

August 30, 2024 in [Election Security](#)

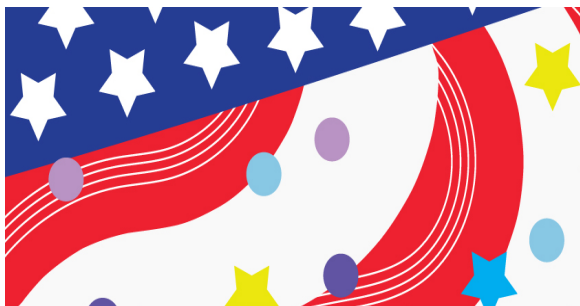
From Misinformation to Trust: Safeguarding the 2024 U.S. Presidential Election

By Josh Dehlinger, Natalie M. Scala

SHARE: [f](#) [in](#) [X](#) [✉](#)

PRINT ARTICLE: [🖨](#)

<https://doi.org/10.1287/orms.2024.03.03>



In what has already been a roller coaster of a U.S. presidential election cycle, many Americans and world leaders are fretting about the unpredictability leading up to Election Day, the election results, public and political acceptance of the election outcome and the transition to the next administration. Outside of the political theater among the presidential nominees, several reoccurring election security themes in mainstream and social media have, again, reemerged (albeit in 2024 incarnations) as perceived public concerns threatening the integrity of the election process and results. In particular, election misinformation/disinformation pervading social media, security of election and voting equipment and processes, and the integrity of the election workers to administer a fair election in which any eligible voter's valid votes are cast and counted as the voter intended. Thus, riding into the November 2024 U.S. presidential election, it is critical to understand the context and veracity of these echoing public concerns to separate polarized hearsay from legitimate concerns.

Election Misinformation and Disinformation Dissemination


Election misinformation/disinformation dissemination has significantly increased and impacted elections, both in the United States and abroad, with the advent and prevalent use of social media weaponizing false

election information to influence its results or, otherwise, sow distrust and/or chaos in the process (e.g., dissemination of lies about election workers roles [1], voting machines [2] and mail voting [3]). Such misinformation is more than simply *fake news* but endangers election officials' jobs with 64% of surveyed election officials indicating that misinformation has made their roles more dangerous [4]. The emergence and increasingly open, public use of generative pretrained transformer (GPT) or other artificial intelligence (AI) models has enabled near-realistic, believable audio and/or video *deepfake* content to further mislead voters [5]. For example, following Vice President Kamala Harris' advancement to the presumed Democratic presidential nominee after President Joe Biden withdrew in late July 2024, the owner of X (formerly Twitter), Elon Musk, shared a video to his 192+ million followers of Harris speaking, using audio generated with AI voice-cloning technology, disparagingly of President Biden and her own ability to serve as president [6]. Although these deepfakes may be dismissed as satire and can be easily fact-checked and debunked as fake, research has shown evidence that even debunked negative political misinformation can continue to influence voters' attitudes [7].

The terms misinformation and disinformation are commonly used interchangeably in media and literature but are indeed different. *Misinformation* is the spread of false or misleading information, such as propaganda, fabrication of the truth or satire. *Disinformation*, however, is the purposeful spread of a false or misleading narrative oftentimes for malicious reasons [8]. Misinformation/disinformation spread is not new to elections and has commonly been used within politics to disenfranchise voters to achieve a desired outcome [9]. An ongoing example of this is the continued insistence that the allowance and broadening use of mail voting will allow for a "massive opportunity for voter fraud" [10] and should be limited in its use, thus, deceptively justifying additional, restrictive voter suppression laws [4]. More broadly, election misinformation/disinformation can include fake statements and/or policies attributed to political candidates, incomplete instructions on how to complete a mail ballot, incorrect voting locations, malicious information about voting machines and election officials, and more.

Going into the 2024 U.S. presidential election, it is a near certainty that misinformation and disinformation, propelled by social media and the production of deepfakes, will not go away and will have some bearing on the national media news cycles and candidate and surrogate messaging, as well as potentially degrade voters' – and the general public's – understanding of the election process and trust in the security, integrity and results of U.S. elections. There have been recent social media transparency/features that provide context to potential misleading content (e.g., X's Community Notes' increased use in 2023 [11]), which could curb the impact and/or spread of misinformation/disinformation. However, it has been shown that social media users still share content that is known to be false [12], which can influence voters' attitudes [7] and thus exacerbate the problem. Until social media platforms or governments take action to combat misinformation/disinformation and promote social media transparency, broader voter education and general technology education could allow social media users and voters strong discrimination between information and misinformation/disinformation and a stronger understanding of how to discern trusted information sources.

The Empowering Secure Elections Research Lab at Towson University [13] has studied how misinformation/disinformation dissemination via social media during the 2020 U.S. presidential election may have impacted voters' perceptions of threats regarding in-person and mail-based voting [14]. We found that there is a general inconsistency in voter perceptions and belief in misinformation/disinformation statements, primarily driven by partisanship, and, as previously mentioned, a person's disbelief in a misinformation/disinformation statement does not necessarily prevent them from sharing it with their social group or reposting it themselves. Although these findings align with existing literature, it may

highlight the disconnect many people have between identifying false information and understanding the consequences sharing it may have on their own or others' beliefs – even when known to be false. 

Election Equipment and Processes Security

The security and integrity of voting machines and election processes has increasingly become a national security concern to the continuance of free and fair elections enabling our democracy – through both real, verified incidents and baseless misinformation/disinformation claims. Most recently, real election security and integrity concerns stem from the Senate Intelligence Committee conclusion that election systems in all 50 states were targeted by the Russian Federation in 2016 [15], and Special Counsel Robert Mueller's testimony before Congress that foreign interference in U.S. elections was ongoing and would continue to occur throughout the 2020 elections [16]. However, former President Donald Trump's continued to voice unfounded claims in 2020 that mail voting ballots can be "manipulated" and the mail voting process, which was significantly expanded in 2020 due to the COVID-19 pandemic, would be "a fraud like you've never seen" [17]. Further, Sidney Powell, an attorney representing former President Trump, baselessly claimed that some voting machines were flipping votes, and that voting software was developed in Venezuela under the guidance of former Venezuelan President Hugo Chavez [2]. These later statements were debunked as false; however, the mix of verified, actual security threats and baseless claimed threats creates confusion among the electorate as to the *actual* security and integrity of voting machines and election processes and allows for state and local legislation to further restrict voter access using false justifications. For example, in July 2024, the Wisconsin Supreme Court overturned its own 2022 ruling that banned ballot drop boxes, except for those in local election clerks' offices and now allows election officials to place ballot drop boxes around the local communities [18].

The U.S. Department of Homeland Security (DHS) defines 16 U.S. critical infrastructure sectors that encompass assets, systems and networks that are so essential that their destruction or incapacitation would significantly impact national security, economic security, and/or public health and safety [19]. In 2017, the DHS added election infrastructure as critical infrastructure within the Government Facilities sector in recognition that election and voting processes and equipment security and integrity are of vital national interest. As such, it is crucial to understand any potential threat to voting equipment and election processes to ensure the nation's overall resilience and preparedness to identify and mitigate threats without disenfranchising voters, thus helping to safeguard the infrastructure that underpins our democracy.

The Empowering Secure Elections Research Lab [13] has examined, or is in the process of examining, the threats to voting machines and election processes. Unlike other researchers in election security that may only focus on the cybersecurity threats, our work was the first to propose a systemic *cyber, physical* and *insider* approach to mitigate risks to elections at both the state and local levels. *Cyber threats* are risks to a system that take place digitally (e.g., hacking a voting machine); *physical threats* include those risks that occur when election equipment is tampered with (e.g., broken tamper tape on a ballot bag); and *insider threats* originate from human interactions with the election process through honest mistakes (e.g., walking away from a pollbook computer without locking it) or with malicious intent (e.g., intentionally sabotaging a ballot) [20]. After identifying these threats, our analysis utilizes an attack tree as an assessment framework to identify the relative likelihood of each attack scenario to understand how voting systems and processes vulnerabilities develop and how specific security measures can aid in mitigating each scenario.

Although our ongoing work is currently funded to examine the precinct count optical scanners, used to count approximately 70% of the in-person ballots cast in the U.S., we have previously completed an

assessment of the mail voting process and identified more than 100 potential threats, along with security measures that could mitigate them [21]. Specifically, our analysis found that most threat scenarios for mail voting are related to insiders and that mail voting disincentivizes adversarial attacks because of its distributed nature and increases voter access. Although these findings align with the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) comment that the 2020 election was the "most secure in American history" despite significant utilization of mail voting [22], it highlights the need to scientifically analyze the threat scenarios of voting machines and election processes *and* publicly communicate these efforts by the government, academia and other election security professionals to diffuse broader misinformation amongst the electorate.

Poll Worker Integrity

Election officials (Board of Elections full-time employees) and poll workers (temporary election workers that help run elections) are the first line of defense to mitigate an emerging threat, if recognized. During a presidential election year, it takes nearly 1 million poll workers to manage voting machines and facilitate the election process at more than 100,000 polling places [23]. With U.S. elections primarily being a one-day event that can't be redone or delayed, election officials and, more importantly, poll workers need to be able to identify and mitigate any threat that may arise on Election Day to ensure the security and integrity of the votes cast. Poll workers are our local friends, parents, neighbors, etc., who volunteer, for minimal pay, to perform this public service. Unfortunately, because of the misinformation/disinformation spread during the 2020 U.S. presidential election and threats to their safety, many states are experiencing a shortage of volunteer poll workers to assist in the 2024 U.S. presidential election [22].

Election officials and poll workers are *trusted insiders* to the election process. CISA defines trusted insiders as someone "who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems." In this sense, poll workers are unique in that they are one of the few roles that help facilitate critical national infrastructure as *temporary* trusted insiders. Despite this, many poll workers are not specifically trained to identify and mitigate the cyber, physical and insider threats that may arise during an election [24].

The Empowering Secure Elections Research Lab [13] has partnered with several county in Maryland to develop and pilot online training modules for poll workers that specifically focus on being able to identify the cyber, physical and insider threats to specific election processes [25]. These training modules were validated to ensure that poll workers' understanding of threats increases. Although training is important, our work has also recognized that a poll worker's *cyber hygiene* (i.e., their personal cybersecurity practices to protect their own computer systems) can impact cybersecurity risk and may impact the effectiveness of cybersecurity training for poll workers. Thus, we have also examined the relationship between developed poll worker training to understand and mitigate the potential cyber, physical and insider threats that may emerge during an election with their individual cybersecurity practices. Specifically, we measured poll workers' cyber hygiene using the Security Behaviors and Intentions Scale (SeBIS) [26] and statistically examined this measure to their performance on three poll worker election security training modules and assessments to find a positive relationship between a poll worker's cyber hygiene and knowledge of the cyber, physical and insider threats related to election equipment and processes [27]. This work may allow for improved election security and integrity with our partnered s, but it also highlights the need for increased focus on improving the training and preparedness of poll workers across the country to handle Election Day threats if they arise, as well as the need to better examine and understand trusted insider threats to all critical systems.

Going Forward



The period leading up to the November 2024 U.S. presidential election is bound to have more twists and turns in the roller coaster of U.S. politics, likely shaped by misinformation/disinformation questioning the security and integrity of voting equipment, election processes and the dedicated election and poll workers. Although threats to our election systems and processes exist, it is imperative that the electorate is able to discern between accurate information and misinformation/disinformation and new approaches and/or training developed to allow people to better identify deepfakes. To understand actual threats that our adaptive adversaries may try to exploit, we need continuous efforts to analyze our election systems and processes to identify the cyber, physical and insider threats and possible mitigations. Finally, the local poll workers that act as the first line of defense to this entire process warrants the training to be able to thwart any threat that may arise. No matter one's political beliefs or affiliations, OR/MS analysts can play an important role in the effort to secure future elections by leveraging the discipline's unique analytical methods to contribute to solving these issues.

References

1. Julie Carr Smyth, 2023, "Election workers who face frequent harassment see accountability in the latest Georgia charges," August 16, AP News, <https://apnews.com/article/election-workers-threats-trump-georgia-indictment-5b056e2c97bfd7146b3bd19cf7f9f588>.
2. Ali Swenson, 2020, "AP FACT CHECK: Trump legal team's batch of false vote claims," November 19, AP News, <https://apnews.com/article/fact-check-trump-legal-team-false-claims-5abd64917ef8be9e9e2078180973e8b3>.
3. Nicholas Riccardi, 2020, "Here's the reality behind Trump's claims about mail voting," September 30, AP News, <https://apnews.com/article/virus-outbreak-joe-biden-election-2020-donald-trump-elections-3e8170c3348ce3719d4bc7182146b582>.
4. <https://www.brennancenter.org/election-misinformation>
5. Sally Adey, 2024, "What are deepfakes and how are they created?," *IEEE Spectrum*, March 8, <https://spectrum.ieee.org/what-is-deepfake>.
6. Ali Swenson, 2024, "A parody ad shared by Elon Musk clones Kamala Harris' voice, raising concerns about AI in politics," AP News, July 29, <https://apnews.com/article/parody-ad-ai-harris-musk-x-misleading-3a5df582f911a808d34f68b766aa3b8e>.
7. Thorson, E., 2015, "Belief Echoes: The Persistent Effects of Corrected Misinformation," *Political Communication*, Vol. 33, No. 3, pp. 460-480, <https://doi.org/10.1080/10584609.2015.1102187>.
8. Jackie Mansky, 2018, "The age-old problem of 'fake news,'" *Smithsonian Magazine*, May 7, <https://www.smithsonianmag.com/history/age-old-problem-fake-news-180968945/>.
9. Keyssar, A., 2009, "The right to vote: The contested history of democracy in the United States," New York: Basic Books.
10. Vice President Mike Pence, 2020 Vice Presidential Debate, October 7, 2020.
11. <https://help.x.com/en/using-x/community-notes>
12. Pennycook, G., & Rand, D. G., 2020, "Who falls for fake news? The roles of bullshit receptivity, overclaiming, familiarity, and analytic thinking," *Journal of Personality*, Vol. 88, No. 2, pp. 185-200, <https://doi.org/10.1111/jopy.12476>.
13. <https://www.linkedin.com/company/ese-research-lab/>
14. Riley, J., Gregorio, V., Scala, N. M., & Dehlinger, J., 2023, "Voting perceptions and the impact of misinformation," Presented at NATO Operations Research and Analysis (OR&A) Conference, October, DOI: 10.14339/STO-MP-SAS-OCS-ORA-2023.

15. <https://www.nytimes.com/2019/07/25/us/politics/russian-hacking-elections.html>
16. Mueller III, R. S., 2019, Report on the Investigation into Russian Interference in the 2016 Presidential Election, Volumes I and II.
17. Nicholas Riccardi, 2020, "Here's the reality behind Trump's claims about mail voting," AP News, September 30, <https://apnews.com/article/virus-outbreak-joe-biden-election-2020-donald-trump-elections-3e8170c3348ce3719d4bc7182146b582>.
18. Todd Richmond, 2024, "Wisconsin Supreme Court changes course, will allow expanded use of ballot drop boxes this fall," AP News, July 5, <https://apnews.com/article/wisconsin-supreme-court-ballot-drop-boxes-2024-9d3973ea65b78436df478e7d8ae28cce>.
19. <https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors>
20. Locraft, H., Gajendiran, P., Price, M., Scala, N. M., & Goethals, P. L., 2019, "Sources of risk in elections security," *IIE Annual Conference Proceedings*, Institute of Industrial and Systems Engineers (IISE), pp. 1572-1577.
21. 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*, Vol. 42, pp. 2327-2343, <https://doi.org/10.1111/risa.13876>.
22. <https://www.cisa.gov/news/2020/11/12/joint-statement-elections-infrastructure-government-coordinating-council-election>
23. United States Election Assistance Commission, 2017, "EAVS deep dive: Poll workers and polling places," November, https://www.eac.gov/sites/default/files/document_library/files/EAVSDeepDive_pollworkers_pollingplaces_nov17.pdf.
24. Christina A. Cassidy, 2024, "Local election workers fear threats to their safety as November nears. One group is trying to help," AP News, April 22, <https://apnews.com/article/election-workers-threats-2024-law-enforcement-d2702ae1e1e57c766c3df36f1a7ff763>.
25. Black, L., 2023, "Preparing Poll Workers to Secure U.S. Elections," *Proceedings of the International Annual Conference of the American Society for Engineering Management*, American Society for Engineering Management (ASEM), pp. 1-11.
26. Egelman, S., Harbach, M., & Peer, E., 2016, "Behavior ever follows intention? A validation of the Security Behavior Intentions Scale (SeBIS)," *Proceedings of the 2016 ACM Conference on Human Factors in Computing Systems*, Association for Computing Machinery, pp. 5257-5261.
27. Kassel A., Bloomquist, I., Scala, N. M., & Dehlinger, J., 2024, "Understanding the Impact of Poll Worker Cybersecurity Behaviors on U.S. Election Integrity," *Proceedings of the 2024 International Industrial and Systems Engineering (IISE) Annual Conference and Expo*, May 18-21, Montreal, QC, Canada.



Josh Dehlinger



Josh Dehlinger, Ph.D., is a professor in the Department of Computer and Information Sciences in the Fisher College of Science and Mathematics at Towson University and codirector of the Empowering Secure Elections Research Lab. His research expertise lies, broadly, in software safety and reliability, election security and software engineering. He is a member of INFORMS.



Natalie M. Scala

Natalie M. Scala, Ph.D., is a professor at Towson University, a fellow of the university's Center for Interdisciplinary and Innovative Cybersecurity and codirector of the Empowering Secure Elections Research Lab. She also holds a faculty affiliation with the University of Maryland's Applied Research Lab for Intelligence and Security. She is an active member of INFORMS and has served as president of the Institute's Military and Security Society.

SHARE: [f](#) [in](#) [X](#) [✉](#)

Keywords:

Election Security; misinformation; poll worker safety; election equipment; disinformation; deepfakes; national security; U.S. presidential election; OR/MS

Recommended

Lessons Unlearned: Misguided Efforts in the Guise of Election Security

Josh Dehlinger , Natalie M. Scala

ORMS TODAY

PUBLISHED ONLINE: 7 JUNE 2021

Modeling a Presidential Prediction Market

M. Keith Chen, Jonathan E. Ingersoll, Jr., Edward H. Kaplan

10 JUNE 2008 | MANAGEMENT SCIENCE, VOL. 54, NO. 8

Keys to the White House: Predicting the 2020 U.S. Presidential Election

Doug Samuelson



ORMS TODAY

PUBLISHED ONLINE: 12 OCTOBER 2020

Quantitative Historian's Perspective: Predicting the presidential election

Doug Samuelson

ANALYTICS

PUBLISHED ONLINE: 1 OCTOBER 2012

Election analytics

Wenda Zhang , Jason J. Sauppe , Sheldon H. Jacobson

ORMS TODAY

PUBLISHED ONLINE: 3 OCTOBER 2016

Sign Up for INFORMS Publications Updates and News

Sign Up

SUBSCRIBE

CONTACT

ADVERTISE



Institute for Operations Research and the Management Sciences

5521 Research Park Drive, Suite 200
Catonsville, MD 21228 USA

phone 1 443-757-3500

phone 2 800-4INFORMS (800-446-3676)

fax 443-757-3515

email informs@informs.org

Get the Latest Updates

Submit



[Discover INFORMS](#)

[Explore OR & Analytics](#)

[Get Involved](#)

[Impact](#)

[Join Us](#)

[Recognizing Excellence](#)

[Professional Development](#)

[Resource Center](#)

[Meetings & Conferences](#)

[Publications](#)

[About INFORMS](#)

[Communities](#)

[PubsOnLine](#)

[2024 INFORMS/ALIO/ASOCIO International Conference](#)

[Certified Analytics Professional](#)

[Career Center](#)

[INFORMS Connect](#)

Copyright 2024 INFORMS. All Rights Reserved

[INFORMS Code of Conduct](#) | [Terms of Use](#) | [Privacy](#) | [Contact INFORMS](#) | [Sitemap](#)

Follow INFORMS on:



Facebook



LinkedIn