Threats to Democracy: Voter Perceptions of Election Cyber Incidents

Danielle Caplinger

Old Dominion University

CYSE 495: Cyber Election Security

Professor Gladden

August 9, 2025

Introduction

In the months and weeks leading up to an election, news of related cyber incidents are almost guaranteed to dominate headlines and garner a considerable amount of attention. However, rather than informing a voter on safety best-practices for election day, they often do the exact opposite: dissuade them from voting or questioning the integrity of an election altogether. These actions do not just affect voter turnout, but could pose dangerous consequences for the foundation of US democracy as a whole. Additionally, they offer a new attack vector for adversaries to exploit; even if an attack is not completed successfully, the news coverage of one could damage an election just as severely in a previously unforeseen nontraditional way.

Research Overview

To best address this new issue, this research focuses on voter perception of past cyber incidents and voter responses to such perceptions. This includes how voters think about election-related cyber incidents, if it affects their likelihood to vote, their method of voting, and how confident they are in election results and system as a whole. By analyzing this data, next steps can be made towards reframing how cyber incidents are portrayed to voters to keep them, and the US democratic system, safe from potential threat actors.

To provide necessary information, it is important to first define what is meant by a “cyber incident” in the context of election security events. For the purposes of this research, a cyber incident simply refers to a malicious or unexpected event that compromises an election-related system with the goal of disrupting any part of a standard election process. This can include data breaches, unauthorized access or changes to systems, hacking techniques, mis- and disinformation campaigns, or physical attacks on digital election systems. Recent events to highlight that fall into this category include failed and successful compromises of US voter registration databases in 2024 (FBI and CISA, 2024), the Russian hacking of DNC emails in 2016, and a ransomware attack against the DC Board of Elections in 2023 that exposed PII for DC voters (Upguard, 2024).

Methodology

To best investigate how voter perception is influenced by cyber incidents and subsequent public news releases, this research used a literature review methodology. Specifically, a review was done on articles documenting election-related cyber incidents, public service announcements published by federal agencies to communicate information regarding cyber threats and the public's potential reaction, and academic research on voter behaviors in response to such news. These sources were analyzed to find overlapping themes, concerns, and patterns regarding how voters are responding to election cyber threat communications.

Resources and Results

From July of 2016 to October of 2024, Upguard identified over 20 articles that reference damaging cyber incidents in relation to election systems or outcomes. However, many of these articles are not technical exploits but are instead instances of disinformation, miscategorization of PII versus publicly accessible data, and social misgivings about the election systems as a whole. Through this analysis, the authors are able to identify that the common pattern is not a threat to election infrastructure that the average voter is concerned about; instead, it is the lack of security for voter privacy. This, they argue, is then used as "fuel for disinformation campaigns" and the subsequent drop in voter turnout (Upguard, 2024). This is becoming a new attack vector for adversaries spreading doubt among American voters in the election system as a whole, and the integrity of such results. According to researchers at Georgia Tech, "Even a single failed intrusion, magnified by sensational headlines and political echo chambers, is enough to shake public trust" ("Cyberattacks", 2025). CISA and the FBI have been seeing this new tactic come in full force, to the extent that they issued a Public Service Announcement in September of 2024, warning citizens of false claims spread online about hacked voter information. They also stress that, contrary to unofficial communications, much of this information is already publicly available and is maliciously exaggerated to promote distrust (FBI and CISA, 2024).

Conclusion

Elections are the foundation of American democracy, and as such, are denoted as critical infrastructure from both a physical and social point of view. However, oftentimes the technical exploits are highlighted in a way that does not simply inform voters, but scares them. Headlines often focus on the potential dangers of an attack, rather than the facts of what actually happened or the mitigation that made it obsolete. Voters are more prone to falling for such perspectives rather than researching it themselves and learning the security in place to protect them. They are also more sensitive to voter privacy issues that decrease their likelihood of registering and participating in the voting process. With every headline, whether exaggerated or simply false, citizens fall further away from trusting election infrastructure, the process itself, or the integrity of the results. In doing so, even a failed attack, coupled with this "lack of public understanding…can undermine confidence" in these systems while increasing the risk to them and our democracy as a whole ("Enhancing Election Security", 2024, p. 4). In order to combat these increasingly fruitful threats, public communications about such incidents, whether successful or failed, must be made in a way that allows the average citizen to understand the situation wholly, even from a nontechnical perspective. The EAC has already put out a guide on how to carry out such procedures, but this needs to be taken a step further. Voters themselves must be made aware of the mis- and disinformation campaigns being carried out by adversaries, both foreign and domestic, to achieve public distrust in their voting systems. Today, the attack may be against the American voter, but the goal is not to disrupt them or even a singular election. It is instead for a much greater end, and a much more important item to protect: the corruption of US democracy as a whole.

References

2024 U.S. Election Integrity Threats: Not Just Data Leaks & Hacks | UpGuard. (2024). Upguard. https://www.upguard.com/blog/2024-u-s-election-integrity-threats-not-just-data-leaks-and-hacks

Cyberattacks Shake Voters' Trust in Elections, Regardless of Party | Research. (2025). Georgia Tech. https://research.gatech.edu/cyberattacks-shake-voters-trust-elections-regardless-party

Election Assistance Commission, CISA (2024). *Enhancing Election Security Through Public Communications*. Cybersecurity & Infrastructure Security Agency. https://www.eac.gov/sites/default/files/2024-06/Enhancing_Election_Security_Through_Public_Communications.pdf

FBI and CISA Release Joint PSA, Just So You Know: False Claims of Hacked Voter Information Likely Intended to Sow Distrust of U.S. Elections | CISA. (2024). Cybersecurity and Infrastructure Security Agency. https://www.cisa.gov/resources-tools/resources/fbi-and-cisa-release-joint-psa-just-so-you-know-false-claims-hacked-voter-information-likely