Proceedings of the American Society for Engineering Management 2025 International Annual Conference
H. Zhang,G. Natarajan, and E.H. Ng eds

SECURING U.S. ELECTIONS: THREATS, VULNERABILITIES, MITIGATIONS, AND OPPORTUNITIES FOR TECHNOLOGY

Amarachi Silverline Offor, M.S., M.A.
Vincent Schiavone, M.S.
Natalie M. Scala, Ph.D.*
Josh Dehlinger, Ph.D.
Towson University

Noah Hibbler, B.S., B.A.
University of Maryland, College Park

Navya Gautam, B.S.
Georgia Institute of Technology

***nscala@towson.edu**

Abstract
Election processes are a crucial function to support the health and strength of a democracy. With the recent rise in the propagation of misinformation and disinformation both in the United States and worldwide, it is more critical than ever that we establish and maintain public trust in democratic election processes. This paper presents and examines current threats to U.S. elections and voting equipment. We provide an inventory of current literature centered around cyber, physical, and insider threats to and vulnerabilities in U.S. voting systems. This inventory is one of the first to comprehensively expand beyond the 2009 Election Assistance Commission (EAC) attack tree, which has long served as a foundational framework for understanding the potential vulnerabilities within U.S. election systems. In addition to identifying, categorizing, and discussing these threats and vulnerabilities, we also conduct a thorough review of proposed voting processes based on cryptography and distributed ledger technologies. This includes examining current implementation status and challenges associated with potential adoption, as well as the feasibility and effectiveness of these solutions. By providing an in-depth analysis of current election threats, vulnerabilities, and proposed solutions, this paper offers valuable insights into ongoing and future efforts to secure U.S. elections. It also highlights areas where further research, technology innovation, and conceptual design are needed to ensure that election systems can withstand emerging threats while maintaining trust in democratic processes.

Keywords
Election security, distributed ledger technologies, risk, U.S. democracy

Introduction
Public trust in elections is one foundation of a free and fair democracy. Recent disinformation narratives have emerged in the United States, especially around Presidential elections. For example, in 2020 the public discourse suggested a "stolen election" and in 2024, rumors immediately circulated, starting on election night, about missing votes and untabulated ballots. Although these narratives are not factual, they can still shape public opinion and erode trust. Pennycook and Rand (2020) show that a single exposure to mis/disinformation begins to shape perceptions of truth, even if the information is not believed. Research shows that historically, supporters of the losing political party or candidate in an election tend to believe votes were miscounted, and that effect has grown over time across the United States (Sances & Stewart, 2015). In 2024, narratives began immediately after the Presidential race was called, and the time needed to count and cure all mail and provisional ballots nationwide plus certify the election allowed for a false perception of truth to take hold on some social media platforms. Silence in the absence of truth allows for rumors and disinformation, and once those enter the discourse, there is a lasting effect on reason, even when corrected (Ecker,

et al., 2022). In the context of the current highly polarized and politically charged culture in the United States, disinformation narratives can be counteracted quickly with secure, trusted, timely counting, and tabulation of votes, allowing for the outcome of the election to be known broadly and swiftly.

However, disinformation narratives are not the only threat to free and fair elections. Actual vulnerabilities in elections equipment, and trusted insiders who have the access to possibly exploit them, pose further risks. Scala, et al. (2024) show that most poll workers are altruistic but some may be rogue; honest mistakes may introduce risk into the elections process. Furthermore, the *Curling v. Raffensperger* (2023) litigation in Georgia revealed vulnerabilities in critical infrastructure ballot marking devices (BMD) electronic voting equipment.

This research examines threats to elections and limitations of currently used electronic voting equipment, proposing emerging technologies to enhance the security of critical infrastructure voting equipment and the timeliness of vote counts. Stronger systems and processes can help to dispel mis/disinformation narratives and enhance both public and global trust in United States elections.

United States Voting Equipment and Associated Threats

States have continuously modernized voting equipment and processes since the late 1800s, introducing what was emerging technology at each historical point in time to improve election integrity and speed up the process of counting votes (Stewart, 2011). Efforts to modernize over time considered shifting demographics in America (e.g. population centers), evolution of state and local election laws, and adaptive adversaries that have interest in meddling in elections.

The types of electronic voting equipment used nationwide have evolved since the Help America Vote Act (HAVA), which Congress passed after the 2000 Presidential election, hanging chads debacle, and subsequent *Bush v. Gore* litigation. HAVA moved elections equipment from mechanical levers and punch cards to electronic systems. Early electronic systems included direct-recording electronic (DRE) machines, which were considered emerging technologies at the time. Those machines had the voter make choices via a touchscreen, and the votes were stored via internal memory with a tabulation printout. This equipment has mostly become obsolete for the lack of a non-auditable paper trail, replaced with the auditable paper trail precinct count optical scanner (PCOS) and ballot marking devices (BMD) machines to support best practices in security. PCOS machines use a voter marked paper ballot which is then scanned through an optical scanner; the ballot is maintained for audit. BMD machines also allow touchscreen voting, but a paper receipt is printed for voter confirmation. The receipts are then typically fed into an PCOS for counting. The goal of DRE, BMD, and PCOS machines post-HAVA are to increase the speed of counting votes, remove ambiguity in voter choice evident in punch cards, and modernize elections in the United States.

During the 2024 election cycle, the majority of the United States electorate (approximately 70%) who voted in-person did so on precinct count optical scanning (PCOS) machines (Verified Voting, n.d.). Most of the remaining electorate voted on BMD. A small percentage of electorate used legacy direct-recording electronic (DRE) voting machines. PCOS machines have increased in use since 2016, which was the first known election that broadly faced allegations of interference from and meddling by foreign nation states (Sanger & Edmonson, 2019).

Although the use of PCOS and BMD machines provide considerable improvements to election integrity, voter accessibility, and the speed at which election officials can determine results over the older pre-HAVA and DRE technologies, threats and vulnerabilities still exist in in-person equipment. The US EAC (2009) present attack trees for in-person voting equipment, including PCOS and DRE machines, outlining all scenarios in which the systems can be breached. The EAC attack tree includes known threats to PCOS equipment, but the attack surface evolved since its creation in 2009. United States election equipment is now critical infrastructure, adversaries adapt, and the COVID-19 pandemic dramatically and quickly changed the way the electorate voted in 2020 (Scala, et al., 2022). The original attack trees are no longer current.

Other research on election security (e.g., Appendix 1) expanded on potential threats or identified case studies of known issues in election voting equipment post HAVA. However, these papers mostly identify potential threats and vulnerabilities; there is no discussion of the risk associated with that threat. The probability or relative likelihood of a threat being exploited along with the corresponding impact in the event of exploitation have not been calculated or measured in the election literature. As a result, states and localities are left with a myriad of potential threats to mitigate, often on limited budgets and with scare resources, without guidance on where to focus their security efforts. The electorate is then exposed to vulnerabilities, slow counts, and delayed certifications that allow disinformation narratives to potentially take hold and threaten the integrity of the cast votes.

Threat, Vulnerability, and Opportunity for Risk Analysis

Appendix 1 presents a selection of literature that identifies or proposes threats to United States voting equipment. To the authors' knowledge, this is the first catalog of threats and vulnerabilities to elections, beyond the United States

EAC (2009) attack tree. This includes implications related to election systems and how those threats can potentially impact the security of voting systems in the United States.

To create a catalog of papers, an initial search was done, with *threats to voting* and *threats to elections* as the keywords, considering papers both domestically and internationally. Other keywords included *disenfrancisment* and *voting technologies*. Relevant papers were then entered into both Google Scholar and Connected Papers to find other papers that cited that work. The catalog was collected over time, with the first searches occurring during spring 2020, and subsequent searches occurring each academic semester through summer 2024.

Appendix 1 is limited by the literature itself in that these papers discuss threat and vulnerability but not risk, failing to calculate a relative likelihood or probability of that threat being exploited. Cahn (2017) discusses known threats that have been exploited in equipment, but these are single, limited instances that, to public knowledge, did not have broad implications to an election. Strength of threat along with broad impact are both important considerations, and the lack of research in those areas provide opportunities for risk analysis to contribute to election security and integrity. Scala, et al. (2022) analyze risk to mail voting and provide a relative likelihood calculation of threats of most concern. However, the research is limited to mail voting, which is fundamentally different from and much smaller than the in-person voting process in the United States.

Price, et al. (2019) and Locraft, et al. (2019) were the first to propose threats to elections as a systemic interplay between cyber, physical, and insider sources and argue that process risk and threats to elections can shift between all three sources, albeit temporarily or via mitigations targeted towards one particular source. We extend and provide context to the inventory of threat literature in Appendix 1 by classifying the threats proposed in those papers into cyber, physical, and insider sources. Following the guidance in Price, et al. (2019) and Locraft, et al. (2019) we define broadly as follows:

- Cyber threats involve the exploitation of digital devices and media for the collection, tallying, and transmission of votes, regardless of whether the system is connected to the Internet.
- Physical threats consist of tampering with or disrupting election equipment before, during, or after an election.
- Insider threats stem from human actions, including unintentional mistakes by users and deliberate malicious activities, with ill-harm effects.

A benefit of considering the source of threat is that mitigations may differ for each source. For example, removing an internet connection from a PCOS scanner can eliminate the threat of vote tampering during transmission from the polling place to the central count, but the PCOS machine will still need a method to store the optically scanned votes. Commonly, flash drives replace internet connections, but those drives may be compromised during manufacture, lost during transfer back to the central count, or misused (Price, et al., 2019). In this example, the overall threat of vote miscount or tampering is not eliminated but rather transferred. The total risk may or may not be reduced. The literature currently does not address total risk in the in-person voting process in the United States, leading to another opportunity for risk analysis in election integrity and security research.

Limitations in Mitigations and Digital Voting

In a broader sense, implementing mitigations against threats may just transfer risk to another source, reduce total risk, or even increase total risk. Regardless, researchers have proposed digital mitigations and process changes for elections to address security risks; promote integrity, security, reliability; and protect voter rights in electoral processes. However, these ideas have faced roadblocks or been ineffective in practice. Common limitations include functional constraints, implementation challenges, and insufficient stakeholder adoption. Other concerns include problems outside the control of the election administration including machine failures or poll worker errors (Lazarus, et al., 2011). Furthermore, mitigations or process changes need to address the risks presented in Appendix 1; the literature has not always been clear on the benefits to actual mitigation of risk through digital forms of voting or related process changes. Moreover, in practical applications, counties and localities have not been able to reach an agreement on cyber norms and best practices to mitigate risk (Shackelford, et al., 2016).

Complexity of the process or equipment changes can also be a roadblock to implementing mitigations or addressing risk. Providing extensive training for election officials or poll workers can be a limitation, considering states and localities have limited budgets for election administration. Those budgets can also limit the opportunity to purchase new digital election equipment. Furthermore, many Americans prefer to vote in person; this is not only driven by familiarity but also tradition, especially among historically marginalized communities (Williams, 2020). Motivations for in-person voting can be influenced by convenience and concerns about ballot security (Riley, et al., 2024). These concerns, along with the user experience and institutional trust, are amplified when considering digital forms of voting. Even though voting online has been considered as a solution to promote universal equal access, pilots

have encountered a myriad of concerns, including the lack of a verifiable paper trail, unclear methods to audit results, questions about voter anonymity, and concerns about protecting against tampering.

Exhibit 1 presents a set of papers in the literature that aim to enable or improve electronic and internet voting. Across these papers and proposals, common limitations to widespread use include implementation vulnerabilities, lack of best practices and consistent frameworks, security vs. usability tradeoffs, and inconsideration of sociotechnical implications. For example, the pilot of internet voting in Washington, D.C. was undermined by poor coding, configuration errors, and insufficient auditing (Wolchok, et al., 2012). In general, the research in Exhibit 1 identifies that voter authentication, auditability, and verification are of prime concern with internet and digital based voting; transparency, rigorous testing, and adversarial auditing become essential for any functional deployment of technology in voting.

Exhibit 1. Literature Addressing Electronic and Internet Voting.

Authors	Goal of Research	Main Finding
Wolchok, et al. (2012)	Describe how implementation errors impact likelihood of exploitation and how election officials can detect, respond, and recover from attacks	Internet voting is vulnerable to various attacks, as secure Internet voting is still far from being achievable; Other methods of voting should be used instead
Simons and Jones (2012)	Research different ways in which internet is used in the voting process and the security of the same	A balance should be maintained between the integrity of the election technology and the convenience of voting; Policymakers need to understand the full effects of the Internet voting systems before they mandate that counties use them
Paul and Tanenbaum (2009)	An electronic voting strategy that takes a systems approach, incorporating a trustworthy process based on open-source software, simplified procedures, and built-in redundant safeguards to prevent tampering	Procedures and techniques function together to yield a reliable voting system; Ensure security from the generation of the first key to the publishing of results
Mursi, et al. (2013)	Examine the evolution of election technology; Provide summary of the security requirements for electronic voting systems; Explore the cryptographic security measures in e-voting schemes; Analyze the vulnerabilities of e-voting systems; Suggest improvements for recent e-voting schemes and systems	Three gaps - technological, sociotechnical, and social - must be understood before developing a system and its corresponding security requirements; Use of biometrics is useful for ascertaining, securing, and maintaining voter identity; Voter education is of utmost importance
Clarkson, et al. (2008)	Describe the design and implementation of Civitas, an electronic voting system for remote voting that is proposed to be resistant to voter coercion	Testing indicates that real-world elections can feasibly balance affordability, efficient vote counting, and strong security measures

The literature also contains some limited research on the use of cryptography in voting systems. Park and Rivest (2017) explore cryptographic and system-level requirements for implementation of quadratic voting, where the electorate not only makes choice but also rates the intensity of their preference. Such a form of voting introduces new complexities in privacy and fairness. The authors argue that quadratic voting requires robust cryptographic primitives, such as zero-knowledge proofs and privacy-preserving tallying mechanisms. That being said, the work is completely conceptual, as voting in the United States does not include intensity of preference, only choice. Juels, et al. (2005) address the risk of voter coercion, which is not addressed in the e-voting literature and is an election security risk. The

authors propose a protocol that uses mix-nets and fake credential generation to protect voters, allowing them to cast ballots even under duress without compromising privacy. This approach has not been implemented or evaluated at scale in real elections. Both papers highlight the gap between cryptographic design and actual application in elections.

Next Generation of Voters and Voting Technologies

United States voting is still primarily an in-person process, with mail voting gaining prominence but still mostly an absentee process. However, the demographics in the electorate are shifting. By 2050, about 20% of the US population will be from Generation Alpha, another 20% from Generation Z, and just 4-5% comprised of Baby Boomers (Vespa, et al., 2020). Younger Americans, such as Generations Alpha and Z, structure their lives differently than older Americans and use cell phones and mobile devices ubiquitously. Generations that are inherently comfortable with digital technologies may be open to new processes or ways to vote. In 2016, a majority of voters in seven states voted by mail (US EAC, 2017). The *Curling vs. Raffensberger* (2023) litigation in Georgia highlighted the inherent risks in ballot marking devices, including the possibilities for flipping votes, under voting, and over voting. The landscape in the United States is slowly becoming primed for new technologies in voting.

Considering cultural shifts, the need for speed with accuracy in the tabulation of votes, and the threats and vulnerabilities inherent in existing voting methods, emerging research should consider new solutions for voting equipment that still uphold the integrity of votes and anonymity of the voter. Distributed ledger technologies (DLT) are one example of such a solution. A DLT is a peer-to-peer network of computers reliant on public key cryptography and consensus mechanisms where every member of the network has a copy of all other records, ensuring data integrity and resilience against tampering (El Ioini & Pahl, 2018). Blockchain, which has gained public attention for its use in Bitcoin, is one common example of a DLT (Zheng et al., 2017). DLT may enhance voter trust and confidence in the electoral process by providing a secure, transparent, and tamper-resistant system in which each voter can independently verify the accurate recording of their vote.

Benefits of and a Vision for DLT in Voting

In particular, DLT technologies can address limitations of current and proposed voting systems while offering mitigations for risks and vulnerabilities. For example, DLT systems can handle large volumes efficiently, reduce manual effort, and minimize human error while maintaining a reliable audit trail of votes. It provides a digital backup that can be verified with the machine and, if necessary, hand counts. Using DLT with current paper ballots still allows for the paper trail with speed of count and verifiable audit.

Every vote recorded on the system is time-stamped, immutable, and publicly verifiable. Every voter could find their private key in the ledger, which should reduce public doubt in counts while addressing potential voter fraud more effectively. The goal is to ensure voter confidence in the legitimacy of the count by increasing transparency in the process. DLT systems are connected by nodes; each piece of equipment can then communicate and verify the deployed software on the network. Furthermore, the distributed data architecture requires multiple, simultaneous incidents of data corruption or manipulation for an entire system failure, dramatically increasing fault tolerance while ensuring a resilient, auditable record.

Votes on the DLT ledger can be tallied in real time. If a transaction size (i.e., number of votes cast) is different than the maximum allowed, the DLT network could flag the record for mandatory review by that precinct. Double voting can also easily be prevented by DLT. A hash algorithm could use voter data and identification to create a unique and anonymized code within the network. That cryptographic key would be both public and private to authenticate and validate interactions with the rest of the network. As a result, a voter would be unable to perform two transactions or votes with their same identifier because their unique ID code would already be registered on the ledger.

DLT can be integrated with existing voting equipment, such as PCOS machines, to address threats and challenges without fundamentally disrupting the current in-person voting process. In one potential model for DLT enabled systems under development, a plug-and-play hardware module could be added to every voting machine in a state or precinct. Data about each ballot and the votes on the ballot would then be recorded with a cryptographic signature in a ledger entry immediately after it passes through the scanner. The record of ballots and votes would then be transmitted to every other node on the DLT network while also receiving vote records from the remote nodes. The record of all votes would then be frozen at the end of the voting day in an immutable ledger; the vote counts but not the voter identification could then be made available for public review and analysis.

Potential Limitations of DLT

Using DLT in United States voting is still in the conceptual stage, and more research is needed to develop prototype systems, test them, and then deploy at scale. Any new system or technology would need to earn the confidence of the

voting electorate, and DLT is not the only potential solution to mitigating existing vulnerabilities, increasing the speed of count, and modernizing voting equipment.

DLT systems would have some limitations. Maintaing scalability during high-traffic periods can be difficult, which may potentially slow the efficiency of vote processing. Additionally, ensuring accessibility to DLT-enabled voting platforms for all voters, including Americans with Disabilities Act compliance and those with limited access to technology or digital literacy, requires design with user-friendly interfaces and adaptations. Implementation of DLT or any emerging technology may require legislation to support the technological standard and voter verification requirements. The passage of legislation would most likely be piecemeal, as elections are state responsibilities in the United States. Each of the states, along with the territories and the district, may have its own process and timeline. The adaptation of a DLT system would need to be done by an entire state at the same time. For example, if two counties or localities are not on the same DLT network, a person could vote once in each county. The network would not catch the double-vote in real time because it occurred on two separate networks. Post-election audits would still be needed to catch potential voter fraud across multiple networks or technologies.

Three major security concerns for DLT are node corruption, denial-of-service attacks, and consensus failure. Some node corruptions caused by disasters, such as power-outages, hardware failure, and human error, can be mitigated by methods such as uninterruptible power supplies, paper backups, and training, which are already implemented for BMDs. An election-oriented DLT would most likely use a permissioned blockchain model, such as Hyperledger Fabric or R3 Corda, that is only accessible to authorized users/nodes (Polge, et al., 2021). Compared to permissionless blockchains (e.g., Bitcoin) which allow anyone to join, permissioned DLT networks control the endpoints, which significantly reduce the risk of malicious actors compromising the confidentiality or integrity of the network. These nodes may still be corrupted or affected by cyber attacks, such as denial-of-service attacks and will require robust firewalls (Zargar, et al., 2013).

Funding would be needed to support the deployment of equipment that either interfaces with existing scanners or is independent of current machines. High speed internet connectivity would be imperative for DLT. Virtual private networks or other security measures can mitigate the additional vulnerabilities created by connecting voting machines to a network, but the raw bandwidth requirements for most DLTs may not immediately be available in rural areas or smaller counties. The DLT benefits related to vote integrity would come from widespread implementation, and the value could considerably diminish or eliminate if parts of a state or precincts are not able to be part of the network.

Looking Forward

Both the benefits and potential limitations of DLT are important ideas to consider as the needs of the United States electorate change. The current polarized state of U.S. culture must lean on data to drive truth and minimize disinformation; the speed of an accurate vote count remains essential. DLT may not be the only solution; quantum computing and quantum blockchains are also showing early conceptual promise in ensuring the integrity of votes while upholding voter integrity. The key is that any new potential technology must outperform the benefits of an existing system, and the threats and risks associated with election technology remain of primary concern. Having a system that can mitigate or reduce total risk while also maintaining speed of count and anonymity would be an improvement and a true countermeasure to any potential adversarial interference or meddling in U.S. elections.

Conclusions

This paper presents an inventory of risks in current U.S. voting systems and identifies a research agenda to incorporate emerging technologies, such as DLT, into election equipment. We identify concerns to address in potential new technologies and offer a direction for the research in this area. We extend the inventory of risks in the literature to highlight the cyber, physical, and insider sources of threat. Although the federal government has identified that recent elections have been secure (CISA, 2020), the public belief in the outcome of elections remains perilous. Any new technology needs to be not only cyber, physical, and insider secure, but also have the support of the voting electorate.

We posit that reasonably measured caution in the literature related to cryptographical voting systems should not prevent the broader exploration of integrating emerging technologies with existing voting technology. DLT and other emerging technologies must be continually evaluated for their potential to improve the existing systems.

DLT is not a panacea, but it addresses a variety of computer-enabled vote manipulation threats directly while also providing an additional means of integrity assurance. The integration of emerging technologies with election systems is necessary to enable rapid adaptation to dynamic risk environments and combat more complex election threats. Future research should address the implementation of DLT and other emerging technologies in election security and investigate complementary technologies to be used in conjunction with existing infrastructure to mitigate damages and stop threats at the cyber, physical, or insider source, ensuring a safe, secure, and trusted election process.

AI in Technical Writing

AI and AI-assisted technologies were not used in preparing this manuscript.

Acknowledgments

The authors would like to thank Alisa C. Martin for her help in verifying the papers in Appendix 1 and Exhibit 1. This research was partially funded by the Office of Graduate Studies and the Provost Research Fellows Program at Towson University. Funding from the Science of Security program at the United States Department of Defense also supported this work.

References

Abilov, A., Hua, Y., Matatov, H., Amir, O., & Naaman, M. (2021). VoterFraud2020: A multi-modal dataset of election fraud claims on Twitter. *Proceedings of the International AAAI Conference on Web and Social Media, 15*(1), 901-912.

Agarwal, P., Ko, J., & Zhang, M. (n.d.). Securing the vote: The risks to election security in 2020. *Carnegie International Relations and Politics (CIRP) Journal, 5*(1), 13-17.

Aviv, A., Cerny, P., Clark, S., Cronin, E., Shah, G., Sherr, M., & Blaze, M. (2008). Security evaluation of ES&S voting machines and election management system. In *Proceedings of the conference on Electronic Voting Technology (EVT'08)* (Article 11, pp. 1–13). USENIX Association.

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.

Barouh, A. (2020). A new old solution: Why the United States should vote by mail-in ballot. *Seattle Journal for Social Justice, 18*(2), 243-273.

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 Klein Center Research Publication No. 2020-6). Berkman Klein Center for Internet & Society at Harvard University.

Blake II, J. (2020). Russian interference in US elections: How to protect critical election infrastructure from foreign participation. *Public Contract Law Journal, 49*(4), 709–734.

Blaze, M., Braun, J., Hursti, H., Hall, J. L., MacAlpine, M., & Moss, J. (2017). *DEF CON 25 voting machine hacking village*. DEF CON Communications. https://tinyurl.com/ymx4r4nw

Blaze, M., Hursti, H., Macalpine, M., Hanley, M., Moss, J., Wehr, R., Spencer, K., & Ferris, C. (2019). *DEF CON 27 voting machine hacking village*. DEF CON Communications. https://tinyurl.com/bdee5a9m

Brunner, J. (2007). *Project EVEREST: Evaluation and validation of election-related equipment, standards and testing*. Ohio Secretary of State. https://tinyurl.com/yn2989dj

Cahn, D. (2017). *Risk assessment: How secure are voting machines*. [Unpublished capstone thesis]. University of Pennsylvania.

Clarkson, M. R., Chong, S., & Myers, A. C. (2008). Civitas: Toward a secure voting system. *2008 IEEE Symposium on Security and Privacy (SP 2008)*, 354–368.

Cui, A., Costello, M., & Stolfo, S. J. (2013). When firmware modifications attack: A case study of embedded exploitation. In *Proceedings of the 2013 Network and Distributed System Security Symposium (NDSS).* https://academiccommons.columbia.edu/doi/10.7916/D8P55NKB

Curling v. Raffensperger, 702 F. Supp. 3d 1303 (N.D. Ga. 2023).

Cybersecurity and Infrastructure Security Agency. (2020, November 12). *Joint statement from Elections Infrastructure Government Coordinating Council & the Election Infrastructure Sector Coordinating Executive Committees*. https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election

de Jong, M., van Hoof, J., & Gosselt, J. (2008). Voters' perceptions of voting technology: Paper ballots versus voting machine with and without paper audit trail. *Social Science Computer Review, 26*(4), 399–410.

Ecker, U. K. H., Lewandowsky, S., Cook, J., Schmid, P., Fazio, L. K., Brashier, N. M., Kendeou, P., Vraga, E. K., & Amazeen, M. A. (2022). The psychological drivers of misinformation belief and its resistance to correction. *Nature Reviews Psychology, 1*(1), 13–29.

El Ioini, N. & Pahl, C. (2018). A review of distributed ledger technologies. In In *Proceedings of the OTM 2018 Confederated International Conferences: CoopIS, C&TC, and ODBASE (Part II)* (Lecture Notes in Computer Science, Vol. 11222, pp. 277–288). Springer. https://doi.org/10.1007/978-3-030-02671-4_16

Epstein, J. (2007). Electronic voting. *Computer, 40*(8), 92–95. https://doi.org/10.1109/MC.2007.271

Epstein, J. (2012). Can we be too careful? *IEEE Security & Privacy, 10*(2), 3–5.

Feldman, A. J., Halderman, J. A., & Felten, E. W. (2007). Security analysis of the Diebold AccuVote-TS voting machine. In *Proceedings of the USENIX Workshop on Accurate Electronic Voting Technology (EVT '07)* (p. 2). USENIX Association. https://dl.acm.org/doi/10.5555/1323111.1323113

Fick, A. (2021). *How states can secure voting by mail*. The Foundation for Government Accountability. https://thefga.org/research/secure-voting-by-mail

Fidler, D. P. (2017). *Transforming election cybersecurity*. Digital and Cyberspace Policy Program. https://www.repository.law.indiana.edu/facpub/2547

Halderman, J. A., Rescorla, E., Shacham, H., & Wagner, D. (2008). You go to elections with the voting system you have: Stop-gap mitigations for deployed voting systems. In *Proceedings of the Conference on Electronic Voting Technology (EVT '08)* (Article 4, pp. 1–14). USENIX Association.

Herron, M. C. & Smith, D. A. (2021). Postal delivery disruptions and the fragility of voting by mail: Lessons from Maine. *Research & Politics, 8*(1), 1-12. https://doi.org/10.1177/2053168020981434

Hopkins, D. J., Meredith, M., Chainani, A., Olin, N., & Tse, T. (2021). Results from a 2020 field experiment encouraging voting by mail. *Proceedings of the National Academy of Sciences, 118*(4), 1-3.

Hughes, L. (2021). *In line of fire: Safeguarding America's election security* (Master's thesis). Naval Postgraduate School.

Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for electronic voting system—Review and open research challenges. *Sensors, 21*(17), 1-22.

Johnson, D. B. (2020). *Voting machine security: Too little too late*? https://www.route-fifty.com/cybersecurity/2020/01/voting-machine-security-too-little-too-late/312540/

Juels, A., Catalano, D., & Jakobsson, M. (2005). Coercion-resistant electronic elections. In *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society (WPES '05)* (pp. 61–70). Association for Computing Machinery.

Kasongo, E. N. (2021). *Texas election security: How prepared are county officials to defend against cyber threats to electoral infrastructure?* (Master's thesis). University of Houston.

Kerschbaum, F. (2022) Security Considerations in Designing Electronic Voting. *Next-Generation Technology and Electoral Democracy: Understanding the Changing Environment*. https://issuu.com/cigi/docs/kas_special_report_march_23_final1/s/15197167

Kortum, P., Stein, R., Acemyan, C. Z., Wallach, D. S., & Vann, E. (2020). How human factors can help preserve democracy in the age of pandemics. *Human factors*, *62*(7), 1077-1086.

Lazarus, E. L., Dill, D. L., & Epstein, J. (2011). Applying a reusable election threat model at the county level. In *2011 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 11)*. USENIX Association.

Lee, S. O. (2020). Vote-from-home? Evaluation framework for election security on remote voting in response to COVID-19. *SSRN preprints.* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3685381

Li, Y., Hu, X., & Zhao, P. (2021). On the reliability of a voting system under cyber attacks. *Reliability Engineering & System Safety, 216*, 1-12. https://doi.org/10.1016/j.ress.2021.107996

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*, 1572–1577. Institute of Industrial and Systems Engineers.

Lott, J. R., Jr. (2021). A simple test for the extent of vote fraud with absentee ballots in the 2020 presidential election: Georgia and Pennsylvania data. *SSRN preprints*. https://doi.org/10.2139/ssrn.3756988

Manpearl, E. (2018). Securing U.S. election systems: Designating U.S. election systems as critical infrastructure and instituting election security reforms. *Boston University Journal of Science & Technology Law, 24*(1), 169–192.

Mursi, M. F., Assassa, G. M., Abdelhafez, A., & Samra, K. M. A. (2013). On the development of electronic voting: a survey. *International Journal of Computer Applications*, *61*(16), 1-11.

Neisler, V. (2020). Voting by mail: Issues and resources. *Michigan Bar Journal, 8,* 46-48.

Park, S. & Rivest, R. L. (2017). Towards secure quadratic voting. *Public Choice*, *172*, 151-175.

Park, S., Specter, M., Narula, N., & Rivest, R. L. (2021). Going from bad to worse: from internet voting to blockchain voting. *Journal of Cybersecurity*, *7*(1), 1-15.

Paul, N. & Tanenbaum, A. S. (2009). Trustworthy voting: From machine to system. *Computer*, *42*(5), 23-29.

Pennycook, G., & Rand, D. G. (2020). Who falls for fake news? The roles of bullshit receptivity, overclaiming, familiarity, and analytic thinking. *Journal of Personality*, *88*(2), 185-200.

Persily, N. & Stewart III, C. (2021). The miracle and tragedy of the 2020 US election. *Journal of Democracy*, *32*(2), 159-178.

Polge, J., Robert, J., & Le Traon, Y. (2021). Permissioned blockchain frameworks in the industry: A comparison. *ICT Express,* 7(2), 229-233.

Price, M., Scala, N. M., & Goethals, P. L. (2019). Protecting Maryland's voting processes. *Baltimore Business Review: A Maryland Journal.* tinyurl.com/PriceEtAl2019

Raunak, M. S., Chen, B., Elssamadisy, A., Clarke, L. A., & Osterweil, L. J. (2006). Definition and analysis of election processes. *Proceedings of Software Process Change: International Software Process Workshop and International Workshop on Software Process Simulation and Modeling.* (pp. 178-185). Springer Berlin Heidelberg.

Riley, J., Gregorio, V., Gautam, N., Kouassi, M., Scala, N. M., & Dehlinger, J. (2024). Voting percetions and the impact of misinformation. *Proceedings of the 17th NATO Operations Research and Analysis (OR&A) Conference.*

Sances, M. W., & Stewart III, C. (2015). Partisanship and confidence in the vote count: Evidence from US national elections since 2000. *Electoral Studies*, *40*, 176-188.

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., Delgado Licona, K., & Ieromonahos, A. (2020, March 18). Empowering election judges to secure our elections. *Baltimore Business Review.* https://wp.towson.edu/bbr/2020/03/18/empowering-election-judges-to-secure-our-elections/

Scala, N. M., Goethals, P. L., Dehlinger, J., Mezgebe, Y., Jilcha, B., & Bloomquist, I. (2022). Evaluating mail-based security for electoral processes using attack trees. *Risk Analysis*, *42*(10), 2327–2343.

Scala, N. M., Rajgopal, J., Mezgebe, Y., & Dehlinger, J. (2024, advance). An information-theoretic analysis of security behavior intentions amongst United States poll workers. *Risk Analysis*, 1–17.

Schmidt, A. & Albert, L. A. (2020). Resilient voting systems during the COVID-19 pandemic: A discrete event simulation approach. University of Wisconsin - Madison. http://pfigshare-u-files.s3.amazonaws.com/24740783/2020ElectionSimulation.pdf

Shackelford, S. J., Schneier, B., Sulmeyer, M., Boustead, A., Buchanan, B., Deckard, A. N. C., Herr, T., & Smith, J. M. (2016). Making democracy harder to hack. *University of Michigan Journal of Law Reform, 50*, 629–678.

Shanton, K. & Underhill, W. (2014, June). Costs of voter identification. *National Conference of State Legislatures*. https://tinyurl.com/3rhac66z

Simons, B. & Jones, D. W. (2012). Internet voting in the US. *Communications of the ACM*, *55*(10), 68-77.

Stewart III, C. (2011). Voting technologies. *Annual Review of Political Science, 14(1)*, 353–378.

Torres-Lugo, C., Yang, K. C., & Menczer, F. (2022, May). The manufacture of partisan echo chambers by follow train abuse on Twitter. *Proceedings of the International AAAI Conference on Web and Social Media* (Vol. 16, pp. 1017-1028). https://ojs.aaai.org/index.php/ICWSM/article/view/19354

United States Election Assistance Commission Advisory Board. (2009). *Election operations assessment: Threat trees and matrices and threat instance risk analyzer (TIRA)*. https://tinyurl.com/4fd2wssw

U.S. Election Assistance Commission. (2017). *The Election Administration and Voting Survey: 2016 comprehensive report*. https://www.eac.gov/sites/default/files/eac_assets/1/6/2016_EAVS_Comprehensive_Report.pdf

Verified Voting. (n.d.). The Verifier — Election Day Equipment. tinyurl.com/4tpfmj9d

Vespa, J., Armstrong, D. M., & Medina, L. (2020). Demographic turning points for the United States: Population projections for 2020 to 2060 (Current Population Reports, P25-1144). *U.S. Census Bureau.* https://www.census.gov/content/dam/Census/library/publications/2020/demo/p25-1144.pdf

Williams C. (2020) Why blacks distrust voting by mail. *The Columbus Dispatch*. https://www.dispatch.com/story/news/politics/elections/2020/08/02/why-blacks-distrust- voting-by-mail/112788502/

Wolchok, S., Wustrow, E., Isabel, D., & Halderman, J. A. (2012). Attacking the Washington, DC Internet voting system. *Proceedings of Financial Cryptography and Data Security: 16th International Conference* (pp. 114-128). Springer Berlin Heidelberg.

Yasinsac, A. (2010, December). Insider threats to voting systems. *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies* (pp. 1-8).

Yoder, J., Handan-Nader, C., Myers, A., Nowacki, T., Thompson, D. M., Wu, J. A., Yorgason, C., & Hall, A. B. (2020). Absentee voting is popular during COVID-19 but does not change turnout or partisan rates of voting. *Democracy & Polarization Lab, Stanford University*.

Zargar, S. T., Joshi, J., & Tipper, D. (2013). A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. *IEEE Communications Surveys & Tutorials, 15*(4), 2046-2069.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. *Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress)* (pp. 557–564). https://doi.org/10.1109/BigDataCongress.2017.85

About the Author(s)

Amarachi Silverline Offor, M.S., M.A. holds a M.S. in Supply Chain Management and Marketing Intelligence from Towson University, an M.A in Communication Management from the University of Alabama at Birmingham, and a BSc. in Marketing from Covenant University, Nigeria. She works as a Continuous Improvement Specialist at Pandora Jewelry. Her research focuses on technology-driven approaches to supply chain risk management, emerging technology for election security, and using marketing analytics to enhance customer experience. Amarachi is a member of WiCyS and WTTC, and shares her passion for storytelling through photography and *The Supply Chain Cafe* podcast, which she hosts and leads.

Vincent Schiavone, M.S. is a research assistant at Towson University where he graduated with a Master's Degree in Supply Chain Management and a Bachelor's Degree in Project Management and Business Analysis. He is credited with acknowledgements and authorship on various academic papers spanning topics such as Naval Seabasing, Collaborative Scheduling in Construction Projects, and Election Security. Vincent is currently a Global Supply Chain Manager for Northrop Grumman and will be moving to a Program Manager role for the new international G/ATOR radar program. In his roles, Vincent works with various vendors across the globe to procure material on-time and within budget.

Natalie M. Scala, Ph.D., is a professor in the College of Business and Economics, a fellow of the Center for Interdisciplinary and Innovative Cybersecurity, and the director of accelerated programs at Towson University. She is also a faculty affiliate of the Applied Research Lab for Intelligence and Security at the University of Maryland. She earned Ph.D. and M.S. degrees in Industrial Engineering from the University of Pittsburgh. Her primary research is in military and security decision analysis, including risk in voting systems, integrity of votes throughout the supply chain, poll worker education, and cybersecurity metrics and best practices.

Josh Dehlinger, Ph.D., is a professor in the Department of Computer and Information Sciences at Towson University. He received his Ph.D. in Computer Science from Iowa State University in 2007 and served as a Research Scientist in the Charles L. Brown Department of Electrical and Computer Engineering at the University of Virginia in 2008. His research expertise lies, broadly, in software safety/reliability, election security, machine learning for software engineering, and computer science education.

Noah Hibbler, B.S., B.A. is a research assistant at the Applied Research Laboratory for Intelligence and Security. He earned a B.S. in Information Science and B.A. in Persian Studies from the University of Maryland. His research interests include information assurance, risk management, and election technologies.

Navya Gautam, B.S. is a current graduate student at the Georgia Institute of Technology, earning a master's of science in computer science with a concentration in machine learning. She previously graduated summa cum laude from the University of Maryland, College Park with a double degree in computer science and mathematics. Her research and career interests include natural language processing, computational linguistics, data science, and machine learning.

Appendix 1. Vulnerabilities and Documented Threats in Academic Literature.

Authors(s)	Threat	Threat Details	Summary / Implications
Kerschbaum (2022)	Cyber	Manipulation by 3rd parties; Errors (user error, configuration error, software error); Effect of accessibility and ease of use on voter turnout - Quantum computers pose threats to the security of cryptographic election voting systems	For a secure election system, it is important to consider the security aspects introduced by the user, configuration and software; assess the distributed nature of the electronic voting system, including the need for reliable communication channels; employ cryptography to create a secure core within a well-designed, multi-layered architecture that is difficult to penetrate
	Physical	Threat of availability of communication channels	
	Insider	Manipulation by voter to cast multiple or invalid votes	
Abilov, et al. (2021)	Cyber	Social media platforms are used to disseminate fraud claims	Voter fraud allegations undermine the integrity of the election and threaten the stability of democracies
	Insider	Dissemination of misinformation before, during, and after election impacts voters and their acceptance of results	
Fick (2021)	Physical	Ballots stolen from drop boxes; Drop boxes set on fire; Lost ballots; Ballot harvesting	Suggest improvements to vote by mail process to help preserve the integrity of elections and maintain voter trust
	Insider	Poor processes and efforts to calculate results and ensure all ballots are counted; Judges and unelected regulators alter or overlook established state procedures; Changes made last minute to election laws and procedures concerning voting by mail	
Herron and Smith (2021)	Physical	Postal service delays could result in ballots arriving late and not being counted	Mail voting has more steps in process, leading to more vulnerabilities and room for error
Hughes (2021)	Cyber	Threats by foreign adversaries and political extremists aiming to manipulate elections	Use systems thinking to understand risks of processes and red teaming to test the system
Jafar, et al. (2021)	Cyber	Large-scale manipulation of votes	Primary concerns for electronic voting systems include privacy protection and transaction speed; Ensuring secure remote participation is crucial
	Physical	Eligibility / identification of legitimate users; Reusability; Privacy / anonymity of votes (blind signatures / encryptions); Soundness and completeness	
Li, et al. (2021)	Cyber	Three attack scenarios: targeted attack (attacker targets specific voting components to launch attack), random attack (attacker randomly selects targets to launch attacks), and dynamic attack (each attack randomly targets specific number of voting components)	Present algorithms to evaluate the reliability of a voting system based on the handling of cyber threats and attacks (categorized into three categories: targeted, random, and dynamic)
Neisler (2020)	Insider	Election officials lack training in accurately counting mail-in votes; Improved processes needed to count votes and maintain the integrity of counting	While the risk of voter fraud may be elevated by mail voting, there is not concrete evidence of increased voter fraud from vote by mail

Authors(s)	Threat	Threat Details	Summary / Implications
Kasongo (2021)	Cyber	Denial of service attack prevents computer system from functioning correctly; Malware attacks; Use of aging and obsolete voting technology; Internet connectivity increases vulnerability of voting infrastructure	Communication and education play a key factor in securing voting systems; Misinformation is key and pressing concern; Current voting systems have technical vulnerabilities that make them susceptible to manipulation; Multiple threats exist to voting systems, highlighting the need to focus on human factors and train election administrators
	Physical	Phishing; Impersonation; Tailgating; Dumpster diving; Shoulder surfing; Social engineering; Natural disasters or severe weather events	
	Insider	Any election officials "intentional misuse" of a system; Some election offices have few dedicated staff and little access to the latest information technology training or tools	
Lott (2021)	Insider	Fraud and intimidation to secure victories; Proxy voting; Unsecured ballots pose risk for creating fraudulent ballots or destroying votes; Absentee voter fraud such as buying and selling votes is difficult to detect when absentee voting restrictions are more lenient	Vote fraud concerns can influence election outcomes and discourage voter participation
Park, et al. (2021)	Cyber	Internet voting increases number of possible attacks including ones that are larger scale, harder to detect, and easier to execute compared to paper ballot voting systems	Lack of conclusive evidence that online voting options will actually improve voter turnout
Persily and Stewart (2021)	Physical	Increase rejection rates for vote by mail ballot because of poor ballot casting	Enhanced auditing practices to ensure accurate results; Establish more uniform and standardized procedures for ballot drop offs and ballot counting
	Insider	Poll worker shortages create need to quickly hire and train new workers; New workers might not have proper training and experience	
Agarwal, et al. (n.d.)	Cyber	Voting databases and related information continue to be vulnerable to attacks or interference by foreign powers; U.S. lacks the capacity to securely conduct virtual election	COVID-19 raised additional election security concerns due to reduced in-person voting; Disinformation and manipulation are equally important to mitigate to prevent cyber threats
	Physical	Issues with mail voting revolve around the transition to digital mail, the spread of disinformation, and lack of accountability	
	Insider	Influential actors attempt to manipulate voters to create narratives that support their agenda; Widespread disinformation results in voter manipulation	
Baringer, et al. (2020)	Physical	Postal delays cause late ballots to election office that cannot be counted in time	Age, disability status, geography, race/ethnicity, and military dependents may have an impact on whether or not ballot is thrown out or not counted
	Insider	Bias of election official reviewing ballot when deciding to count or throw out	

Authors(s)	Threat	Threat Details	Summary / Implications
Barouh (2020)	Cyber	Electronic equipment more vulnerable than paper; Interference from other countries hacking into emails and systems	Recommend switching to a universal mail ballot to enhance election security; Mail voting increases turnout and improves access
	Physical	In-person voting has more vulnerabilities and more opportunities to attack; Polling places are negatively affected by malfunctions in voting machines; Machines are unreliable and can disrupt the electoral process	
	Insider	Pre-election management choices can allow those opposed to a representative government to manipulate the voting population, instead of advocating for widely supported positions; Day of election management faces threats to voting from suppressive laws, long wait times, policies creating further delays, and inconsistent staffing due to untrained, temporary poll workers	
Benkler, et al. (2020)	Cyber	Mass media and social media disinformation campaign disseminating false claims about voter fraud	To prevent spread of misinformation, require harsher policing for professional media, not just fact checking by platforms like Facebook
	Insider	Mass media spreading misinformation by relying on elite institutions as presumed sources of truth, using sensationalist headlines to attract attention, and presenting issues with a false sense of balance to appear neutral	
Blake (2020)	Cyber	Using hacking to release private resources or documents; Using social media to spread misinformation to influence public sentiment and/or election outcome; Employing technology to undermine the public's trust in the election system	Do not allow foreign companies to partake in election contract; Ensure cybersecurity is the most important consideration with regards to contracts
	Insider	Foreign sourced election equipment can be hacked; Foreign adversary would have access to the equipment	
Hopkins, et al. (2021)	Physical	Mail votes take longer to be counted and must be delivered on time to count	No significant differences found to indicate that voter education about the process before the election increased turnout
	Insider	Mail votes have higher rates of clerical errors when manually counting	
Lee (2020)	Cyber	Online voting is vulnerable	Operational risks with paper ballots are lower than internet cyber threats
	Physical	Technology failures due to the premature deployment of systems	
de Jong, et al. (2008)	Cyber	Simple to write and conceal malicious code in a program but difficult to detect and fix it; Possible to influence election results by making minor adjustments in numerous voting machines	Voting machine (with or without paper trail) regarded as more user-friendly than the paper ballot while helping to increase voter confidence

Authors(s)	Threat	Threat Details	Summary / Implications
Johnson (2020)	Cyber	Ballot marking devices (BMDs) may have limitations with effective voter verification and postelection auditing procedures	Examination of regulatory and reporting requirements proposed in a House Administration Committee hearing
	Physical	Concerns surround the software and hardware supply chains of companies producing election devices; Major manufacturers rely on foreign equipment, opening the door to potential comprise or sabotage by malicious actors	
Kortum, et al. (2020)	Insider	Pandemic created voting hazard to health; Consider using voting drive through	Human factors of safe election for poll workers and voters
Lee (2020)	Cyber	Online voting is vulnerable	Operational risks with paper ballots are lower than internet cyber threats
	Physical	Technology failures due to the premature deployment of systems	
Pennycook and Rand (2020)	Insider	Widespread false allegations of election fraud undermines trust in the results of election	Voters can believe in systemic election fraud
Schmidt and Albert (2020)	Physical	Voter registration requires close contact with poll workers, suggest election process changes to avoid contact; Process improvements to decrease wait times and crowds; Poll booths need proper sanitation, voters may be afraid to use them otherwise; Alternative polling places increase complexity and risk	Improve processes for use during a pandemic; Consider potential additional social distancing requirements.
	Insider	Poll worker shortages; Less training for poll workers	
Torres-Lugo, et al. (2022)	Cyber	Vulnerability in social media platforms particularly with regards to creating hyper-partisan spaces online that rapidly propagate misinformation	Follow trains suggest other accounts for users to follow and are often abused to help spread misinformation and create dangerous echo chambers, further and more rapidly propagating misinformation
	Insider	Features of social media can encourage inappropriate spread of misinformation that undermines integrity	
Yoder, et al. (2020)	Physical	Logistics issues sending and receiving ballots absentee ballots	Democrats more likely vote to vote by mail while Republicans more likely vote in person, but no evidence method of choice impacts election results
Blaze, et al. (2019)	Cyber	Advanced Persistent Threat continues to be detected; Direct Recording Electronic (DRE) machines are not suitable for auditable elections	There is an immediate need for paper ballots and risk-limiting audits; Infrastructure and supply chain challenges continue to present significant security risks
Feldman, et al. (2007)	Cyber	Attacker can modify the DRE machines by changing the code on a memory card, which could lead to fraudelent vote counts that may be indectiable	The vulnerabilities can be quiet as well, happening many months before Election Day and being passive, with the alteration of logs to make them virtually undetectable
Epstein (2007)	Cyber	Using a mix of various voting systems; Injection of harmful code; Unintentional programming mistakes	Deemphasize DRE machines for optical scan systems

Authors(s)	Threat	Threat Details	Summary / Implications
Manpearl (2018)	Cyber	Malicious software inserted into voter registration database by attackers; Attackers selectively disenfranchising certain voters; Electronic overseas voting could be susceptible to attack; Attackers could exploit online connection to infiltrate and compromise the files; State and local computers that compile the vote totals from precincts at risk	Support the classification of U.S. elections systems as critical infrastructure; Advocate for states and localities to implement reforms; Urge Congress to pass legislation to strengthen the security and resilience of election systems nationwide; Highlight the vulnerability of voter registration systems due to their online maintenance
	Physical	Removing voters from the registration database to favor one candidate over another	
	Insider	Large volume of provisional ballot requests or long lines potentially discourage people from voting; Nation-state adversary recruits workers with direct access to the voting machines or election management computers	
Blaze, et al. (2017)	Cyber	Universal default password found online; Live voter information not properly deleted from the system; Sensitive data exposed	Every piece of equipment was compromised in some way by the conclusion of the DEFCON conference, an exercise in ethical hacking; Systems contained internal parts manufactured aboard, posing a supply chain vulnerability
	Physical	Attackers take advantage of vulnerabilities in supply chain security to insert malware into machines before they are even delivered	
Halderman, et al. (2008)	Cyber	Creating a memory card that appears to be normal but contains malicious information can compromise software; Memory card can be infected by a machine and then inserted into other machines, leading to further compromises; A single compromised memory card has the potential to jeopardize the entire Election Management System (EMS) and the elections in that county; If one EMS is compromised, other EMS within the same precinct could also be at risk	Enhance security by containing viral spread, ensuring accurate vote tabulation, and detecting compromised individual devices
Fidler (2017)	Cyber	Adversaries could hack into voting machines, voter registration databases, or election results systems to alter vote count, affecting election outcomes; Use of digital platforms to spread misinformation and disinformation	Increased vulnerabilities in election systems by foreign actors; At the federal level, the classification of election systems as critical infrastructure should be maintained, as it guarantees these systems are given priority for cybersecurity assistance from the Department of Homeland Security; Efforts to enhance cybersecurity at the state level in the U.S. have been inconsistent, and before 2016, analysis of policies seldom prioritized elections-related concerns
	Physical	Tampering with voting machines and electronic records	
	Insider	U.S. government agencies lacking enough commissioners to operate effectively or address vulnerabilities	

Authors(s)	Threat	Threat Details	Summary / Implications
Cui, et al. (2013)	Cyber	Updated firmware can be exploited by attackers, allowing them to inject modifications into embedded devices; General firmware modification attacks occur when attackers alter a device's firmware due to design flaws in the embedded software; End users responsible for mitigating the vulnerabilities associated with updated firmware; Firmware update signing is not a complete solution; Malware targeting printers can be executed using standard Printer Job Language (PJL) commands and may be hidden within apparently harmless document formats like PostScript	Vulnerabilities in printer firmware can be exploited; Methods used to exploit printers can generally be applied to other voting equipment and ballot printers
Epstein (2012)	Cyber	Enabling online voter address changes heightens risks; For, Internet Voting, faudsters can install malware on the voter's computer to alter votes, attack vote servers, or conduct phishing attack	While computers can indeed cause security and reliability failures, they are not the sole source of such issues
	Insider	Greatest risks are threats from insider election officials	
Yasinsac (2010)	Cyber	Increase in different technologies for election equipment; Increased use of outside contractors to help with equipment	Insiders pose strong threat to election integrity
	Insider	Election insiders include poll workers, local election officials, judges, policy makers and legislators	
Aviv, et al. (2008)	Cyber	DRE and optical scan voting systems are susceptible to attacks that may modify or falsify precinct results, install corrupt firmware, and erase audit records; Poor access control such as unauthorized screen calibration and configuration	Machines contain exploitable vulnerabilities in almost every aspect of the election security and software system
Raunak, et al. (2006)	Insider	Errors in the Statement of Results can occur due to an honest mistake or intentional fraudulent behavior	Consider agent behaviors to iteratively improve the process to make it robust against more complicated fraudulent behavior
Scala, et al. (2024)	Insider	Poll workers have little in-person training; They bring their personal cybersecurity behaviors and cyber hygiene to the polling place, which may introduce risk with poor behaviors	Cyber hygiene may not be familiar to poll workers; Training can help to mitigate poor behaviors
Shanton and Underhill (2014)	Insider	Local election offices have to enforce voter ID laws and may not be equipped to enforce; Enforcement of voter ID laws impacts who is allowed to vote or not allowed to vote in election	State pays most of cost for voter ID checks, but local election offices have to follow through with enforcement

Authors(s)	**Threat**	**Threat Details**	**Summary / Implications**
Brunner (2007)	Cyber	Insufficient robust encryption for storing and transmitting the data	Must adhere to recommended practices and implement foundational security measures; Absence of encryption for election data makes information susceptible to attacks during both storage and transmission
	Physical	Absence of established best practices	
	Insider	Lack of implementation of efficient security policies or procedures	
Scala, et al. (2020)	Cyber	Use of cell phones at polling places increases risks of meddling or disclosing voter choice	Poll workers can be trained to identify and respond to threat real time if they may emerge at a polling place
Scala, et al. (2022)	Cyber	Ballot scanner hacked	Expanded mail voting due to COVID-19 did not increase risk; Mail voting increases voter access and disincentivizes adversarial meddling in elections
	Physical	Destroy drop box; Defeat signature check; Vote denied or altered; Alter ballot and return to storage; Manipulate return envelope	
	Insider	Acquire access to ballots through relationships with postal workers; Error in instructions; Expired voterID	