threat) becomes the most likely threat. Mitigations for errant failed signatures include making sure election officials are trained and educated properly, having a second election official review a questionable signature during verification before rejecting the ballot, and setting up an automated system that checks signatures with human verification for questionable ballots. Relative likelihoods for three scenarios – S_{47}, S_{23}, and S_{58} – fall below 0.10 if the weight for AC moves to about 0.35, 0.45, and 0.65, respectively, showing some sensitivity in these results. If AC becomes more significant than TD or DD in evaluating

threats, these three scenarios lessen their importance. However, if the weight for AC shifts to less than about 0.2, then S_7 lessens in significance with a relative likelihood of less than 0.10.

For technical difficulty (TD), S_{64} (voter error) and S_{32} (insider threat) change in relative ranked significance with a small shift in weight for this attribute. S_{32} is the most likely threat on the insider branch of the attack tree; the sensitivity of a small change in weight highlights the need for policy makers and elections officials to anticipate the potential for ballots to be lost in destination mailrooms and consider corresponding mitigations for that threat. Similar to AC, S_{58}, S_{66}, and S_{23} fall in significance if the weight for TD decreases.

Finally, for discovering difficulty (DD), S_{64} (voter error) and S_{32} (insider threat) also change in relative ranked significance with a small shift in weight for DD. This once again highlights the need for strong mitigations and surveillance for these most likely threats. S_{66}, S_{23}, and S_7 lessen in significance with shifts in weight to 0.5 and above.

For all three attributes, all other scenarios remained below 0.10 relative likelihood when testing for sensitivity. Figure 5 depicts the sensitivity analysis graphs for AC, TD, and DD with respect to the six most likely scenarios. In the figure, the *x*-axis represents the weight of the attribute that is evaluated for sensitivity, with all other attribute weights constant but normalized, while the *y*-axis represents the relative likelihood for each threat scenario. It is noted that there are some crossovers when adjusting the weights, which suggests some sensitivity among the six different most likely scenarios. For instance, S_7 should be considered as most likely if the weight for AC shifts above 0.5. Despite small shifts in placement among the most likely six scenarios, depending on the weight of each attribute, none of the top six scenarios are supplanted by any of the other scenarios listed in Table 4. Hence, we can infer that this 'group' of six most likely

scenarios is less sensitive to the changes in the weights of the attributes. This offers some insight into the robustness of the threat structure for mail-based voting.

Insert Figure 5 here.

5. CONCLUSIONS AND EXTENSIONS

This research establishes an updated attack tree for mail-based voting plus an analytic utility-based assessment of the relative likelihood of those threats. The study is the first to consider likelihood of threat for elections security and also updates the only known attack tree for mail voting in U.S. elections. This research has direct implications for the security of U.S. elections and the security of the critical infrastructure of elections equipment.

In summary, the findings suggest that a majority of threat scenarios (40) are tied to insider actions, while 23 scenarios are for external or adversarial actions, and 10 threats are related to voter error. Eight threat scenarios are of highest relative likelihood (~11% of total scenarios and ~8% of total threats); as such, mitigations are presented for these threats on each branch of the attack tree. It is recognized that not every election process will have the same array of threat scenarios for mail-based voting; states may have cities with different policies or systems that warrant considering only portions of each threat category. In these instances, the comprehensive nature of the updated attack tree provided as part of this research can facilitate developing a more refined threat picture for a specific locality. Aggregating these threat pictures at the state level or even at the national level may provide new information on geographic vulnerability densities where state or national policy initiatives may be prioritized.

Future research, which involves understanding where vulnerabilities may exist in a mail-based voting process, is important. To prioritize defensive measures or mitigate against those vulnerabilities, an awareness of when they may occur in the voting process provides a significant

advantage. Process mapping and temporal analysis, such as Markov Chains, may address these concerns. The model and utility assessment may also be extended to attack trees for in-person voting on various types of equipment, such as precinct count optical scanners and direct recording equipment. The utility assessment could also be extended by including the direct input of elections officials in the ratings. In addition, an analysis of supporting resources, such as available poll workers, facilities, and materials may provide new information on threat characteristics. Finally, research in computer science and information assurance can address the strength of mitigations, develop metrics for security assessment, and also develop training for insiders to identify and mitigate threats while lessening the likelihood that trusted insiders become known threats. Similar training for poll workers (Scala, et al., 2020b) can be extended and designed for election officials and trusted insiders. This model extends beyond the 2020 U.S. General Election, as mail voting will continue to be used in some capacity, at a minimum as absentee voting, in future elections and in a post-pandemic society.

6. ACKNOWLEDGEMENTS

REFERENCES

Abraham, S., & Nair, S. (2014). Cyber security analytics: A stochastic model for security quantification using absorbing markov chains. *Journal of Communications*, *9*(12), 899–907. https://doi.org/10.12720/jcm.9.12.899-907

Abrams, A. (2020, September 30). Absentee ballot applications are not accessible to voters with disabilities in 43 states. *Time*. https://time.com/5894405/election-2020-absentee-ballot-applications-disability-rights/

Bagnato, A., Kordy, B., Meland, P. H., & Schweitzer, P. (2012). Attribute decoration of attack–
     defense trees. *International Journal of Secure Software Engineering (IJSSE)*, *3*(2), 1-35.
     https://doi.org/10.4018/jsse.2012040101

Ballotpedia. (n.d.) *Votes cast in the names of deceased people*.
     https://ballotpedia.org/Votes_cast_in_the_names_of_deceased_people

Baringer, A., Herron, M. C., & Smith, D. A. (2020). Voting by mail and ballot rejection: Lessons
     from Florida for elections in the age of the coronavirus. *Election Law Journal: Rules,
     Politics, and Policy*, *19*(3), 289–320. https://doi.org/10.1089/elj.2020.0658

Benkler, Y., Tilton, C., Etling, B., Roberts, H., Clark, J., Faris, R., Kaiser, J. & Schmitt, C.
     (2020). Mail-in voter fraud: Anatomy of a disinformation campaign. (Berkman Center
     Research Publication 2020-6). http://dx.doi.org/10.2139/ssrn.3703701

Belfer Center for Science and International Affairs (2018). The state and local election
     cybersecurity playbook. https://www.belfercenter.org/publication/state-and-local-
     election-cybersecurity-playbook

Blaze, M., Braun, J., & Advisors, C. G. (2017). DEFCON 25 voting machine hacking
     village. *Proceedings of DEFCON 25,* Washington DC, 1-18.

Blaze, M., Braun, J., Hursti, H., Jefferson, D., MacAlpine, M., & Moss, J. (2018). DEFCON 26
     voting village: Report on cyber vulnerabilities in us election equipment, databases, and
     infrastructure. *Proceedings of DEFCON 26*, Las Vegas, NV.

Blaze, M., Hursti, H., MacAlpine, M., Hanley, M., Moss, J., Wehr, R., Spencer, K. & Ferris, C.
     (2019). DEFCON 27 voting machine hacking village. *Proceedings of DEFCON 27*, Las
     Vegas, NV.

Bote, J. (2020, October 1). West Virginia mail carrier guilty of election fraud after altering ballot

requests to Republican. *USA Today*.

https://www.usatoday.com/story/news/nation/2020/07/10/west-virginia-mail-carrier-guilty-

election-fraud-altered-ballot-requests/5412010002/

Braswell, S. (2020). *Get rid of live audiences at presidential debates*.

https://www.ozy.com/news-and-politics/get-rid-of-live-audiences-at-presidential-

debates/71964/

Cahn, D. (2017). *Risk assessment: How secure are voting machines*. [Unpublished capstone

thesis]. University of Pennsylvania.

Center for Internet Security (2018). A handbook for elections infrastructure security.

https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-14-Feb.pdf

Carlisle, M. (2020, October 15). Have a problem with your mail-in ballot? Advocates are

pushing states to let you correct it. *Time*. https://time.com/5900567/mail-in-ballot-mistakes/

Cremer, J. (2020, October 15). Six common ballot mistakes to be aware of when you vote.

Alliance for Science. https://allianceforscience.cornell.edu/blog/2020/10/six-common-

ballot-mistakes-to-be-aware-of-when-you-vote/

Dalkey, N., & Helmer, O. (1963). An experimental application of the DELPHI method to the use

of experts. *Management Science*, *9*(3), 458–467. https://doi.org/10.1287/mnsc.9.3.458

United States Department of Homeland Security. (2020). *Election security*.

https://www.dhs.gov/topic/election-security#:~:text=Election infrastructure was designated

as,Facilities sector in January 2017.&text=The designation allows DHS to,state and local

election officials

Du, S., & Zhu, H. (2013). *Security assessment in vehicular networks.* Springer.

Estep, B. (2009, May 29). Former Clay official to change plea in vote-buying case. *Lexington*

Herald Leader. https://www.kentucky.com/latest-news/article44000220.html

Feng, T., & Keller, L. R. (2006). A multiple-objective decision analysis for terrorism protection:

Potassium iodide distribution in nuclear incidents. *Decision Analysis*, *3*(2), 76–93.

https://doi.org/10.1287/deca.1060.0072

Goethals, P. L., Scala, N. M., & Bastian, N. D. (2021, forthcoming). Operations research. In P.

L. Goethals, N. M. Scala, & D. Bennett (Eds.), *Mathematics in cyber research.* CRC Press /

Taylor and Francis.

Goodwin, P., & Wright, G. (1998). *Decision analysis for management judgment* (2nd ed.).

Wiley.

Graham, D. A. (2020, October 21). Signed, sealed, delivered—then discarded. *The Atlantic*.

https://www.theatlantic.com/ideas/archive/2020/10/signature-matching-is-the-phrenology-

of-elections/616790/

Helmer-Hirschberg, O. (1967). *Analysis of the future: The Delphi method*. RAND Corporation.

https://www.rand.org/pubs/papers/P3558.html

Howard County, Maryland. (2020). *Vote by mail ballot requests*.

https://www.howardcountymd.gov/Departments/Board-of-Elections

Janoff, A. (2020, March 6). Mail Services prioritizes electoral mail following concerns of lost

ballots. *The Tufts Daily*. https://tuftsdaily.com/news/2020/03/06/mail-services-prioritizes-

electoral-mail-following-concerns-lost-ballots/

Kavanagh, J., Hodgson, Q., Gibson, C. Ben, & Cherney, S. (2020). *An assessment of state voting

processes: Preparing for elections during a pandemic*. RAND Corporation.

https://doi.org/10.7249/RRA112-8

Keene, K. K., & Livingston, D. E. (2016). *Election Judge Manual 2016*. Harford County,

Maryland.

Keeney, R. L., & von Winterfeldt, D. (2011). A value model for evaluating homeland security

    decisions. *Risk Analysis*, *31*(9), 1470–1487. https://doi.org/10.1111/j.1539-

    6924.2011.01597.x

Lallie, H. S., Debattista, K., & Bal, J. (2020). A review of attack graph and attack tree visual

    syntax in cyber security. *Computer Science Review*, *35*, 100219.

    https://doi.org/10.1016/j.cosrev.2019.100219

Lee, S.O. (2020). *Vote-from-home? Evaluation framework for election security on remote voting*

    in response to COVID-19. SSRN. https://doi.org/10.2139/ssrn.3685381

Leonard, K., Mueller, T., Stott, S., & Orozco Rodriguez, J. (2020, June 8). The Indy explains:

    What happens to my ballot after I mail it in? *The Nevada Independent*.

    https://thenevadaindependent.com/article/indy-explains-how-mail-in-ballots-work-from-

    filling-out-to-official-results

Locraft, H., Gajendiran, P., Price, M., Scala, N. M., & Goethals, P. L. (2019). Sources of risk in

    elections security. *Proceedings of the 2019 IISE Annual Conference*.

    http://tinyurl.com/LocraftEtAl2019

Maryland Office of the Attorney General. (n.d.). *Voting FAQ for 2020.*

    https://www.marylandattorneygeneral.gov/Pages/votingFAQ.aspx

Maryland State Board of Elections. (n.d.) *Voting in Maryland*.

    https://elections.maryland.gov/voting/index.html

Mayse, J. (2020, June 16). Absentee ballots with labeling mistake still valid. *The Messenger-*

    Inquirer. https://www.messenger-inquirer.com/news/absentee-ballots-with-labeling-

    mistake-still-valid/article_d4f3826e-e24e-5e54-a258-4042bad16227.html

Merelli, A. (2020, October 14). What happens to absentee ballots after you mail them? *Quartz*.

https://qz.com/1916959/how-are-mail-in-ballots-in-the-presidential-election-counted/

Mueller, R. S. (2019). *Report on the investigation into Russian interference in the 2016*

presidential election. United States Department of Justice.

https://www.justice.gov/storage/report.pdf

National Conference of State Legislatures (2021, July 15). *Voter identification requirements |*

Voter ID laws. https://www.ncsl.org/research/elections-and-campaigns/voter-id.aspx

National Institute of Standards and Technology (n.d.). *Election terminology glossary - draft*.

https://pages.nist.gov/ElectionGlossary/

Olivares, V., Samuels, A., & Pollock, C. (2020, August 14). Democrats, local election leaders

fear Donald Trump's attacks on mail-in voting foreshadow voter suppression. *The Texas*

Tribune. https://www.texastribune.org/2020/08/14/texas-mail-in-voting-postal-service/

Pennycook, G., & Rand, D. G. (2021). Research note: Examining false beliefs about voter fraud

in the wake of the 2020 Presidential Election. *Harvard Kennedy School Misinformation*

Review. https://doi.org/10.37016/mr-2020-51

Prasad, M., & Avadhani, P. (2019). Attack tree design and analysis of offshore oil and gas

process complex SCADA system. *International Journal of Computer Applications*, *181*(41),

12–18. https://doi.org/10.5120/ijca2019918440

Price, M., Scala, N. M., & Goethals, P. L. (2019). Protecting Maryland's voting processes.

Baltimore Business Review: A Maryland Journal, 36–39. http://tinyurl.com/PriceEtAl2019

Root, D., Solomon, D., Cokley, R., O'Neal, T., Watkins, J. R., & Whitehead, D. (2020, April

20). In expanding vote by mail, states must maintain in-person voting options during the

coronavirus pandemic. *Center for American Progress and the NAACP*.

https://www.americanprogress.org/issues/democracy/news/2020/04/20/483438/expanding-vote-mail-states-must-maintain-person-voting-options-coronavirus-pandemic/

The New York Times (2021). *Russian hacking and influence in the U.S. Election.* https://www.nytimes.com/news-event/russian-election-hacking

Saini, V., Duan, Q., & Paruchuri, V. (2008). Threat modeling using attack trees. *Journal of Computing Sciences in Colleges*, *23*(4), 124–131.

Sanger, D., & Edmonson, C. (2019, July 25). Russia targeted election systems in all 50 states, report finds. *The New York Times*. https://www.nytimes.com/2019/07/25/us/politics/russian-hackingelections.html

Scala, N. M., Dehlinger, J., Black, L., Harrison, S., Licona Delgado, K., & Ieromonahos, A. (2020a). Empowering Election Judges to Secure Our Elections. *Baltimore Business Review: A Maryland Journal*. http://wp.towson.edu/bbr/2020/03/18/empowering-election-judges-to-secure-our-elections/

Scala, N. M., Dehlinger, J., & Black, L. (2020b). *Preparing pollworkers to secure U.S. elections.*[Manuscript submitted for publication]. Towson University.

Schneier, B. (1999). *Attack trees.* Schneier on security. https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Selvi, M., Aksu, E. B., Dilek, M. H., Erkan, A., & Demirezen, M. U. (2014). Attack Tree Visualization for Cyber Security Situational Awareness. *7th International Conference on Information Security and Cryptology*, 102–107. https://api.semanticscholar.org/CorpusID:15783067

Shackelford, S., Schneier, B., Sulmeyer, M., Boustead, A., Buchanan, B., Craig Deckard, A., Herr, T., & Malekos Smith, J. (2017). Making democracy harder to hack. *University of*

Michigan Journal of Law Reform, 50(3), 629–668.

Shino, E., Suttmann-Lea, M., & Smith, D. A. (2020, May 21). Here's the problem with mail-in

ballots: They might not be counted. *The Washington Post*.

https://www.washingtonpost.com/politics/2020/05/21/heres-problem-with-mail-in-ballots-

they-might-not-be-counted/

Simons, B., & Jones, D. W. (2012). Internet voting in the U.S. *Communications of the ACM*,

55(10), 68–77. https://doi.org/10.1145/2347736.2347754

Southwick, R. (2020, May 28). Dealing with mail-in ballots emerges as major challenge for PA

primary election. *Penn Live Patriot News.*

https://www.pennlive.com/news/2020/05/dealing-with-mail-in-ballots-emerges-as-major-

challenge-for-pa-primary-election.html

Timm, J. C. (2020, August 9). A white person and a Black person vote by mail in the same state.

Whose ballot is more likely to be rejected? *NBC News.*

https://www.nbcnews.com/politics/2020-election/white-person-black-person-vote-mail-

same-state-whose-ballot-n1234126

United States Election Assistance Commission Advisory Board. (2009). *Election operations*

assessment: Threat trees and matrices and threat instance risk analyzer (TIRA).

https://www.eac.gov/assets/1/28/Election_Operations_Assessment_Threat_Trees_and_Matr

ices_and_Threat_Instance_Risk_Analyzer_(TIRA).pdf

United States Election Assistance Commission Advisory Board. (2018). *Help America Vote Act*.

https://www.eac.gov/about/help-america-vote-act/

Volou, K., & Franklin, J. (2020, October 14). Virginia judge extends voter registration for 48

hours following system outage. *WUSA9.*

https://www.wusa9.com/article/news/local/virginia/virginia-voter-registration-site-down-on-last-day-to-register-to-vote-officials-say/65-3e5b390b-3e47-4a22-a440-6afddf770f3a

WKRN Web Staff and Nexstar Media Wire. (2020, November 5). 6 post office break-ins investigated in Tennessee. *Fox 8.* https://fox8.com/news/6-post-office-break-ins-investigated-in-tennessee/

Wolchok S., Wustrow E., Isabel D., Halderman J.A. (2012). Attacking the Washington, D.C. internet voting system. In A. D. Keromytis (Ed.), *Financial Cryptography and Data Security.* Springer. https://doi.org/10.1007/978-3-642-32946-3_10

Appendix I

EAC Threat Tree (US EAC, 2009)

O 1 Insider attack
    O 1.1 Edit marked ballots
        O 1.1.1 Edit at local elections office
            A 1.1.1.1 Edit during duplication
                T 1.1.1.1.1 Form collaboration of poll workers
                T 1.1.1.1.2 Gain exclusive access to ballots
                T 1.1.1.1.3 Mark under/overvotes or change votes
            T 1.1.1.2 Edit during counting
            T 1.1.1.3 Edit during other handling
        O 1.1.2 Edit in transit
            T 1.1.2.1 Edit in post office
            T 1.1.2.2 Edit in intermediate mail room
    O 1.2 Discard marked ballot
        O 1.2.1 Challenge committed ballot
            O 1.2.1.1 Errant challenge
                T 1.2.1.1.1 Judge misinterprets rule
                T 1.2.1.1.2 Errant failed signature
            O 1.2.1.2 Malicious challenge
                T 1.2.1.2.1 Challenge signature
                T 1.2.1.2.2 Challenge postmark
                T 1.2.1.2.3 Challenge intent
        O 1.2.2 Marked ballot lost in the mail
            T 1.2.2.1 Malicious loss
            T 1.2.2.2 Accidental loss
        O 1.2.3 Discard marked ballots at local elections office
            A 1.2.3.1 Delete during duplication
                T 1.2.3.1.1 Form collaboration of poll workers
                T 1.2.3.1.2 Gain exclusive access to ballots
                T 1.2.3.1.3 Overcome controls
            T 1.2.3.2 Remove during counting
            T 1.2.3.3 Mark registration system to reflect duplicate
            T 1.2.3.4 Remove during other handling
    O 1.3 Miscount duplicated ballots
        A 1.3.1 Count original and duplicate
             T 1.3.1.1 File duplicate with duplicated ballot
            T 1.3.1.2 Defeat ballot accounting
        T 1.3.2 Omit original and duplicate
    O 1.4 Marked ballot stuffing
        T 1.4.1 Insert ballots during envelope separation
        T 1.4.2 Insert ballots during counting
        T 1.4.3 Insert ballots during recount
        T 1.4.4 Insert ballots during audit
    O 1.5 Manipulate or discard votable ballot
        O 1.5.1 Delete at local elections office
            T 1.5.1.1 Fail to stuff envelope
            T 1.5.1.2 Send wrong or pre-marked ballot
            T 1.5.1.3 Mis-address envelope
            T 1.5.1.4 Destroy prepared envelope
            T 1.5.1.5 Destroy batch of prepared envelopes
        O 1.5.2 Delay delivery past deadline

T 1.5.2.1 Election process delay
T 1.5.2.2 Handling delay
T 1.5.2.3 Delay in the mail
O 1.5.3 Delete at destination
    T 1.5.3.1 Lost in destination mail room
    T 1.5.3.2 Mailbox attack
O 2 Masquerade Attack
  A 2.1 Deceased voters
    T 2.1.1 Identify target deceased voters
    T 2.1.2 Register them to an accessible address
    T 2.1.3 Receive, mark, return their ballot
    T 2.1.4 Defeat signature check
  T 2.2 Family members
  A 2.3 Central housing
    T 2.3.1 Identify target residents
    T 2.3.2 Register them
    T 2.3.3 Intercept, mark, and return their ballot
    O 2.3.4 Defeat signature check
      T 2.3.4.1 Register as the voter
      T 2.3.4.2 Forge the signature
  A 2.4 Mailbox attack
    T 2.4.1 Identify target
    T 2.4.2 Steal blank ballot from mailbox
    T 2.4.3 Receive, mark, return their ballots
    O 2.4.4 Defeat signature check
      T 2.4.4.1 Register as the voter
      T 2.4.4.2 Forge the signature
  T 2.5 Malicious "messenger ballots"
O 3 Voting process attacks
  O 3.1 Vote buying
    T 3.1.1 Bookie model
    A 3.1.2 Internet vote buying attack
      O 3.1.2.1 Attract voters
        T 3.1.2.1.1 Attract voters with internet adds
        T 3.1.2.1.2 Identify prospective vote sellers from voter rolls
      T 3.1.2.2 Receive, mark, return their ballots
      T 3.1.2.3 Pay the voters via the internet
    T 3.1.3 Pay voters not to vote
  O 3.2 Organizer coercion attack
    T 3.2.1 Attribution threats
    T 3.2.2 Debate and vote parties
  T 3.3 Employer coercion attack
  T 3.4 Family member coercion attack
  T 3.5 Distribute false ballots
O 4 Errors in voting system processes
  O 4.1 Administrative error
    T 4.1.1 Failure to sign correctly
    T 4.1.2 Signature mismatch
    T 4.1.3 Failure to bundle correctly
    T 4.1.4 Failure to meet time requirements
    T 4.1.5 Confusion with federal write-in absentee ballot
  O 4.2 Selection error
    T 4.2.1 Human error mis-mark
    T 4.2.2 Ballot design flaw
    T 4.2.3 Correction mistake
    T 4.2.4 Candidate name confusion

Appendix II
Updated attack tree outline

O 1 Insider attack
    O 1.1 Edit marked ballots
        O 1.1.1 Edit at local elections office
            A 1.1.1.1. Edit during duplication
                T 1.1.1.1.1 (X1) Form collaboration of poll workers
                T 1.1.1.1.2 (X2) Gain exclusive access to ballots
                T 1.1.1.1.3 (X3) Mark under/over votes or changes votes
            T 1.1.1.2 (X4) Edit during counting
            T 1.1.1.3 (X5) Edit during other handling
        O 1.1.2 Edit in transit
            A 1.1.2.1 Edit in post office
                T 1.1.2.1.1 (X73) Form collaboration with mail worker and acquire access
                T 1.1.2.1.2 (X74) Break into post office
                T 1.1.2.1.3 (X6) Edit in post office
            A 1.1.3.1 Gain exclusive access to intermediate mailroom
                T.1.1.3.1.1 (X75) Form collaboration with mail worker and acquire access
                T.1.1.3.1.2 (X76) Break into intermediate mailroom
                T 1.1.3.1.3 (X7) Edit in intermediate mailroom
    O 1.2 Discard marked ballot
        O 1.2.1 Challenge committed ballot
            O 1.2.1.1 Errant challenge
                T 1.2.1.1.1 (X8) Judge misinterprets rule
                T 1.2.1.1.2 (X9) Errant failed signature
            O 1.2.1.2 Malicious challenge
                T 1.2.1.2.1 (X10) Challenge signature
                T 1.2.1.2.2 (X11) Challenge postmark
                T 1.2.1.2.3 (X12) Challenge intent
        O 1.2.2 Marked ballot lost in the mail
            T 1.2.2.1 (X13) Malicious loss
            T 1.2.2.2 (X14) Accidental loss
        O 1.2.3 Discard marked ballots at local elections office
            A 1.2.3.1 Delete during duplication
                T 1.2.3.1.1 (X15) Form collaboration of poll workers
                T 1.2.3.1.2 (X16) Gain exclusive access to ballots
                T 1.2.3.1.3 (X17) Overcome controls
            T 1.2.3.2 (X18) Remove during counting
            T 1.2.3.3 (X19) Mark registration system to reflect duplicate
            T 1.2.3.4 (X20) Remove during other handling
    O 1.3 Miscount duplicated ballots
        A 1.3.1 Count original and duplicate
            T 1.3.1.1 (X21) File duplicate with duplicated ballot
            T 1.3.1.2 (X22) Defeat ballot accounting
        T 1.3.2 (X23) Omit original and duplicate
    O 1.4 Marked ballot stuffing
        T 1.4.1 (X24) Insert ballots during envelope separation
        T 1.4.2 (X25) Insert ballots during counting
        T 1.4.3 (X26) Insert ballots during recount
        T 1.4.4 (X27) Insert ballots during audit
    O 1.5 Manipulate or discard votable ballot
        O 1.5.1 Delete at local elections office
            T 1.5.1.1 (X28) Fail to stuff envelope
            T 1.5.1.2 (X29) Send wrong or pre marked ballot
            T 1.5.1.3 (X30) Mis-address envelope

T 1.5.1.5 (X31) Destroy prepared envelope
T 1.5.1.6 (X32) Destroy batch of prepared envelopes
T 1.5.1.4 (X77) Manipulate return envelope
O 1.5.2 Delay delivery past deadline
T 1.5.2.1 (X33) Election process delay
T 1.5.2.2 (X34) Handling delay
T 1.5.2.3 (X35) Delay in the mail
O 1.5.3 Delete at destination
T 1.5.3.1 (X36) Lost in destination mailroom
T 1.5.3.2 (X37) Mailbox attack
O 1.6 Suppress voter turnout
T 1.6.1 (X78) Misallocate polling or drop box locations
T 1.6.2 (X79) Provide regional mail-in voting misinformation
T 1.6.3 (X80) Hinder or suppress regional postal services
T 1.6.4 (X81) System Outage
T 1.6.5 (X82) Name deliberately misspelled on ballot
O 1.7 Digital Attack
T 1.7.1 (X83) Paper ballot scanner hacked
T 1.7.2 (X84) Vote denied or altered
O 2 Masquerade attack
A 2.1 Deceased voters
T 2.1.1 (X38) Identify target deceased voters
T 2.1.2 (X39) Register the to an accessible address
T 2.1.3 (X40) Receive, mark, return their ballot
T 2.1.4 (X41) Defeat signature check
T 2.2 (X42) Family members
A 2.3 Central housing
T 2.3.1 (X43) Identify target residents
T 2.3.2 (X44) Register them
T 2.3.3 (X45) Intercept, mark, and return their ballot
O 2.3.4 Defeat Signature check
T 2.3.4.1 (X46) Register as the voter
T 2.3.4.2 (X47) Forge the signature
A 2.4 Mailbox attack
T 2.4.1 (X48) Identify target
T 2.4.2 (X49) Steal blank ballot from mailbox
T 2.4.3 (X50) Receive, mark, return their ballots
O 2.4.4 Defeat signature check
T 2.4.4.1 (X51) Register as the voter
T 2.4.4.2 (X52) Forge the signature
T 2.5 (X53) Malicious "messenger ballots"
O 2.6 Drop box attack
A 2.6.1 Steal/manipulate ballots in drop box
T 2.6.1.1 (X85) Identify target
T 2.6.1.2 (X86) Acquire access to drop box
T 2.6.1.3 (X87) Alter marks and return their ballots
T 2.6.2 (X88) Destroy drop box
O 2.7 Ballot storage attack
A 2.7.1 Manipulate ballots in storage
T 2.7.1.1 (X89) Gain exclusive access to ballot storage
T 2.7.1.2 (X90) Alter marks and return to storage
A 2.7.2 Steal/destroy ballots in storage
T 2.7.2.1 (X91) Gain exclusive access to ballot storage
T 2.7.2.2 (X92) Steal/destroy ballots
A 2.8 Caregivers
T 2.8.1 (X93) Steal blank ballot from mailbox

T 2.8.2 (X94) Mark and return their ballot
T 2.8.3 (X95) Defeat signature check
O 3 Voting process attacks
    O 3.1 Vote buying
        T 3.1.1 (X54) Bookie model
        A 3.1.2 Internet vote buying attack
            O 3.1.2.1 Attract voters
                T 3.1.2.1.1 (X55) Attract voters with internet adds
                T 3.1.2.1.2 (X56) Identify prospective vote sellers from voter rolls
            T 3.1.2.2 (X57) Receive, mark, return their ballot
            T 3.1.2.3 (X58) Pay the voters via the internet
        T 3.1.3 (X59) Pay voters not to vote
    O 3.2 Organizer coercion attack
        T 3.2.1 (X60) Attribution threats
        T 3.2.2 (X61) Debate and vote parties
    T 3.3 (X62) Employer coercion attack
    T 3.4 (X63) Family member coercion attack
    T 3.5 (X64) Distribute false ballots
    A 3.6 Digital Attack
        T 3.6.1 (X96) Paper ballot scanner hacked
        T 3.6.2 (X97) Vote denied or altered
    T 3.7 (X98) Invalid identification card attack
O 4 Errors in voting system processes
    O 4.1 Voter administrative error
        T 4.1.1 (X65) Failure to sign correctly
        T 4.1.2 (X66) Signature mismatch
        T 4.1.3 (X67) Failure to bundle correctly
        T 4.1.4 (X68) Failure to meet time requirements
        T 4.1.5 (X69) Confusion with federal write-in absentee ballot (overseas vote)
    O 4.2 Voter selection error
        T 4.2.1 (X70) Human error mismark
        A 4.2.2 Ballot design flaw
            T 4.2.2.1 (X99) Error in instructions
            T 4.2.2.2 (X100) Unclear assistance instructions when you don't require one
            T 4.2.2.3 (X101) Ballot says ID required when you don't require one
        T 4.2.3 (X102) Expired voter ID
        T 4.2.4 (X71) Correction mistake
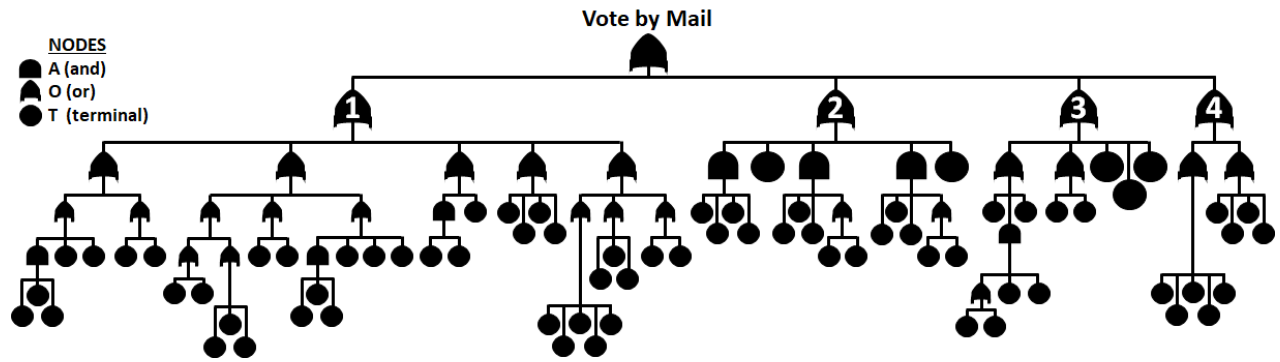   T 4.2.5 (X72) Candidate name confusion

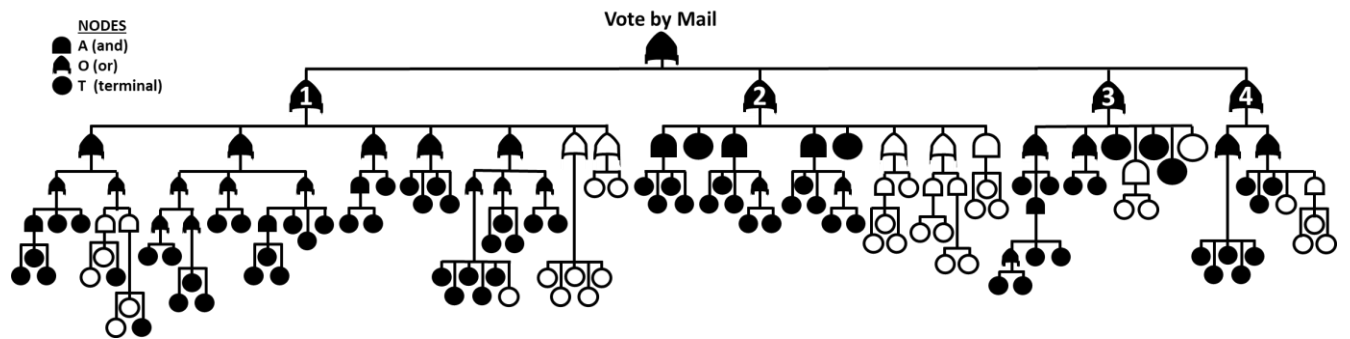Figure 1: Attack Tree Structure for Mail-in Voting (US EAC, 2009)

Figure 2: Updated Attack Tree Structure for Mail-in Voting

Node	Vulnerability	Branch	Reference
X_{73}	Form collaboration with mail worker and acquire access	Insider	Bote (2020)
X_{74}	Break into post office	Insider	WKRN and Nexstar (2020)
X_{75}	Form collaboration with mail worker and acquire access	Insider	Bote (2020)
X_{76}	Break into intermediate mail room	Insider	Merelli (2020)
X_{77}	Manipulate return envelope	Insider	Shino, et al. (2020)
X_{78}	Misallocate polling or drop-box locations	Insider	Baringer, et al. (2020)
X_{79}	Provide regional mail-in voting misinformation	Insider	Baringer, et al. (2020)
X_{80}	Hinder or suppress regional postal services	Insider	Olivares, et al. (2020); Timm (2020)
X_{81}	System outage	Insider	Volou, et al. (2020)
X_{82}	Name deliberately misspelled on ballot	Insider	Mayse (2020)
X_{83}	Paper ballot scanner hacked	Insider	Leonard, et al. (2020)
X_{84}	Vote denied or altered	Insider	Leonard, et al. (2020)
X_{85}	Identify target	External	Adapted from US EAC (2009); Estep (2008)
X_{86}	Acquire access to drop box	External	Adapted from US EAC (2009)
X_{87}	Alter marks and return their ballots	External	Ab intra
X_{88}	Destroy drop box	External	Leonard et al. (2020)
X_{89}	Gain exclusive access to ballot storage	External	Adapted from US EAC (2009)
X_{90}	Alter marks and return to storage	External	Ab intra
X_{91}	Gain exclusive access to ballot storage	External	Adapted from US EAC (2009)
X_{92}	Steal/destroy ballots	External	Adapted from USEAC (2009)
X_{93}	Steal blank ballot from mailbox	External	Ab intra
X_{94}	Mark and return their ballot	External	Adapted from US EAC (2009)
X_{95}	Defeat signature check	External	Adapted from US EAC (2009)
X_{96}	Paper ballot scanner hacked	External	Leonard, et al. (2020)
X_{97}	Vote denied or altered	External	Leonard, et al. (2020)
X_{98}	Invalid ID card attack	External	NCSL (2021)
X_{99}	Error in instructions	Voter error	Southwick (2020)
X_{100}	Unclear assistance instructions when not required	Voter error	Southwick (2020)
X_{101}	Ballot says ID required when not required	Voter error	NCSL (2021)
X_{102}	Expired voter ID	Voter error	NCSL (2021)

Table 1: Additional Threats to Mail-Based Voting

Attack Cost (AC)		Technical Difficulty (TD)		Discovering Difficulty (DD)	
Grade	Standard	Grade	Standard	Grade	Standard
5	Severe consequences likely	5	Extremely difficult	1	Extremely difficult
4	High consequences likely	4	Difficult	2	Difficult
3	Moderate consequences likely	3	Moderate	3	Moderate
2	Mild consequences likely	2	Simple	4	Simple
1	Little to no consequences likely	1	Very simple	5	Very simple

Table 2: Evaluation Standards for Model Attributes

Terminal Node	AC	TD	DD	Relative Likelihood	Terminal Node	AC	TD	DD	Relative Likelihood
T 1.1.1.1.1 (X_1)	4	2	2	0.08	T 2.1.3 (X_{40})	5	2	3	0.07
T 1.1.1.1.2 (X_2)	4	3	2	0.07	T 2.1.4 (X_{41})	4	2	1	0.12
T 1.1.1.1.3 (X_3)	3	4	2	0.07	T 2.2 (X_{42})	5	2	2	0.08
T 1.1.1.2 (X_4)	5	3	3	0.06	T 2.3.1 (X_{43})	4	3	3	0.06
T 1.1.1.3 (X_5)	3	4	3	0.06	T 2.3.2 (X_{44})	4	2	3	0.07
T 1.1.2.1.1 (X_{73})	5	3	2	0.07	T 2.3.3 (X_{45})	4	4	3	0.06
T 1.1.2.1.2 (X_{74})	5	4	4	0.05	T 2.3.4.1 (X_{46})	4	4	3	0.06
T 1.1.2.1.3 (X_6)	3	4	3	0.06	T 2.3.4.2 (X_{47})	4	1	2	0.12
T 1.1.3.1.1 (X_{75})	5	3	2	0.07	T 2.4.1 (X_{48})	4	2	4	0.07
T 1.1.3.1.2 (X_{76})	5	4	3	0.05	T 2.4.2 (X_{49})	4	4	3	0.06
T 1.1.3.1.3 (X_7)	3	2	2	0.09	T 2.4.3 (X_{50})	5	2	2	0.08
T 1.2.1.1.1 (X_8)	3	2	4	0.07	T 2.4.4.1 (X_{51})	5	3	3	0.06
T 1.2.1.1.2 (X_9)	1	2	4	0.12	T 2.4.4.2 (X_{52})	4	4	3	0.06
T 1.2.1.2.1 (X_{10})	2	3	3	0.08	T 2.5 (X_{53})	4	4	1	0.1
T 1.2.1.2.2 (X_{11})	2	3	3	0.08	T 2.6.1.1 (X_{85})	4	2	4	0.07
T 1.2.1.2.3 (X_{12})	2	3	2	0.09	T 2.6.1.2 (X_{86})	4	4	2	0.07
T 1.2.2.1 (X_{13})	4	2	2	0.08	T 2.6.1.3 (X_{87})	4	4	2	0.07
T 1.2.2.2 (X_{14})	2	2	2	0.1	T 2.6.2 (X_{88})	5	4	4	0.05
T 1.2.3.1.1 (X_{15})	5	1	1	0.15	T 2.7.1.1 (X_{89})	4	3	2	0.07
T 1.2.3.1.2 (X_{16})	4	3	2	0.07	T 2.7.1.2 (X_{90})	4	4	2	0.07
T 1.2.3.1.3 (X_{17})	4	4	3	0.06	T 2.7.2.1 (X_{91})	4	3	2	0.07
T 1.2.3.2 (X_{18})	4	3	3	0.06	T 2.7.2.2 (X_{92})	4	4	3	0.06
T 1.2.3.3 (X_{19})	4	4	4	0.05	T 2.8.1 (X_{93})	4	4	3	0.06
T 1.2.3.4 (X_{20})	3	3	3	0.07	T 2.8.2 (X_{94})	5	2	3	0.07
T 1.3.1.1 (X_{21})	4	3	3	0.06	T 2.8.3 (X_{95})	4	2	1	0.12
T 1.3.1.2 (X_{22})	4	4	4	0.05	T 3.1.1 (X_{54})	4	4	2	0.07
T 1.3.2 (X_{23})	2	3	3	0.08	T 3.1.2.1.1 (X_{55})	4	2	2	0.08
T 1.4.1 (X_{24})	4	3	2	0.07	T 3.1.2.1.2 (X_{56})	4	3	2	0.07
T 1.4.2 (X_{25})	4	3	4	0.06	T 3.1.2.2 (X_{57})	4	2	3	0.07
T 1.4.3 (X_{26})	4	3	4	0.06	T 3.1.2.3 (X_{58})	4	2	2	0.08
T 1.4.4 (X_{27})	4	3	2	0.07	T 3.1.3 (X_{59})	4	2	2	0.08
T 1.5.1.1 (X_{28})	4	1	3	0.11	T 3.2.1 (X_{60})	4	4	3	0.06
T 1.5.1.2 (X_{29})	4	4	3	0.06	T 3.2.2 (X_{61})	4	1	2	0.12
T 1.5.1.3 (X_{30})	3	4	3	0.06	T 3.3 (X_{62})	3	3	2	0.08
T 1.5.1.4 (X_{31})	4	2	2	0.08	T 3.4 (X_{63})	4	2	2	0.08
T 1.5.1.5 (X_{32})	4	4	2	0.07	T 3.5 (X_{64})	5	4	4	0.05
T 1.5.1.6 (X_{77})	4	3	3	0.06	T 3.6.1 (X_{96})	4	3	3	0.06
T 1.5.2.1 (X_{33})	3	2	3	0.08	T 3.6.2 (X_{97})	4	3	2	0.07
T 1.5.2.2 (X_{34})	4	3	4	0.06	T 3.7 (X_{98})	4	2	5	0.06
T 1.5.2.3 (X_{35})	4	3	2	0.07	T 4.1.1 (X_{65})	2	1	2	0.13
T 1.5.3.1 (X_{36})	2	2	1	0.13	T 4.1.2 (X_{66})	4	2	3	0.07
T 1.5.3.2 (X_{37})	4	2	2	0.08	T 4.1.3 (X_{67})	2	1	5	0.11
T 1.6.1 (X_{78})	4	2	4	0.07	T 4.1.4 (X_{68})	4	3	4	0.06
T 1.6.2 (X_{79})	4	4	3	0.06	T 4.1.5 (X_{69})	3	2	2	0.09
T 1.6.3 (X_{80})	4	3	4	0.06	T 4.2.1 (X_{70})	3	2	4	0.07
T 1.6.4 (X_{81})	3	2	3	0.08	T 4.2.2.1 (X_{99})	4	3	3	0.06
T 1.6.5 (X_{82})	3	3	5	0.06	T 4.2.2.2 (X_{100})	3	3	3	0.07
T 1.7.1 (X_{83})	4	3	3	0.06	T 4.2.2.3 (X_{101})	2	2	3	0.09
T 1.7.2 (X_{84})	4	3	2	0.07	T 4.2.3 (X_{102})	3	2	4	0.07
T 2.1.1 (X_{38})	4	5	4	0.05	T 4.2.4 (X_{71})	3	2	2	0.09
T 2.1.2 (X_{39})	4	4	3	0.06	T 4.2.5 (X_{72})	3	2	2	0.09

Table 3: Evaluation of Updated Attack Tree Terminal Nodes

Attack Scenario	Leaf Node(s)	Relative Likelihood	Attack Scenario	Leaf Node(s)	Relative Likelihood
S_1	X_1, X_2, X_3	0.0004	S_{38}	X_{82}	0.0600
S_2	X_4	0.0600	S_{39}	X_{83}	0.0600
S_3	X_5	0.0600	S_{40}	X_{84}	0.0700
S_4	X_{73}, X_{74}, X_6	0.0002	S_{41}	$X_{38}, X_{39}, X_{40}, X_{41}$	0.0000
S_5	X_{75}, X_{76}, X_7	0.0003	S_{42}	X_{42}	0.0800
S_6	X_8	0.0700	S_{43}	$X_{43}, X_{44}, X_{45}, X_{46}$	0.0000
S_7	X_9	0.1200	S_{44}	$X_{43}, X_{44}, X_{45}, X_{47}$	0.0000
S_8	X_{10}	0.0800	S_{45}	$X_{48}, X_{49}, X_{50}, X_{51}$	0.0000
S_9	X_{11}	0.0800	S_{46}	$X_{48}, X_{49}, X_{50}, X_{52}$	0.0000
S_{10}	X_{12}	0.0900	S_{47}	X_{53}	0.1000
S_{11}	X_{13}	0.0800	S_{48}	X_{85}, X_{86}, X_{87}	0.0003
S_{12}	X_{14}	0.1000	S_{49}	X_{88}	0.0500
S_{13}	X_{15}, X_{16}, X_{17}	0.0006	S_{50}	X_{89}, X_{90}	0.0049
S_{14}	X_{18}	0.0600	S_{51}	X_{91}, X_{92}	0.0042
S_{15}	X_{19}	0.0500	S_{52}	X_{93}, X_{94}, X_{95}	0.0005
S_{16}	X_{20}	0.0700	S_{53}	X_{54}	0.0700
S_{17}	X_{21}, X_{22}	0.0030	S_{54}	X_{55}, X_{57}, X_{58}	0.0004
S_{18}	X_{23}	0.0800	S_{55}	X_{56}, X_{57}, X_{58}	0.0004
S_{19}	X_{24}	0.0700	S_{56}	X_{59}	0.0800
S_{20}	X_{25}	0.0600	S_{57}	X_{60}	0.0600
S_{21}	X_{26}	0.0600	S_{58}	X_{61}	0.1200
S_{22}	X_{27}	0.0700	S_{59}	X_{62}	0.0800
S_{23}	X_{28}	0.1100	S_{60}	X_{63}	0.0800
S_{24}	X_{29}	0.0600	S_{61}	X_{64}	0.0500
S_{25}	X_{30}	0.0600	S_{62}	X_{96}, X_{97}	0.0042
S_{26}	X_{31}	0.0800	S_{63}	X_{98}	0.0600
S_{27}	X_{32}	0.0700	S_{64}	X_{65}	0.1300
S_{28}	X_{77}	0.0600	S_{65}	X_{66}	0.0700
S_{29}	X_{33}	0.0800	S_{66}	X_{67}	0.1100
S_{30}	X_{34}	0.0600	S_{67}	X_{68}	0.0600
S_{31}	X_{35}	0.0700	S_{68}	X_{69}	0.0900
S_{32}	X_{36}	0.1300	S_{69}	X_{70}	0.0700
S_{33}	X_{37}	0.0800	S_{70}	X_{99}, X_{100}, X_{101}	0.0004
S_{34}	X_{78}	0.0700	S_{71}	X_{102}	0.0700
S_{35}	X_{79}	0.0600	S_{72}	X_{71}	0.0900
S_{36}	X_{80}	0.0600	S_{73}	X_{72}	0.0900
S_{37}	X_{81}	0.0800			

Table 4: Attack Scenarios for Mail-Based Voting
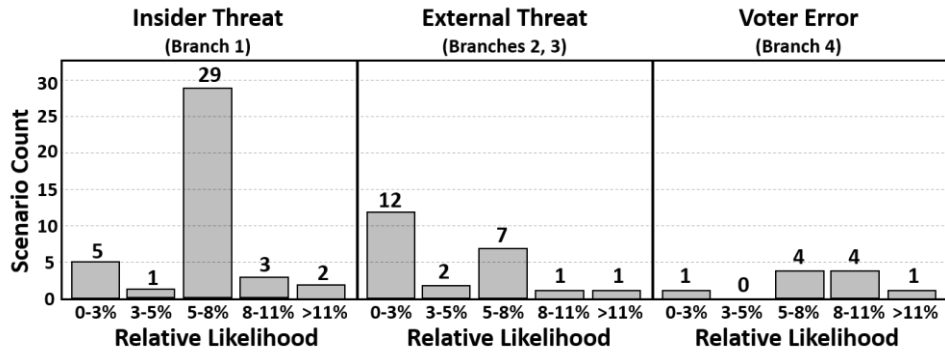
Figure 3: Histograms of Attack Scenario Counts

Branch	Specific Scenarios		Mitigations
Insider Threat (Total: 40)	Most Likely	S_{32}: Ballot lost in destination mailroom	Need to be appropriately staffed in order to handle the influx of ballots and timely delivery of ballots; emphasize that the information is accurate when requesting ballot (house number, spelling name correctly, etc.); immediately send ballots as requests come in.
	Least Likely	S_4: Edit in transit at post office	Ballot storage should be checked daily to ensure no tampering; only select few at the post office should have access to the ballots.
External Threat (Total: 23)	Most Likely	S_{58}: Organized coercion through debate and vote parties	Mail ballots should not be filled out in group settings; attendees made aware of possible occurrence and informed of what to do if it happens; provide guidelines for attendance at event; have security personnel present for incident reporting; no audience during debates; attendees should remove themselves and their ballots if persuaded at the party; disabled voters who require assistance should only vote with unbiased aid.
	Least Likely	S_{43}: Identify target residents	Frequent checks of voter registration lists; ensure voter signatures are authenticated by two different election officials; ballot status tracking for central housing residents.
Voter Error (Total: 10)	Most Likely	S_{64}: Fail to sign ballot correctly	Implement a "notice and cure" system for rejected votes, allowing voters opportunity to correct submission mistakes; enhanced standardized training to promote consistency among officials; encourage voters to monitor status of returned ballots.
	Least Likely	S_{70}: Ballot design flaw	Encourage voters to consult non-partisan sources for voter information; carefully read instructions with ballot and provide all required documentation.

Table 5: Attack Scenarios, Most and Least Likely (by Branch)

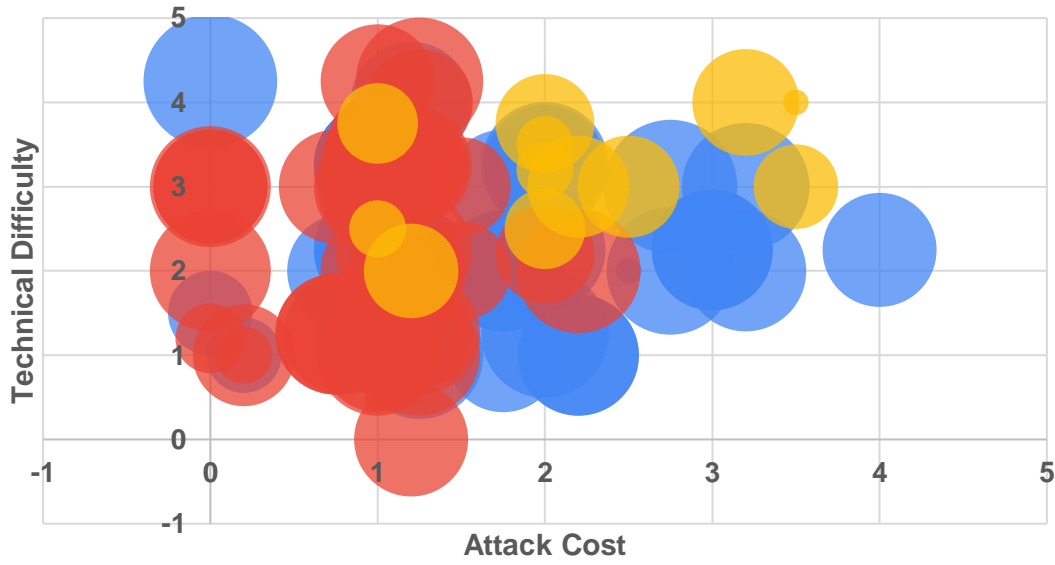| Scenario	Threats		Relative Likelihood	Branch
S_7	X_9	Errant failed signature	0.12	Internal
S_{12}	X_{14}	Accidental loss	0.10	Internal
S_{23}	X_{28}	Failure to stuff envelope	0.11	Internal
S_{47}	X_{53}	Malicious "messenger ballots"	0.10	External
S_{66}	X_{67}	Failure to bundle correctly	0.11	Voter Error

Table 6: Additional Higher-than-Average Threats

Figure 4: Mail-Based Voting Threats Bubble Chart
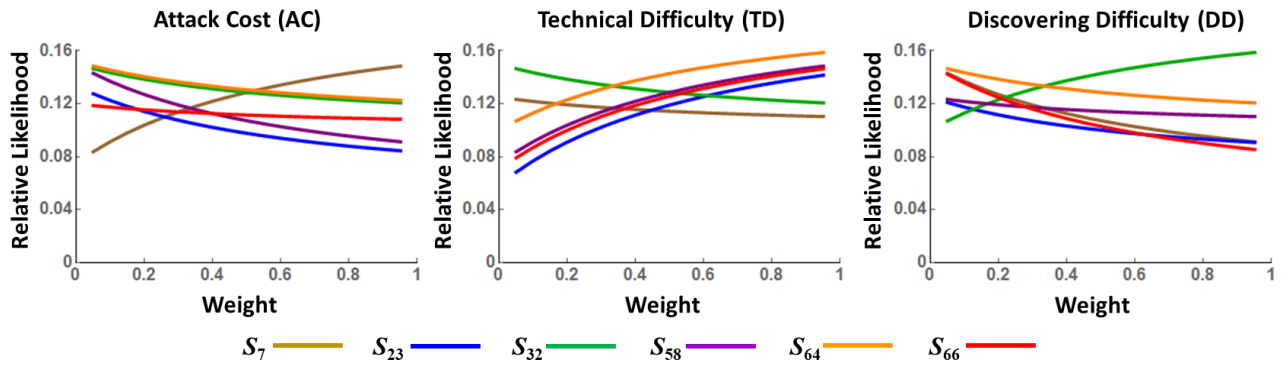(Blue = Insider Threat, Red = External Threat, Yellow = Voter Error)

Figure 5: Sensitivity Analysis for AC, TD, and DD