Proceedings of the 2021 IISE Annual Conference
A. Ghate, K. Krishnaiyer, K. Paynabar, eds.

A Process Map and Risk Assessment for Mail-based Voting

Natalie M. Scala, Isabella Bloomquist, Yeabsira Mezgebe, Betelhem Jilcha
Department of Business Analytics and Technology Management
Towson University, Towson, MD 21252

Paul L. Goethals
Department of Mathematical Sciences
United States Military Academy, West Point, NY 10996

Josh Dehlinger
Department of Computer and Information Sciences
Towson University, Towson, MD 21252

Abstract

The sudden shift to mail-based voting because of the COVID-19 pandemic precipitated national concerns about the security of this process. This research addresses mail-based voting impacts to elections security. Specifically, we develop a process model for mail-based voting and identify and map cyber, physical, and insider threats to the process. We then apply a utility-based methodology for assessing threat to evaluate the process model scenarios and nodes. We illustrate the model using Maryland's mail-based voting process as a case study and identify nodes or activities of concern due to higher relative risk. The goal of this research is to better understand how the dramatic shift and scaling of mail-based voting during the 2020 General Election can impact threat. Results will provide election officials insight on how voting system vulnerabilities develop and when and where to employ mitigating security measures.

Keywords

Process map; risk; elections security; mail-based voting; COVID-19

1. Introduction and Motivation

The 2020 General Election was unprecedented, as COVID-19 threatened the United States and forced widescale changes and adjustments to the states' elections processes. When the primary election season began in early February 2020 with the Iowa caucuses, COVID-19 was not in the global discussion, but by March, many states were scrambling to adjust their primary election plans. By summer, 40% of states had made a process change to their 2020 Primary Election, and 47 states continued with expanded mail-based voting for the General Election [1]. Even with the societal upheaval caused by a deadly pandemic, a record number of Americans voted in the 2020 General Election, with historic early voting turnout, reflecting that Americans were seeking safe, socially distant methods of voting [2,3].

However, the rapid expansion of mail-based voting leads to questions and concerns about the security of the process and integrity of votes cast by mail. As states made process changes literally overnight – for example, Ohio postponed its primary the night before the election, converting it to extended absentee voting [4] – the focus of elections officials was bringing a traditionally limited absentee process to scale. As a result, the essence of time may not have allowed policy makers and elections officials to consider corresponding security threats. This research addresses risk in and the security of voting by mail, specifically the process integrity of votes. As part of a large-scale research effort, we examine elections security, the complex nature of the mail-based voting process, and where risk lies in the process. In the larger work, we first identify vulnerabilities in the mail-based voting process and actions that can attack and compromise the process. We then employ a utility model to calculate the relative likelihood of those threats in order to identify the scenarios of highest concern, along with mitigations to reduce the relative likelihood and/or impact if the threat arises [1]. This research addresses the safety of voting by mail, from trusted insider, external adversarial, and voter fraud perspectives, and it contributes to the elections security discussion by imparting a process map for mail-based voting. We also apply the risk model in our larger work [1] to identify process nodes of interest in terms

of security and their relative likelihood of concern. Mail-based voting will continue in the United States beyond the 2020 elections, and it is conceivable that a more widespread use will remain in a post-pandemic society. Therefore, it is critical to understand where and when threats occur as well as the extent of those threats.

2. Literature Review

2.1. History and Risks

Mail-based voting has been used in the United States in some form since the Civil War [5]. Traditionally, states have been using mail-based voting for their absentee voting as well as for overseas and military voters. However, even before COVID-19, some states expanded mail-based voting to the primary method of voting. Specifically, Oregon has conducted elections fully by mail since 1998, Washington state since 2011, and Colorado since 2013 [6]. In addition, Hawaii and Utah planned to hold the 2020 elections entirely by mail, even before COVID-19. A 2016 report from the U.S. Elections Assistance Commission (EAC) shows that a majority of voters cast ballots by mail in seven states: Arizona, California, Colorado, Montana, Oregon, Utah, and Washington [7].

Mail-based voting, like all forms of voting, has some inherent risks. In 2009, the EAC, an independent and bipartisan commission developed as part of the Help America Vote Act (HAVA) of 2002, sponsored an assessment of elections operations to comprise an inventory of threats to various forms of voting, including in-person (via multiple types of elections equipment), mail, phone, and by internet [8]. Threats were arranged into attack trees, which are graphical representations of a security problem, decomposing complex actions into hierarchical levels, terminating at the lowest level of single actions taken to compromise a system; the decomposition enumerates all threats to aid in the understanding of the full scope of threat and needed countermeasures [1, 9]. Attack trees were first used for security problems in the 1990s [10], and a detailed discussion of their use and design, along with applications to elections security, can be found in [9, 11]. A review of attack trees as policy models for cybersecurity can be found in [12].

The EAC attack tree [8] identifies 72 risks to mail-based voting, organized into four branches of threats: insider (branch 1), external (branches 2 and 3), and voter error (branch 4). The inventory of attacks was comprehensive at the time of development and include activities such as errant failed signatures, delay in the mail, and deceased voters [8]. Based on the nature of attacks, and if actions need to be executed in parallel or singularly, the tree identifies a total of 57 attack scenarios, with 32 insider scenarios, 16 from an external actor, and 9 aligned to voter error.

In general, the literature on elections security becomes active after the passage of HAVA in 2002, transitioning the United States to electronic forms of voting and increasing voter access in response to the punch card controversy and *Bush v. Gore* litigation after the 2000 General Election. The academic literature becomes rather silent after 2010, until the end of the decade when security and interference concerns related to the 2016 General Election are examined and addressed. The Department of Homeland Security designated elections infrastructure as critical infrastructure in 2017 [13], further emphasizing the fundamental need to secure the integrity of votes to support confidence in this fundamental practice of democracy.

Recent academic research includes Price, et al. [14], who focus specifically on the in-person election process in Maryland and identify 25 vulnerabilities in that state's process, organized into cyber, physical, and insider threats. They were also the first to consider threats to elections security systemically and not just in terms of cyber threat. Locraft, et al. [15] contribute influence diagrams for sources of threat and focus on the activity of external adversarial actors in 2016. Both papers address vulnerabilities and threat but in the context of in-person voting. Natural extensions of that work include how and if the Price, et al. [14] vulnerabilities extend to mail-based voting as well as corresponding external actor threats to mail-based voting, especially in a pandemic. In general, the literature on mail-based voting is nascent and needed, as the literature of the last 20 years focuses on in-person voting and overarching policy.

2.2. Research Extensions

This research addresses the need for academic treatment of threats to the security of mail-based voting. Our larger research effort considers the EAC [8] attack tree and how threats have evolved since its design, due to adaptive adversaries, advances in technology, and the emerging COVID-19 pandemic. We contribute 30 additional threats and assign them to branches of the attack tree [1]. We then evaluate these threats via three attributes – attack cost, technical difficulty, and discovering difficulty – whereby a utility-based metric provides the relative likelihood of each of the 102 threats and 73 scenarios on the updated attack tree. Finally, we identify eight scenarios of highest concern, with relative likelihoods of 0.10 or greater. The natural extension of this work is to identify *where* vulnerabilities exist

within the mail-based voting process, along with *when* they might occur. Such an understanding of the threats provides a significant advantage in mitigating and defending against the external adversary, nefarious insider, or fraudulent voter. To facilitate this understanding, we begin with the design of the mail-based voting process.

3. Process Map for Mail-Based Voting

A process map illustrates the end-to-end components of a process from start to finish; process management is a systemic approach for capturing, designing, executing, documenting, measuring, monitoring, and controlling a process to meet objectives [16]. The goal of process management is to assess the current state of the entire process to identify continuous improvement opportunities. It also involves multiple stakeholders who provide inputs and are actively involved in roles such as owner, manager, analyst, and engineer [16]. Process maps allow for identification of bottlenecks and nodes of concern or attention, which may then be abated using various analytical methods.

Price, et al. [14] contribute the first known process map for elections security in the literature by illustrating the in-person voting process in Maryland. Polling place voting may have some process nuances between states, and those authors note that an understanding of roles and how they relate to the process facilitates awareness of mitigation actions to reduce threat [14]. To our knowledge, we are the first to contribute a process map for mail-based voting. Unlike in-person voting, mail-based voting has a more standard nationwide process between states. Even so, we model the process using the State of Maryland as a guide; our model design was iterative, receiving and incorporating feedback from county Board of Elections (BoE) officials in the state.

Figure 1 presents the process map for mail-based voting. Note the three main stakeholders and corresponding swim lanes of elections officials, the voter, and the post office. Regardless of risk, the process is complex and occurs over multiple days and/or weeks. To follow the map, start on the left-hand side and move through the process arrows. Note that the map identifies activities in mail-based voting but does not necessarily reflect time; activities that are vertically above/below each other do not necessarily occur in parallel. Figure 1 includes a legend for gateways, events, and messages icons that help the user navigate the flow of the process. Squares are used to denote process activities, and the figure includes a list of those activities. For brevity, a full discussion of each activity node is omitted here but available online [17].

3.1. Process Flow and Design

The mail-based voting process commences when elections officials mail a ballot to the voter through the post office. Once the voter receives their ballot, they examine inclusion and accuracy of the documents, which may be comprised of instructions, the ballot, a return envelope, the location of voting centers to drop off ballots, an assistance form, an ID request (if required), and an identification form. The voter should then understand what is required of them and subsequently mark their ballot correctly. If the voter needs assistance in marking their ballot, they submit an assistance certification form with the return of their ballot. If not, they simply mark the ballot themselves. If the voter's ballot requires an ID, then voter needs to include a valid copy in the return envelope; a similar practice occurs if the identification form is required.

Once the voter marks their ballot, they need to sign and date the oath of absentee. After that, the voter has the option of returning their ballot via mail or drop box. If they choose the drop box method, the ballot will be collected by an election official. If they choose to mail their ballot through the USPS, their ballot will be returned to their county BoE. Once the BoE receives the ballot, a notification is sent to the voter. Once an election official receives a marked ballot, they first check if it has been signed. If so, they verify the signature using signature verification from the voter's registration record. If not, the ballot is rejected or culled with the voter. The elections official then checks for any discrepancies with the ballot (filling in more than one candidate, etc.) If any exist, the voter may receive a chance to correct. If the voter chooses to correct the mistake, they have to resend their ballot again for another verification; otherwise their ballot will not be counted. Once fully checked, the ballot is opened and prepared for tabulation.

4. Risk in the Mail-Based Voting Process

Although an understanding of the mail-based voting process is important for elections security, elections officials need to understand how changes to the process can affect policy as well as actions to take to improve the process. Traditional industrial engineering analysis will reveal process bottlenecks that could slow down the processing and movement of ballots, but the integrity and security of ballots as they move through the system also need to be considered. To evaluate risk, we consider the risk model developed in [1] to identify the relative likelihood for risks

at established process nodes. To fully understand how and where risks develop over time and inform mitigations, we first must map the identified threats of concern to the mail-based voting process nodes.

The updated attack tree in [1] is organized into four branches, with a multitude of threat scenarios on each branch. Scenarios may consist of a single threat or a set of threats that must happen in parallel in order to attack and compromise the process. Scenarios that involve a single threat are evaluated to determine their respective relative likelihood of occurring; scenarios that involve a set of threats have a relative likelihood equivalent to the product of the relative likelihoods of all threats in that set (joint probability). Table 1 presents a summary of the threats of most concern, based on the analysis in [1]. The relative likelihood of each scenario is presented, along with the corresponding branch of the tree or source of the threat. This paper extends the analysis in [1] to include the process node to which the scenario is located. As a result, election officials may understand not only what is of most concern but also where and when that concern is in the process.

Table 1: Threat Scenarios of Most Concern (expanded from [1])

Scenario	Threat		Relative Likelihood	Branch	Process Node
S_7	X_9	Errant failed signature	0.12	Insider	47
S_{12}	X_{14}	Accidental loss	0.10	Insider	4
S_{23}	X_{28}	Fail to stuff envelope	0.11	Insider	38
S_{32}	X_{36}	Lost in destination mailroom	0.13	Insider	3
S_{47}	X_{53}	Malicious "messenger ballots"	0.10	External	18
S_{58}	X_{61}	Debate and vote parties	0.12	External	18
S_{64}	X_{65}	Failure to sign correctly	0.13	Voter Error	21
S_{66}	X_{67}	Failure to bundle correctly	0.11	Voter Error	17

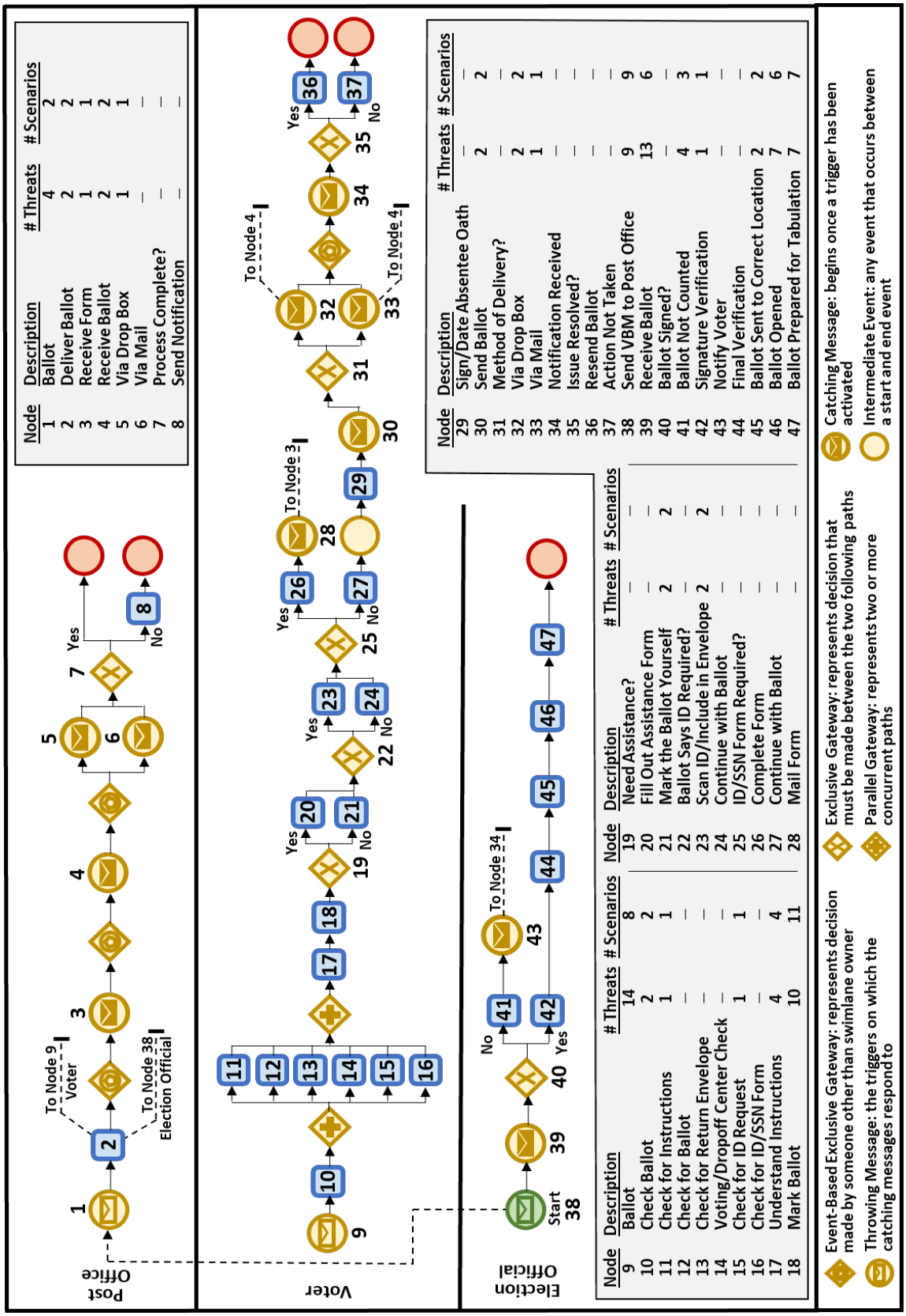
Our larger work [1] identifies S_{32}, S_{58}, and S_{64} as the most concerning scenarios within the insider, external, and voter error branches, respectively. Of the 40 attack scenarios that can be executed by a trusted process insider, losing ballots in the destination mailroom is the most concerning; mitigations include appropriate staffing and expeditiously sending ballots once requested [1]. Within the 23 scenarios of an external process attack, a debate and vote party is most concerning. Voters bring their ballots to a debate and vote party and may receive influence or pressure to mark their ballot in favor of a candidate; mitigations include attendance guidelines and supporting only unbiased aid for disabled voters who require assistance [1]. Finally, only 10 scenarios exist that are related to voter error or fraud. A failure to sign a ballot correctly is the most concerning, with mitigations including notice and cure for rejected ballots, enhanced standardized training, and encouraging voters to monitor the status of their ballot [1].

Within the map, there are certain process nodes that have multiple threats assigned to them but are not necessarily high concern scenarios. Those assigned threats may also be part of a parallel scenario, with the other threats in the scenario occurring at different nodes. Still, these nodes are of interest when designing process risk mitigations. Within the *voter* lane, this includes *ballot,* with 14 threats ranging in relative likelihood from 0.05 to 0.12, and *mark ballot,* with 10 threats ranging in relative likelihood from 0.06 to 0.12. In the *election officials* lane, *receive ballot* has 13 assigned threats, ranging from 0.05 to 0.08; *send Vote-By-Mail (VBM) to post office* has 9 threats, ranging from 0.05 to 0.11; *ballot is open* has 7 threats, ranging from 0.05 to 0.08; and *ballot is prepared for tabulation* has 7 threats, ranging from 0.06 to 0.12. Finally, the *post office* lane has the fewest assigned threats, with *ballot* being the most with four assigned, ranging from 0.06 to 0.07 relative likelihood. Overall, elections officials should be alert to these nodes, along with the nodes of most concern. If limited resources for mitigations exist, then officials can focus their efforts on the most concerning nodes, followed by the nodes with a high volume of threats.

Overall, the number of threats that map to each node are listed in Figure 1 along with the number of unique scenarios associated with each node. Note that some threats on the attack tree in [1] are outside of the mail-based process (e.g., X_{81} system outage), so the total number of threats mapped to the process does not align with the total of 102 threats. Furthermore, some scenarios involve a set of threats, and those threats may occur at multiple nodes. Thus, the total scenarios on the process map does not align with the total of 73 attack tree scenarios [1].

5. Conclusions and Future Work

Our research provides a process map for mail-based voting and identifies the extent of the threat in its activities. For the threats of most concern, mitigations are provided. In doing so, election officials may obtain greater awareness of where vulnerabilities may exist and the relative likelihood of their occurrence. They may also be able to apply security



Node	Description	# Threats	# Scenarios
1	Ballot	4	2
2	Deliver Ballot	2	2
3	Receive Form	1	1
4	Receive Ballot	2	2
5	Via Drop Box	1	1
6	Via Mail	—	—
7	Process Complete?	—	—
8	Send Notification	—	—

Node	Description	# Threats	# Scenarios
29	Sign/Date Absentee Oath	—	—
30	Send Ballot	2	2
31	Method of Delivery?	—	—
32	Via Drop Box	2	2
33	Via Mail	1	1
34	Notification Received	—	—
35	Issue Resolved?	—	—
36	Resend Ballot	—	—
37	Action Not Taken	—	—
38	Send VBM to Post Office	9	9
39	Receive Ballot	13	6
40	Ballot Signed?	—	—
41	Ballot Not Counted	4	3
42	Signature Verification	1	1
43	Notify Voter	—	—
44	Final Verification	—	—
45	Ballot Sent to Correct Location	2	2
46	Ballot Opened	7	6
47	Ballot Prepared for Tabulation	7	7

Node	Description	# Threats	# Scenarios
9	Ballot	14	8
10	Check Ballot	2	2
11	Check for Instructions	1	1
12	Check for Ballot	—	—
13	Check for Return Envelope	—	—
14	Voting/Dropoff Center Check	—	—
15	Check for ID Request	1	1
16	Check for ID/SSN Form	—	—
17	Understand Instructions	4	4
18	Mark Ballot	10	11
19	Need Assistance?	—	—
20	Fill Out Assistance Form	—	—
21	Mark the Ballot Yourself	2	2
22	Ballot Says ID Required?	—	—
23	Scan ID/Include in Envelope	2	2
24	Continue with Ballot	—	—
25	ID/SSN Form Required?	—	—
26	Complete Form	—	—
27	Continue with Ballot	—	—
28	Mail Form	—	—

Figure 1: Mail-Based Voting Process Map

measures more effectively and efficiently against the spectrum of threats from an insider, an external actor, or voter error.

Extensions of this research include identification of how risk evolves over time and introducing a temporal framework to risks in the process. A Markov model can further analyze and assess risk. In addition, this process map for mail-based voting can be incorporated with the in-person voting process map of Price, et al. [14] to create a holistic view of voting and associated elections security risks. Moving forward, mail-based voting will remain relevant and may continue to be used at scale, so this risk assessment has value beyond the 2020 election.

Acknowledgements

The views expressed in this paper are those of the authors and do not represent the official policy or position of the United States Military Academy, the United States Army, or the United States Department of Defense. This research is partially supported by the National Science Foundation, Grant 1663184, and the Towson University BTU Initiative.

References

[1] N. M. Scala, P. L. Goethals, J. Dehlinger, Y. Mezgebe, B. Jilcha, and I. Bloomquist, "Evaluating mail-based security for electoral processes using attack trees," journal paper under review.

[2] A. Smith, N. Zhou, and J. Wu, "Map: Turnout surged in 2020. See the numbers where you live," *NBC News,* December 2, 2020. [Online], Available: https://www.nbcnews.com/politics/2020-election/turnout-map-2020-election-n1249620. [Accessed Dec. 30, 2020].

[3] K. Walsh, "Early voting hits historic numbers in 2020," *ABC News,* November 2, 2020. [Online]. Available: https://abcnews.go.com/Politics/2020-early-voting-data-continues-hit-record-numbers/story?id=73701061. [Accessed Dec. 30, 2020].

[4] N. Corasaniti and S. Saul, "16 states have postponed primaries during the pandemic. Here's a list," *The New York Times,* August 10, 2020. [Online], Available: https://www.nytimes.com/article/2020-campaign-primary-calendar-coronavirus.html. [Accessed Dec. 30, 2020].

[5] J. P. Rotondi, "Vote-by-mail programs date back to the Civil War," *history.com*, Nov. 2, 2020. [Online]. Available: https://www.history.com/news/vote-by-mail-soldiers-war. [Accessed Dec. 30, 2020].

[6] "Postal voting in the United States," *Wikipedia.com*. [Online]. Available: https://en.wikipedia.org/wiki/Postal_voting_in_the_United_States#In_states. [Accessed Dec. 30, 2020].

[7] United States Election Assistance Commission, "The election administration and voting survey: A report to the 115th Congress," Washington, DC: 2016.

[8] University of South Alabama, "Election operations assessment: Threat trees and matrices and threat instance risk analyzer," Mobile, Alabama, 23 Dec. 2009.

[9] P. L. Goethals, N. M. Scala, and N. Bastian, "Operations research," in *Mathematics in Cyber Research*, P. L. Goethals, N. M. Scala, and D. Bennett, Eds. CRC Press, 2021, forthcoming.

[10] B. Schneier, "Attack trees," 1999. [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html. [Accessed: Sept. 26, 2020].

[11] H. S. Lallie, K. Debattista, and J. Bal, "A review of attack graph and attack tree visual syntax in cyber security," *Computer Science Review,* vol. 35, pp. 1-41, 2020.

[12] N. M. Scala and P. Goethals, "A review of and agenda for cybersecurity policy models," In Proc. Industrial and Systems Engineering Research Conference, 2006.

[13] Cybersecurity and Infrastructure Security Agency, "Election infrastructure security," *cisa.gov*. [Online]. Available: https://www.cisa.gov/election-security. [Accessed: Dec. 30, 2020].

[14] M. Price, N. M. Scala, P. L. Goethals, "Protecting Maryland's voting processes," *Baltimore Business Review,* pp. 36-39, 2019.

[15] H. Locraft, P. Gajendiran, M. Price, N. M. Scala, and P. L. Goethals, "Sources of risk in elections security," In Proc. Industrial and Systems Engineering Research Conference, 2019.

[16] J. Freund and B. Rücker, *Real-life BPMN, with introductions to CMMN and DMN*, 3rd ed. Camunda.

[17] "Mail voting process node descriptions," [Online]. Available: www.drnataliescala.com/projects. [Accessed: Apr. 9, 2021].