Online Appendix

Hacking Voters' Trust in Democracy:
Panel Evidence on Safeguarding Confidence in Election Integrity

Contents

Appendix A: Balance Test & Attrition Analysis

Our sample was designed to be nationally representative, with respondent pools constructed using a quota system that matched the sample demographics to the national population based on gender, age, education level, and political orientation. To verify that the random assignment to the experimental conditions was conducted successfully, we conducted a balance test that presents the means and standard errors of key covariates across the experimental conditions (Table A1). The equivalent mean scores across experimental treatment groups suggest that treatment assignment was effectively randomized and that any differences between the groups are not the result of imbalanced samples.

Table A1: Balance Check Showing Covariate Means

Treatment Group	**Age**	**Gender (female)**	**Political Orientation**	**Education**	**Income**	**News**
Control	53.714 (0.569)	0.527 (0.018)	5.546 (0.106)	3.861 (0.053)	6.952 (0.122)	5.126 (0.083)
Cyber Treatment (Energy)	53.428 (0.602)	0.548 (0.018)	5.631 (0.11)	3.754 (0.055)	6.86 (0.127)	5.092 (0.083)
Cyber Treatment (Voting)	53.401 (0.618)	0.514 (0.018)	5.651 (0.109)	3.735 (0.053)	6.954 (0.13)	5.208 (0.084)
Inoculation Group	52.847 (0.587)	0.506 (0.018)	5.39 (0.109)	3.807 (0.055)	6.843 (0.129)	5.037 (0.085)

Note: Standard errors in parentheses. Education is measured on a six-point scale with 6 indicating a postgraduate academic degree. Political ideology is measured on an eleven-point scale with 0 denoting strong progressive ideologies. Income is measured on a ten-point scale with 10 indicating a much higher than average income. News consumption is measured on an eight-point scale with higher scores depicting more frequent news consumption.

It is possible that respondents who were already inclined to harbor doubts about election integrity dropped out between wave 1 and 2, or that viewing the inoculation video caused people to abstain from taking the second survey wave? Below, in Table A2, we report the results of a balance check that regresses respondent covariates on attrition between waves. The dependent variable in this case is a binary variable called attrition. Respondents who participated in both survey waves are assigned a score of 1, while people who dropped out are denoted as 0. Predictor variables include basic socio-demographic measures as well as the variable of election integrity beliefs and inoculation treatment assignment. Unsurprisingly, we can see that younger and wealthier respondents were slightly more likely to leave the study. Yet importantly, our treatment assignment and primary dependent variable of interest does not predict attrition.

Table A2: Balance Test Showing Factors Predicting Respondent Attrition

	Estimate	**Std. Error**	**p**
(Intercept)	0.405	0.041	0.000 ***
Inoculation Group Treatment Assigned	-0.002	0.016	0.8785
Wave 1 Election Integrity Beliefs	-0.006	0.003	0.0514
Age	-0.002	0.000	0.000 ***
Political Orientation	-0.004	0.002	0.1089
Education	0.004	0.005	0.4642
Income	0.004	0.002	0.0426 *
News Consumption	-0.003	0.003	0.3398

Note: The above model reports a probit regression analysis testing how respondent characteristics predict participant attrition across waves. * p < 0.05, ** p < 0.01, *** p < 0.001

Appendix B: Screenshots and Transcripts of Breaking News Segments

As part of this study, participants viewed a professionally produced television news segment that simulated breaking reports on ABC News. The 70-second segments were filmed, edited, and produced by media industry professionals, and the final clips include realistic cutaway clips and chyrons to maximize external validity. Two of the breaking news clips reported on a cyberattack against the energy grid or against voting equipment. The news stories differed only by the target of the attack, and all other descriptions were identical. In both segments, the newscaster reports that the attack causing a momentary disruption that was quickly rectified. The video clips begin with introductory news music identical to ABC Breaking News segments, and then the video moves between a news anchor reporting, and 'live' video footage of the targeted energy infrastructure. A third video clip was a control video, which used identical actors and introductory music, yet reported on an emotionally neutral topic – the unveiling of upgraded power lines. The fourth video that we used was the inoculation video clip that was produced by Verified Voting and which reported on the safeguards in place to protect the integrity of voting results.

Below we copy screenshots from each of the news segments and video clips, along with a complete transcript of the segment.

Cyber Attack on Energy Treatment

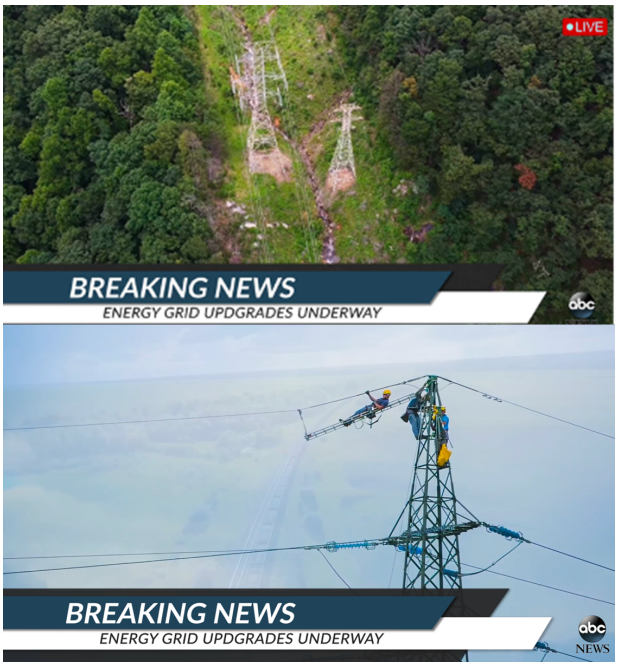
We're here live near the regional headquarters of the Department of Energy, and in just a few minutes we'll be cutting to live coverage of a press conference with the department's security chief, who will address this latest incident. According to initial reports, a cyberattack has struck the energy grid, disrupting the power supply to homes, businesses, and hospitals across the region. Authorities expect that any blackouts will be temporary, and there are reports that backup power is already flowing to affected areas. For those of you joining us, we can now report that a few hours ago a malicious cyberattack struck a section of the US electric grid. As part of the attack, hackers deployed malware that temporarily granted them access to critical systems controlling the region's electricity supply. National security officials declared that it will take time to definitively identify who is behind the attack, but initial assessments hint at the involvement of a foreign group. One official, speaking on condition of anonymity, remarked that the sophistication of the attack likely required the support of a nation state. The worry, of course, is that this attack is merely a preview of the cyber capabilities that could be used against America in the future. Until the press conference begins, back to you in the studio.

Cyber Attack on Election Treatment

We're here live near the state election board headquarters, and in just a few minutes we'll be cutting to live coverage of a press conference where the Secretary of State's spokesperson will address this latest incident. According to initial reports, a cyberattack has struck servers connected to statewide voting systems. As a precaution, officials have disconnected all digital election systems - including voter registration software, voting machines, and vote counting systems - and isolated them from all connected networks. Authorities expect that the systems will remain offline and inoperable until the malicious software is identified and cleansed from affected computers. Though details are still murky, it appears that a malicious cyberattack struck sensitive electoral computer systems. As part of the attack, hackers deployed

malware that temporarily granted them access to critical systems containing voter registration details and other election data. Security officials have declared that it will take time to definitively identify who is behind the attack, but initial assessments hint at the involvement of a foreign group. One state election board member, speaking on condition of anonymity, remarked that the sophistication of the attack likely required the support of a nation state. The worry, of course, is that this attack is merely a preview of the cyber capabilities that could be used against American elections in the future. Until the press conference begins, back to you in the studio.

Control Treatment



We're here live near the regional headquarters of the Department of Energy, and in just a few minutes we'll be cutting to live coverage of a press conference with local officials, who will announce the opening of a new electricity substation that will increase power transmission across the region. According to projections, the new substation will enhance power supply to homes, businesses, and hospitals by about 20%. Authorities expect that three additional substations will be constructed in the coming years according to a staged plan. For those of you joining us, we can now report that a few hours ago a new central substation distributing power across a section of the US energy grid was brought online. As part of the activation, engineers tied transmission routes into existing software to maximize efficiency, a program they say they have been working on for months. State authorities and citizens are celebrating the upgraded infrastructure. This region's electricity network has relied on archaic technology and dated equipment for decades, and this new substation will introduce more flexibility and reliability. One official remarked that, amid the pride at this breakthrough, it's merely a preview of the capabilities that will accompany additional upgrades in the future. Until the press conference begins, back to you in the studio.

Inoculation Treatment

How can we check that ballots are accurately counted during an election? Counting ballots by hand takes a long time, so most jurisdictions use machines to count. Post-election audits can then be used to make sure the machine's results are accurate. The best type of post-election audit is a Risk-Limiting

Audit, or RLA. RLAs are a form of quality control. Instead of recounting every ballot, we count a random selection of ballots by hand. Thanks to statistics, if we count enough random ballots and they show the same results as the machine count, we can be confident the election results are accurate. The number of ballots we inspect depends on the election results. The closer the election, the more we'll check! If the race is really close, or we uncover unexpected results, we can even do a total hand recount. Ideally, RLAs happen after the initial count butbefore official election results are certified. When machine-counted paper ballots are combined with Risk-Limiting Audits, voters can be ultra-confident that the election results are correct! Learn more about election audits at VerifiedVoting.org.

Appendix C: Codebook of Measures Used in Questionnaire

Variable Name	**Variable Construction**
Voter state residency	A single question asking: In which state are you registered to vote? The answer to this question was subsequently embedded in later questions that asked about attitudes within each respondents' state.
Perceived integrity of elections	Two-item measure asking participants to evaluate how much they trust the accuracy and integrity of elections in their state and in the US? Items were answered on a scale of 0 (completely distrust) to 10 (completely trust). Final value calculated as a mean of the two items.
Vote fraud	One-item measure asking whether participants believe that official state or county election authorities – such as the Secretary of State, registrar, or elections director – ever engage in any form of vote fraud? Items were answered on a scale of 0 (fraud never occurs) to 10 (fraud occurs frequently).
Technological literacy	Scale that captures a participant's technological literacy (developed by Kostyuk and Wayne 2021). Participants answer three questions probing whether they are aware of how information is broken down, terminology concerning unsolicited e-mails, and definitions of technological terms.
Vulnerability of election system of cyberattacks	Two-item measure asking participants to evaluate how concerned they are that computer hackers can hack into voting equipment and change election results in their state and in the US? Items were answered on a scale of 1 (not at all concerned) to 5 (extremely concerned). Final value calculated as a mean of the two items.
Cyber threat perception	Two-item measure asking participants whether they believe that cyberattacks pose a threat to a) them and their family, and b) to the United States. Items were answered on a scale of 0 (no threat) to 5 (existential threat).
Cyber helplessness / efficacy	Two-item measure asking participants the following questions to assess their agreement with the following statements. 1) The amount of information out there is so overwhelming that I've given up trying to figure out what is true or false. 2) Cyberattacks are just a fact of life. There's no way to stop them. Items were answered on a scale of 1 (strongly disagree) to 5 (strongly agree). Final value calculated as a mean of the two items.

Personal exposure to cyberattacks	Participants were asked a series of yes / no questions to gauge whether they have personally experienced different kinds of cyberattacks ranging from malware infections, to accounts being hacked, to data breaches.
Electoral reliance on technology	Participants were asked a single question about how reliant they believe their state's voting system is on digital technologies? Answers ranged from 0 (The voting system is not reliant on digital technologies) to 10 (The voting system is entirely reliant on digital technologies)
Trust in institutions	Participants were ask to assess their trust in three institutions: the national government in Washington, the State Election Commission (or equivalent institution depending on each state), and US national security authorities. Answered were scored on a scale of 0 (do not trust them at all) to 10 (trust them a great deal).
Objective understanding of electoral process	Participants were asked the following question: Which official is responsible for overseeing all election activity, including voter registration, municipal, state, county, and federal elections? Possible answers included The Governor of their state, The President of the United States, the Secretary of State of their state, the Chief Justice of the State Supreme Court, I don't know. The correct answer (which is different for different states) was always included as an option depending on the participant's state.
Political orientation	Single-item measure asking respondents the following question: "In politics people sometimes talk of left and right. Where would you place yourself on a scale from 0 to 10 where 0 means the left and 10 means the right?"
Partisan identity	Following the ANES method, participants first indicate whether they feel close to a particular party, and then to rate their closeness as very close, somewhat close, or not very close. The final product is a seven-point scale ranging from feeling extremely close to the Republican party to feeling extremely close to the Democratic party.
News consumption	Participants were asked in a typical week, how many days do they watch, read or listen to news about politics and the economy? The options range from at least once per day to not at all.
Anxiety	Participants answered a six-item scale that assessed how they were feeling at this moment on the following items: *do you feel tense / calm / relaxed / upset / content / worried.* Answers were given on a six-point Likert-scale ranging from 1 (not at all) to 6 (completely).
Voting in 2024 election	Participants were asked: did you vote in the 2024 presidential election. If they answered yes, the vote choice was marked.
Voting method	For participants who voted, we asked after their vote method (in person on election day, in person on an early voting day, mail in ballot, drop-box). For in-person voting, additional questions asked about the use of BMD, DRE, or paper ballots.
Ticket splitters	Participants who indicated that they voted were asked whether voted for the same party for all down ballot votes (i.e., Senate, state elected positions, etc.)

Appendix D: Baseline Data on Partisan Perceptions of Election Integrity

In Figure 3 in the main manuscript, we visualize the shift in perceived integrity of election results from before to after the election for Republicans, Democrats and unaffiliated votes. Perceived integrity scores were measured on a 10 point scale, and higher scores indicate higher perceived integrity. Below, in Table D1, we show the mean scores for each subgroup and the results of a paired t-test that compares the magnitude and statistical significance of the within subject change from pre-election score to the post-election score.

Table D1: Changes in Election Integrity Beliefs Disaggregated by Partisan Identity

	Pre-Election Belief in Election Integrity	**Post-Election Belief in Election Integrity**	**Difference in Means**	**p**
Republicans	5.332 (0.071)	7.076 (0.061)	1.746	0.000
Democrats	7.921 (0.048)	6.827 (0.072)	-1.090	0.000
No Affiliation	6.340 (0.085)	6.858 (0.078)	0.514	0.000

Note: Cells show mean score for outcome variable for each sub-group along with the standard errors in parentheses. The statistical significance of the difference between the pre- and post- scores is calculated using paired t-tests.

Appendix E: Modeling Cyber and Inoculation Treatment Effects

In figures 5, 7, 8 and 9 in the main manuscript, we showcase how electoral integrity beliefs change across time for different treatment groups. In this appendix, we provide the regression models underpinning these effects. In the tables below, we spotlight the regression coefficient and standard error for each of the treatment groups (cyber - energy, cyber - voting, inoculation groups) relative to the control group using linear regression models. These models provide the between-subject treatment effect as registered during the post-election survey wave. The within-subject change from wave 1 to wave 2 is reported in the main manuscript itself.

Reflecting the analyses presented in the main manuscript, we disaggregate the table by Republican and Democratic voters.

Table E1: Regression Tables for Analytical Models in Manuscript

Models for Electoral Losers

	(Fig. 5)	(Fig. 7)	(Fig. 8)	(Fig. 9)
Cyber Treatment (Energy) Group		-0.629***		
		(0.179)		
Cyber Treatment (Voting) Group	-1.266***	-1.266***	-1.266***	-1.266***
	(0.174)	(0.176)	(0.173)	(0.173)
Combined Inoculation Group			-0.217	
			(0.172)	
Inoculation Group (No Booster)				-0.284
				(0.208)
Inoculation Group (With Booster)				-0.143
				(0.216)
Constant	7.443***	7.443***	7.443***	7.443***
	(0.121)	(0.123)	(0.120)	(0.120)
Observations	819	1,189	1,220	1,220
Adjusted R^2	0.060	0.040	0.046	0.046
Residual Std. Error	2.488 (df = 817)	2.515 (df = 1186)	2.468 (df = 1217)	2.469 (df = 1216)
F Statistic	52.970*** (df = 1; 817)	25.918*** (df = 2; 1186)	30.409*** (df = 2; 1217)	20.370*** (df = 3; 1216)

Models for Electoral Winners

	(Fig. 5)	(Fig. 7)	(Fig. 8)	(Fig. 9)
Cyber Treatment (Energy) Group		-0.627***		
		(0.146)		
Cyber Treatment (Voting) Group	-1.086***	-1.086***	-1.086***	-1.086***
	(0.149)	(0.150)	(0.149)	(0.149)
Combined Inoculation Group			-0.202	
			(0.150)	
Inoculation Group (No Booster)				-0.235
				(0.182)
Inoculation Group (With Booster)				-0.165
				(0.187)
Constant	7.450***	7.450***	7.450***	7.450***
	(0.104)	(0.104)	(0.104)	(0.104)
Observations	781	1,195	1,153	1,153
Adjusted R^2	0.063	0.041	0.047	0.047
Residual Std. Error	2.076 (df = 779)	2.089 (df = 1192)	2.083 (df = 1150)	2.084 (df = 1149)
F Statistic	53.391*** (df = 1; 779)	26.667*** (df = 2; 1192)	29.600*** (df = 2; 1150)	19.753*** (df = 3; 1149)

** p < 0.05, ** p < 0.01, *** p < 0.001*

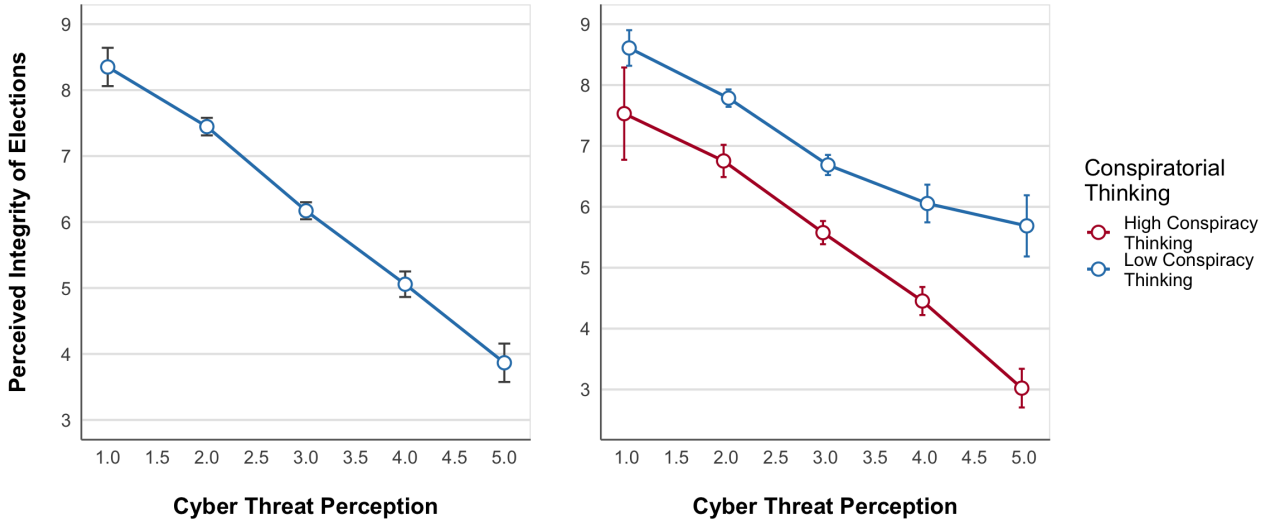
Appendix F: Exploring the Dynamics of Threat Perception, Exposure and Trust

The political psychology literature distinguishes between two related but distinct concepts that are central to this research: *exposure to cyber events* and *perceived cyber threat*. In the main manuscript, we focus primarily on the effects of exposure to media coverage of cyberattacks, which we conceptualize as an external shock that propels individuals to adopt different beliefs and behaviors as they process and cope with the situation (Snider et al., 2021).

At the same time, perceptions of cyber threat play an equally important role in this broader dynamic. Threat perception reflects individuals' evaluative judgments of the cyber risks posed by out-group actors or by the cyber domain more generally to their individual or collective goals. Even prior to any exposure, individuals hold preexisting beliefs about the level of threat posed by cyberattacks, and these perceptions may themselves shift in the aftermath of exposure. Indeed, many models in the political psychology and conflict literatures adopt a sequential framework in which exposure to threat elicits emotional distress, which heightens perceived threat, which in turn produces changes in political attitudes and behaviors (see among others, Canetti, 2017; Canetti et al., 2013, Snider et al., 2021).

We recognize that both constructs — perceived threat and exposure to cyberattack stimuli — are intertwined in shaping how individuals evaluate election integrity in response to cyber threats. Our pre-treatment (wave 1) dataset sheds light on this relationship. As shown in Panel A of Figure F1, individuals with higher baseline perceptions of cyber threat are substantially less trusting of election integrity, even prior to viewing our experimental stimulus ($r = 0.49, p < 0.001$). Importantly, cyber threat perception is not merely a proxy for general conspiratorial thinking: individuals high and low on the conspiratorial thinking scale both show a strong negative correlation between perceived cyber threat and electoral trust (Panel B), though the magnitude of the relationship differs. This pattern suggests that perceptions of cyber threat are meaningfully associated with our outcome variable and that threat perceptions shape beliefs about election integrity.

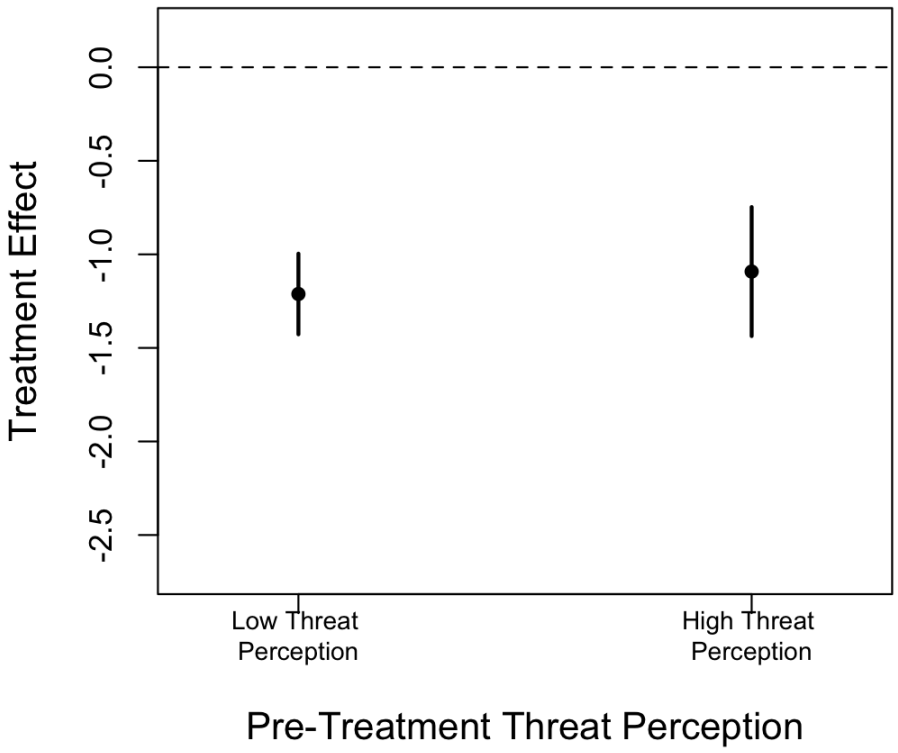
Figure F1: Pre-Treatment Correlation Between Cyber Threat Perception and Electoral Trust



Note: Dots reflect the mean level of election integrity beliefs at each level of cyber threat perception. Bars depicts the 95% CIs at each point. On the x-axis, 0 indicates a low level of cyber threat perception, and 5 denotes the highest perceptions of threat.

While recognizing the importance of this dynamic, our study is designed to do more than identify a correlation between cyber threat perception and trust in digitally conducted elections. Rather, we build on this baseline by examining how exposure to breaking media coverage of concrete cyberattacks influences attitudes above and beyond individuals' preexisting threat perceptions. As shown in Figure F2, for respondents who rank both high and low on pre-treatment threat perception, exposure to the cyberattack media treatments produces a significant reduction in electoral integrity beliefs. The stimulus, which mirrors authentic societal experiences, meaningfully shifts attitudes across the board — among Democrats and Republicans alike, and among individuals with both high and low initial threat perceptions.

Figure F2: Cyber Treatment Effect Disaggregated by Levels of Pre-Treatment Threat Perception



Note: The plot depicts estimates of the treatment effect on election integrity beliefs for each sub-group. Bars represent 95% confidence intervals and dots depict regression coefficients

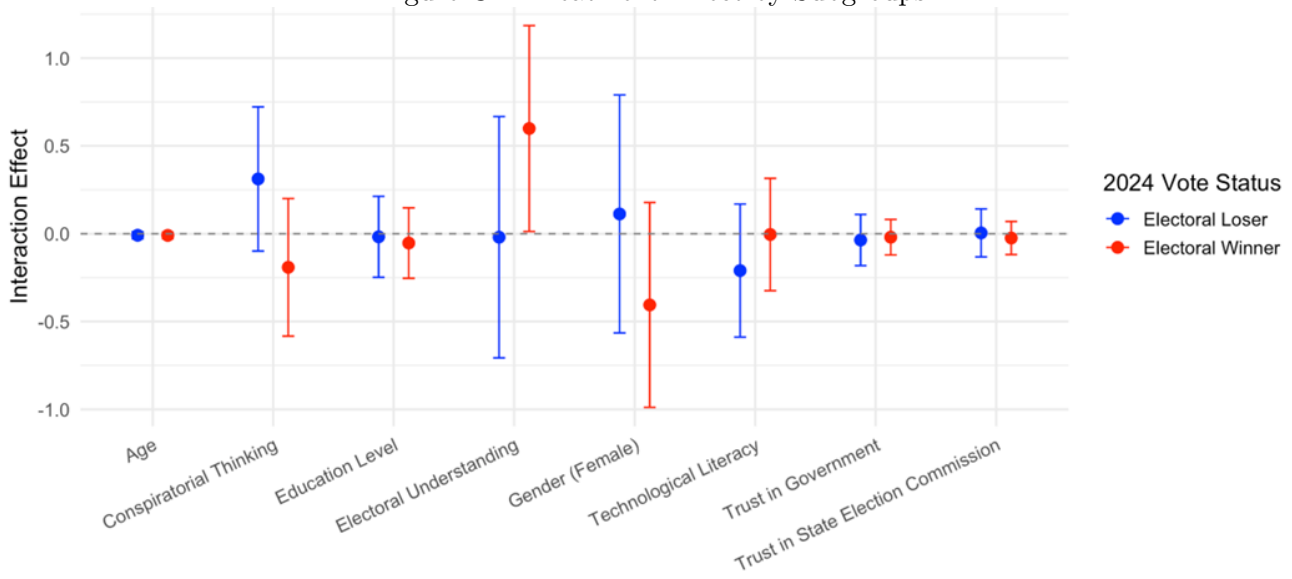
Future research should continue to disentangle the complex dynamics between perceived threat and exposure as they relate to political attitudes and behaviors. The extent to which threat perception moderates or mediates the effect of exposure on election integrity beliefs, as well as the psychological mechanisms underlying these pathways, lies beyond the scope of the present study but represents a promising avenue for subsequent investigation.

Appendix G: Evaluating the Cyber Effect by Demographic Subgroups and by State Election Methods

In the following set of analyses, we conduct several robustness tests to examine whether exposure to cyber threats equally reduces trust in electoral integrity among different demographic subgroups. In Figure G1, we regress wave 2 election integrity beliefs on the treatment assignment (cyberattack on voting system), interacting the equation with a series of different moderating variables: age, technological literacy, education level, understanding of the electoral system, gender and conspiratorial thinking, trust in government, and trust in state election commissions. Each of these moderating variables was measured in wave 1 prior to the experimental treatments that were administered much later in wave 2. If the 95% confidence intervals of the interaction term overlap with the x-axis, then we conclude that our cyber treatment generates a reduction in election integrity views among respondents who measured high and low on that moderating variable.

The results suggest that the cyberattack stimulus broadly reduced trust in election integrity among people with different ages, genders, education levels, and more. We conclude that cyber threats are a potent factor that cuts across many of the typical predictors of democratic legitimacy. The one factor that significantly interacted with the cyber treatment was electoral understanding – a question that measured objective knowledge about electoral machinery by probing whether or not the respondents could identify the person responsible for administering the election in their state (i.e., the Vice-Governor or the Secretary of State in their state). For the 55% of Republican voters who correctly answered this question, we find that they experienced significantly reduced negative effects stemming from the cyberattack treatment when compared with Republican voters who possess low levels of electoral understanding (interaction effect $\beta = 0.599, p < .046$).

Figure G1: Treatment Effect by Subgroups



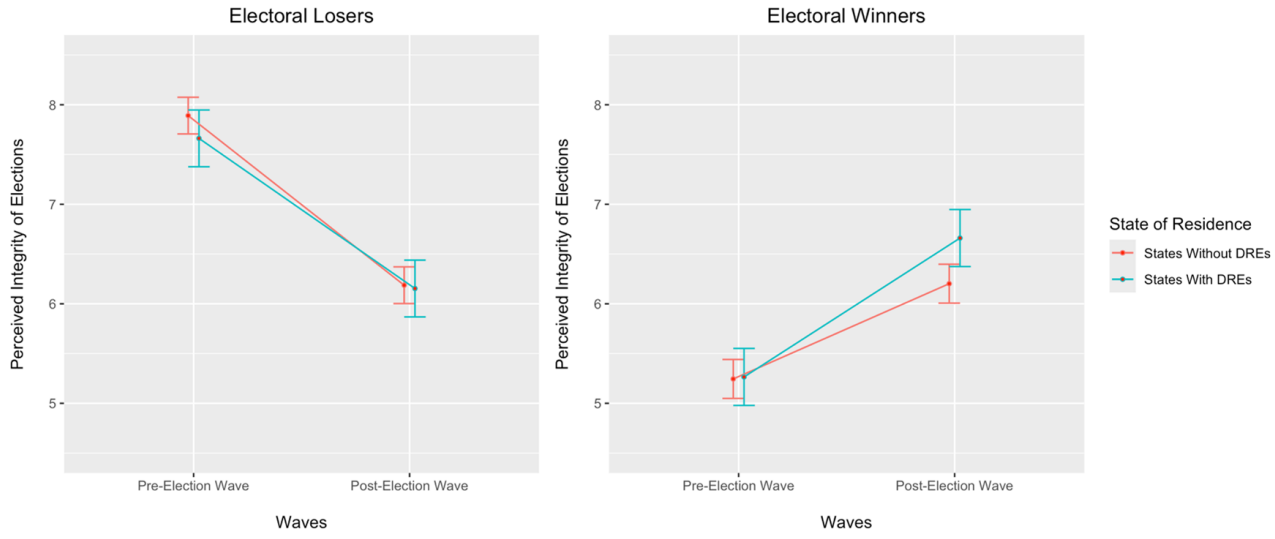
Note: The plot depicts estimates of the interacted treatment effect on election integrity beliefs. Estimates are based on an OLS models. Bars represent 95% confidence intervals and dots depict regression coefficients.

Having found that cyber threats exert a potent effect on electoral integrity beliefs across demographic boundaries, we move on to see whether residents of different states experience the effects differently.

Some states have moved quicker than others to digitize their election infrastructure, and so it reasonable to presume that residents of states using direct-recording electronic (DRE) voting machines may be more susceptible to the cyber news stories.

In Figure G2, we focus in on treatment group members (who received the cyberattack against voting machines treatment) and compare the changing election integrity beliefs as a function of their belonging to a state with and without DREs. Among Democratic voters, the results indicate that belonging to a state with greater digital electoral connectivity does not amplify the negative effect of exposure to cyber threats, as members of both state-level groupings experience identical reductions in trust. Among Republican voters, they too experience a statistically similar increase in election integrity beliefs (which appears to increase over time, but which we know is a lesser increase than members of the control group). If anything, Republican voters in digitally connected states experience less of a negative effect than other states.

Figure G2: Election Integrity Beliefs Among Treatment Group Members – Disaggregated by Belonging to States With and Without DREs



Note: Dots indicate mean scores and lines represent 95% CIs. There are 14 states that use DREs, and 36 states that do not use DREs.

Appendix H: Comparing the Cyber Threat Effect in States with Smaller and Larger Winning Margins

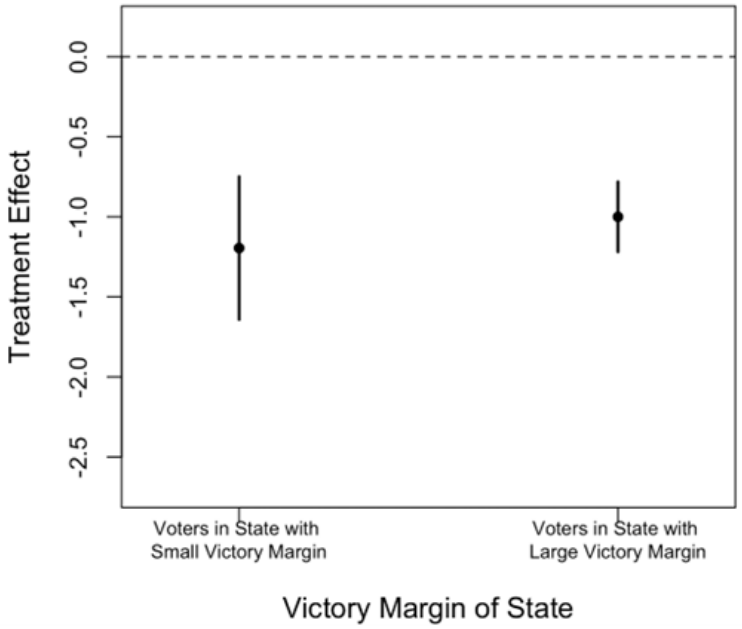
In this appendix, we entertain the possibility that the cyber threat effect may be amplified or muted in states that have smaller and larger winning margins. In states where the race is particularly close, allegations of digital improprieties may have a larger effect since even minor deviations from procedure can influence the result. In this robustness test, we look at voters' beliefs about electoral integrity in their own state and not in the country as a whole.

Table H1: States with Smallest Margins of Victory

Smallest Margin of Republican Victory			**Smallest Margin of Democratic Victory**		
State	**Winner**	**Margin**	**State**	**Winner**	**Margin**
Wisconsin	Trump	0.8%	New Hampshire	Harris	2.8%
Michigan	Trump	1.4%	Minnesota	Harris	4.2%
Pennsylvania	Trump	1.7%	Virgina	Harris	5.8%
Georgia	Trump	2.2%			

In Figure H1, we illustrate the treatment effect which shows the effect of exposure to the cyberattack stimuli on belief in the integrity of the vote in each voters' state relative to the neutral control group. On the left, we plot the treatment effect among voters registered in the above listed states that are denotes as states with small margins of victory. On the right, we plot the treatment effect among all other states, with relatively large margins of victory. Though not statistically different due to the large confidence intervals in the "small victory margin" states, the trend appears to signify that cyberattacks stimulate marginally greater concern among voters in competitive states ($\beta = -1.20$) than among voters in non-competitive states ($\beta = -0.99$).

Figure H1: Effect of Cyber Threats on Perceived Integrity of Elections in State by Closeness of Election



Note: Dots indicate differences in mean scores between the control group and the cyberattack (voting) treatment group, and bars depict 95% CIs.

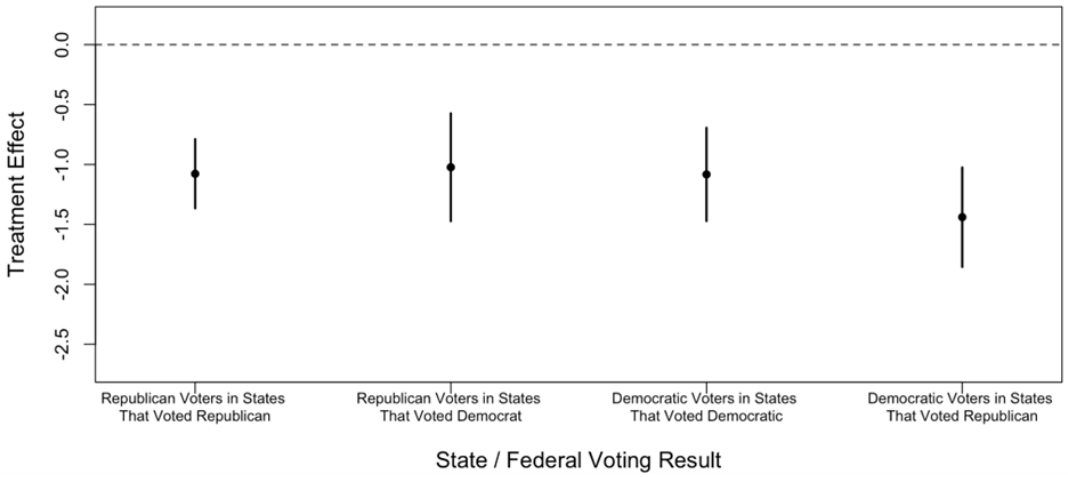
Appendix I: Comparing the Cyber Threat Effect Among Voters with Different State / Federal Vote Outcomes

In the following analysis, we compare the cyberattack treatment effect among voters where there was and was not a difference in their presidential vote choice and the outcome in their state. The rationale

for this analysis is that voters who voted for the Trump / Vance ticket but whose state voted for the Harris / Waltz ticket, may be more willing to downgrade their beliefs about election integrity following cyberattacks than "double winning" voters. Likewise, Democratic voters whose state sent its electoral college votes to the Republican ticket may be more willing to downgrade their expectations of electoral integrity than Democratic voters who achieved success at state level.

The results in Figure I1 suggest that achieving mixed results (winning at federal level and losing at state level, or vice versa) does not mitigate the negative effects of cyberattacks by giving voters a crutch by which to dismiss the impact of cyberattacks. Voters of all stripes – those who won and lost at federal and state level, and those who received mixed results – all experienced an equivalent treatment effect stemming from their exposure to cyberattacks on voting machines and election infrastructure.

Figure I1: Effect of Cyber Threats on Perceived Election Integrity by State / Federal Vote Outcomes



Note: Dots indicate differences in mean scores between the control group and the cyberattack (voting) treatment group, and bars depict 95% confidence intervals.

Appendix J: Do Voters Lose Trust in the Accuracy of the Vote Count in Their State or in the Country?

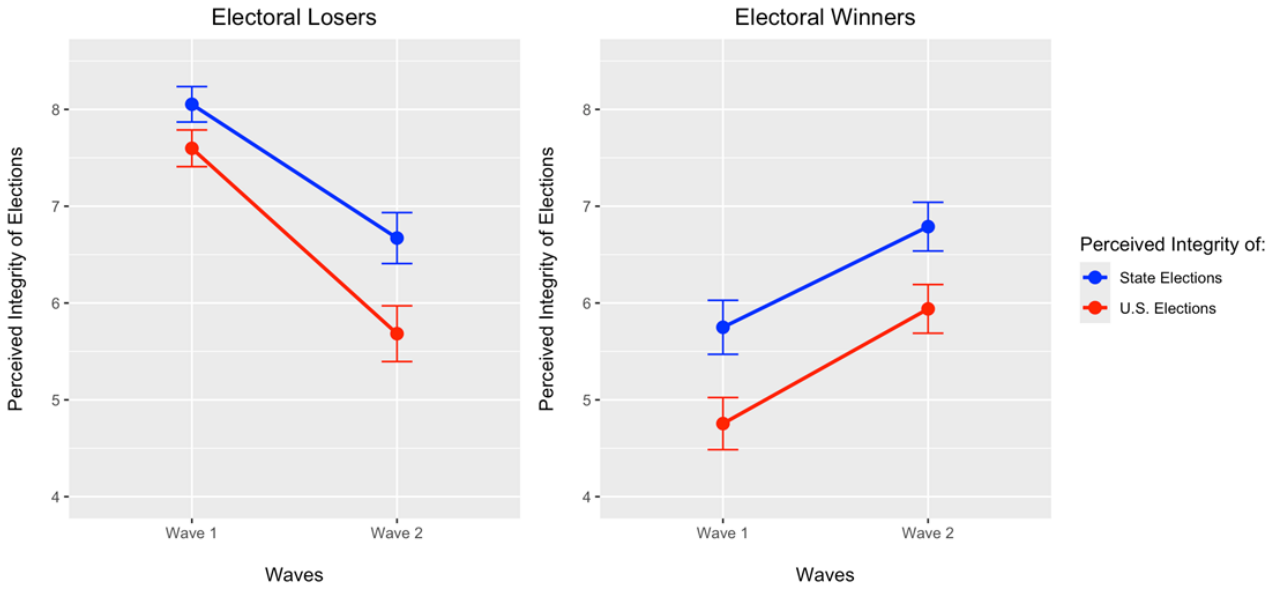
Previous research has demonstrated that US voters exhibit far higher trust in the integrity of the vote count in their own state compared with the integrity of the vote count in other states (Bowler & Donovan 2016; Gaudette et al. 2025). The logic is intuitive. Seeing as voters are more familiar with the election laws in their own state, and seeing as the vast majority of voters do not personally witness any political violence or suspicious behavior at polling places, they feel a measure of confidence about the system. Yet because voters tend not to inform themselves about election laws in other states, they have less reason to trust its integrity. This process is aggravated by affective polarization that causes them to dislike the political culture in states governed by partisan rivals, and since some number of other states fall into this category, it stands to reason that the vote count in other states is less trustworthy.

In the following analysis, illustrated in Figure J1, we disaggregate the two items making up our dependent variable, which asked voters to assess the integrity of the election a) in their own state and b) in the country as a whole. The analysis zooms in participants in the primary treatment group – those that witnessed a cyberattack against the voting system. On the surface, the findings match the

expectation in the literature that 'familiarity breeds confidence', and that voters are more predisposed to doubt the election in other states than in their own. Among both electoral winners and losers, both before and after the election, we see that participants are more believing that the elections have been fairly administered in their own state than in other states.

For Democratic voters who were exposed to the cyber threats, they experience a stark reduction in integrity beliefs when evaluating their own state (reduction of 1.38 units), however they experience an even greater reduction in trust when evaluating the country as a whole (reduction of 1.92 units). It appears as though media coverage of cyberattacks reduces trust in the system across the board, but that it reduces trust in the electoral integrity of other states more than at home. For Republican voters, they experience an equivalently muted increase in election integrity beliefs in their own state (increase of 1.04 units) and in the country as a whole (increase of 1.19 units).

Figure J1: Election Integrity Beliefs Among Treatment Group Members – Disaggregating the Items of the Dependent Variable



Note: Dots indicate mean scores and lines represent 95% CIs.

Appendix K: Effects of Treatments Among Political Independents

In the main manuscript, we demonstrate how partisan dynamics interact with cyber threats to shape voters' post-election beliefs in electoral integrity. Specifically, Figure 5 illustrates that electoral winners exhibit a significant increase in electoral trust, a pattern consistent with partisan-motivated reasoning. However, this increase is notably attenuated among individuals exposed to narratives concerning cyber-attacks on voting infrastructure. Conversely, electoral losers display a substantial decline in electoral trust, also attributable to partisan-motivated reasoning, and this decline is further intensified among those exposed to cyberattack narratives.

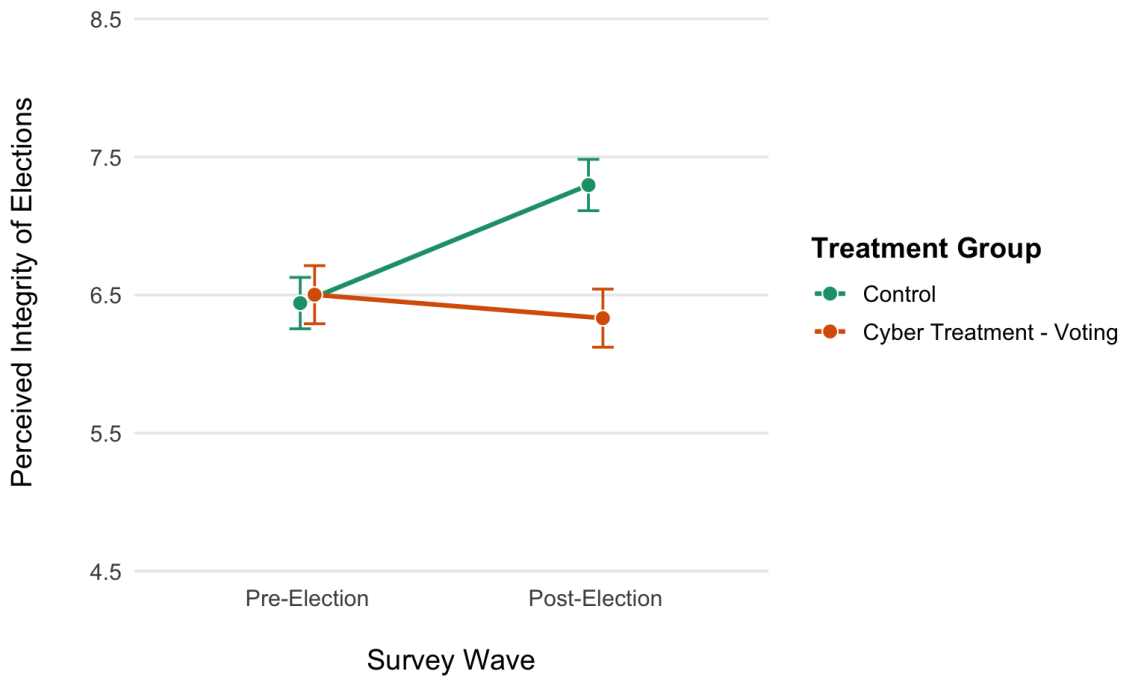
A relevant question concerns how political independents—those who do not affiliate with either major political party—respond to these same dynamics. The existence and stability of genuine independents

has long been debated in political science, with prior research suggesting that many self-identified independents move in and out of independent status across election cycles (Reilly and Hunting, 2023; Fiorina, 2016). For the purposes of this study, however, we analyze respondents who self-reported independent status at the time of data collection, constituting 26% of the sample (n = 871).

Figure K1 presents the results for this subgroup. The data reveal that independents occupy an intermediate position between Republican and Democratic respondents. Among independents in the control condition, we observe a significant increase in electoral confidence from pre- to post-election. This finding is intuitive: when individuals have no partisan stake in the outcome, a smoothly conducted election should enhance confidence in the democratic process.

However, independents exposed to the electoral cyberattack treatment exhibited no such increase. In contrast to partisans, for whom cyber exposure either exacerbated losses (among Democrats) or muted gains (among Republicans), independents displayed no change in trust. This pattern underscores the broad capacity of cyberattack narratives to dampen shifts in political attitudes, even among those with ostensibly neutral partisan orientations.

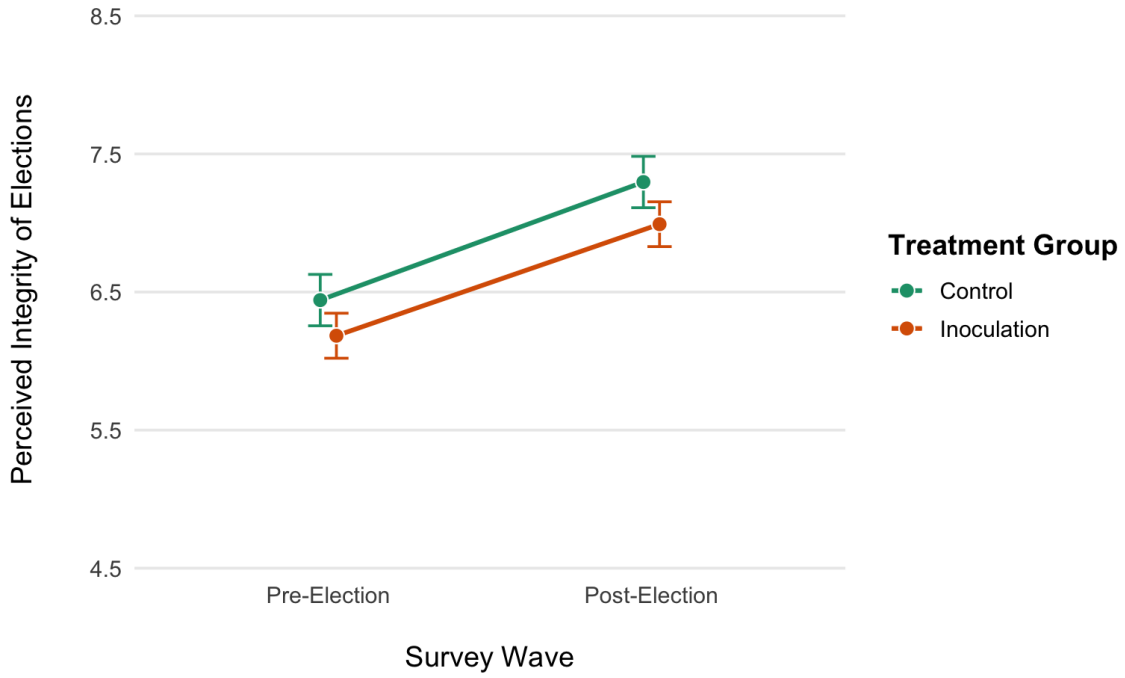
Figure K1: Cyberattack Treatment Effect Among Political Independents



Note: Dots indicate group mean scores, and bars depict 95% confidence intervals. Difference-in-differences estimates indicate a significant post-election difference among political independents ($\beta = -1.02$, $p < 0.000$) in the treatment group compared to the control group.

Figure K2 further examines the effect of the inoculation intervention on political independents. The results indicate that the inoculation video was equally effective within this group. Despite exposure to the cyberattack treatment, independents who viewed the inoculation exhibited trust levels indistinguishable from those in the control condition. These findings suggest that the inoculation effectively neutralized the negative effects of cyberattack narratives, rendering independents substantively immune to such influences.

Figure K2: Inoculation Effect Among Political Independents

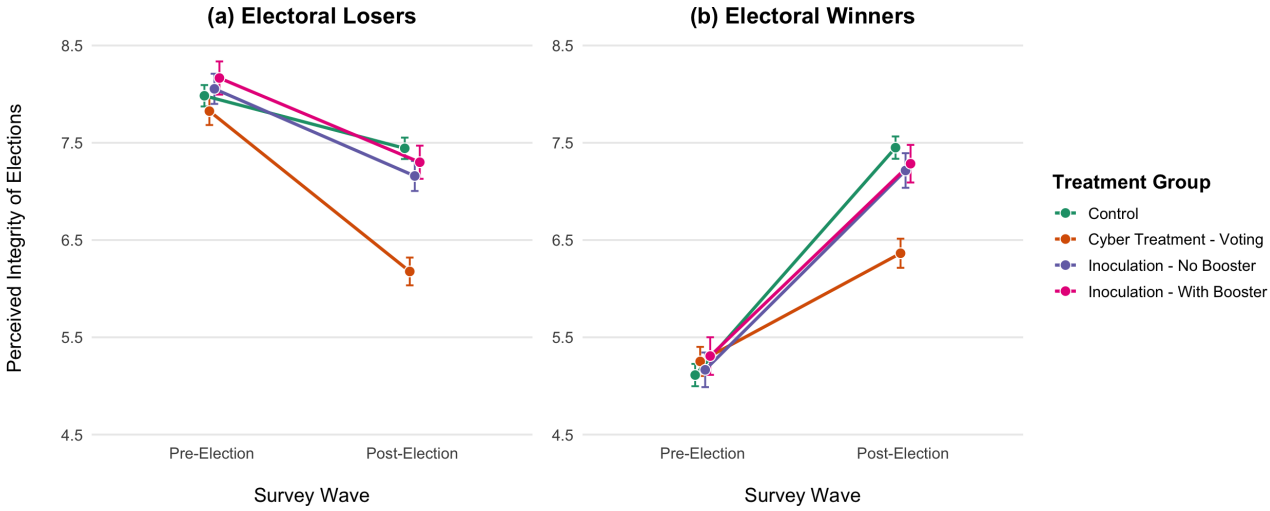


Note: Dots indicate group mean scores, and bars depict 95% confidence intervals. Difference-in-differences estimates indicate no significant post-election difference among political independents ($\beta = -0.05$, $p = 0.828$) in the inoculation group compared to the control group.

Appendix L: The Effects of "Booster" Messages on Inoculation Effectiveness

Is a single dose of the inoculation effective on its own? Prior research suggests that the protective effect of preventive interventions can diminish over time and may require ongoing reinforcement through booster messages. Our design allows us to test this directly: while the full inoculation treatment group received natural boosters between waves one and two, a randomly selected half of the inoculation group received an experimental booster message immediately before viewing the cyberattack video, while the other half did not. Figure L1 breaks down the inoculation group by booster status and reveals that both subgroups are equally resistant to the negative effects of the cyberattack treatment. The absence of a booster did not reduce inoculation effectiveness, nor did an experimental booster provide additional benefit. This pattern aligns with inoculation theory, which holds that an initial treatment can be reinforced by natural boosters, especially in high-salience issue environments. The minimal impact of our synthetic boosters suggests that once an inoculation is established and naturally reinforced, additional artificial reinforcement may be unnecessary.

Figure L1: Inoculation Results - With and Without Booster



Note: Dots indicate group mean scores, and bars depict 95% confidence intervals. Difference-in-differences estimates indicate statistically indistinguishable declines among electoral losers with and without inoculation boosters ($\beta = 0.030$, $p < 0.890$) and statistically indistinguishable increases among electoral winners with and without boosters ($\beta = 0.071$, $p < 0.774$). Full model appears in Online Appendix E.

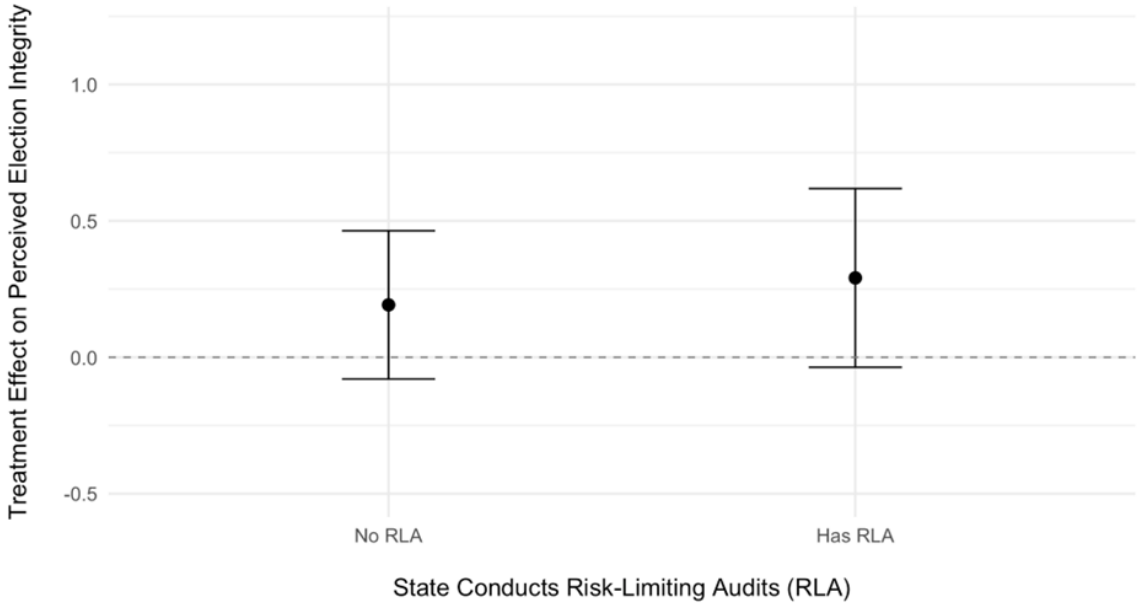
Appendix M: Inoculation Effectiveness By State Usage of RLAs

We previously found that inoculating participants using a dedicated inoculation video mitigated the negative effect of later exposure to cyberattack stimuli. Despite the inoculation group members later viewing the cyberattack videos, they did not experience the negative effects, and instead acted exactly like the control group who was not exposed to any cyberattack stimuli.

Below, we look to see whether the inoculation is equally effective among residents of states that conduct risk-limiting audits (RLAs) and residents of states that do not. The reasoning behind this robustness test is that the inoculation video highlighted several measures that safeguard the integrity of the vote count, and RLAs were presented as a prominent measure. However, since RLAs are not conducted in every state, it tracks that we may see different responses among residents of these states.

In Figure M1, we model the difference between the control group and inoculation group while disaggregating between residents of these two groups of states. A null effect indicates that the perceived election integrity levels among the inoculation group was indistinguishable from the control group, meaning that the inoculation group entirely overcame any negative effect stemming from the cyberattack video that the inoculation group viewed in wave 2. The results show that our inoculation video was equally effective in states with and without RLAs, thus indicating that the inoculation is not contingent on one particular electoral defensive measure.

Figure M1: Comparing Difference in Wave 2 Electoral Integrity Beliefs Between Control Group and Inoculation Group Among States With and Without RLAs



Note: Dots indicate differences in mean scores between the control group and the cyberattack (voting) treatment group, and bars depict 95% confidence intervals.

Appendix N: Pre-Analysis Plan

This study was conducted as part of a broader project investigating the impact of technology on modern elections. The overarching project focused on a variety of different elements, including online voting, trust in democracy, and the effect of cyberattacks on critical infrastructure. For this reason, we present here anonymized excerpts of the pre-analysis plan that relates to the research question at the heart of this paper: the effect of exposure to media coverage of cyberattacks on trust in election integrity. We confirm that the pre-analysis plan was registered prior to the collection of data.

Note on Deviation from the Pre-Analysis Plan: The original pre-analysis plan specified that all participants assigned to the inoculation condition would receive a refresher message in wave 2. Prior to fielding the second wave, this plan was modified so that only half of the inoculation group was randomly assigned to receive the refresher. This change was introduced to enable an additional experimental test of whether the effects of the inoculation persisted in the absence of a booster message. The modification was implemented before the collection of wave 2 data and does not affect the integrity of the experimental design or the interpretation of the preregistered hypotheses.

Introduction

In recent years, public interest technologies have become central to the integrity of democratic elections. These technologies offer the potential to deeply improve the safety, security, and trustworthiness of democratic elections (McGuiness & Schank, 2021). However, these benefits may be a double-edged sword as a steady stream of media reporting describing cyberattacks against critical infrastructure causes people to doubt the security of electoral systems and reach false conclusions about the susceptibility of electoral systems to cyber threats (Garnett & Hames, 2020). Technology might make elections more

objectively trustworthy at the same time as it reduces public perceptions of electoral trustworthiness.

Our chain of reasoning is as follows. First, voters' exposure to media coverage of cyberattacks causes strong psychological and political reactions (Shandler, Gross & Canetti, 2023). Media coverage of cyberattacks against commercial operations and critical infrastructure propagates a cyber doom narrative, according to which the authorities are incapable of preventing omniscient and unknowable hackers from causing chaos (Lawson, 2019; Gomez & Whyte, 2021). As a result of their exposure to attacks, voters adopt a fatalistic mindset toward cyber threats and re-evaluate their trust in societal institutions that are connected with seemingly vulnerable technological foundations.

Simultaneously, elections are increasingly being conducted using digital technologies (Cheeseman, Lynch & Willis, 2018). Between ballot marking devices, QR codes, direct recording electronic systems, electronic poll books, remote ballot marking systems, and online registrations – digital technologies are in widespread use in all jurisdictions. What is more, use of election technologies globally is on the rise with over 100 countries adopting some form of election technology, ranging from electronic voting machines to digital voter registration systems.

Connecting these two separate processes, we propose that voters make a clear link between the first premise (cyber insecurity) and the second premise (digitally conducted elections). The logic is as follows:

> *IF digital infrastructure is constantly being breached by cyberattacks AND elections are run on digital technology THEN our elections are susceptible to being breached and the integrity of our election results are suspect.*

This is a perfectly rational though erroneous thought process, which forms an example of a transitive fallacy. Voters' deductive thought process reaches the conclusion that if A equals B, and B equals C, then A must equal C. The errors in this syllogistic reasoning ignore the facts that attacks are difficult, checks and balances and resiliency measures remain in place, and there is no evidence of active exploitation of digital electoral vulnerabilities. Essentially, A $\neq$ B (not all digital technologies are being breached). B $\neq$ C (not all elections are run on digital technologies, and most maintain auditable paper trails). Therefore, A $\neq$ C.

This process is compounded by voters' tendencies toward motivated reasoning. Voters on the losing side of a competitive election are motivated to doubt that the elections results are accurate as a method of avoiding cognitive dissonance. In an attempt to reconcile their preconceived views with reality, voters buy into plausible (and sometimes implausible) explanations that cast doubt on the integrity of the elections (Mochtak, Lesschaeve & Glaurdić, 2021; Edelson et al., 2017). We argue that the process of motivated reasoning is exacerbated by perceptions of digital insecurity. Exposure to media coverage of cyberattacks sets the conditions for skepticism toward election results by encouraging people to adopt the view that digital infrastructure is inherently vulnerable to exploitation. Disappointed voters are more likely to engage in motivated reasoning and subscribe to stolen election myths. But disappointed voters who are also primed to think about cyber insecurity will subscribe to these myths to a larger degree.

We explore this topic by conducting a longitudinal survey experiment that explores how media coverage of cyber threats causes people to lose trust in the integrity of electoral outcomes. Drawing upon a representative sample of U.S. respondents who will be surveyed immediately before and after the 2024 US Presidential elections, we will randomly assign groups of survey participants to differently framed media coverage of cyber threats that depicts attacks on energy and electoral infrastructures. Other groups of survey respondents will receive an intervention designed to promote democratic resilience in the face of cyber insecurity. Specifically, we will test the effectiveness of education campaigns on the topic of *risk-limiting audits* (RLAs) as a method of overcoming voters' distrust in elections. Working with our

partners, we will assess the efficacy of a specially created educational video that describes how RLAs contribute to election integrity. The data will have a measurable impact by producing empirical models explaining public trust in election technologies, and producing policy relevant materials explaining how RLA education combats cyber insecurity – and among which groups.

Study Design & Sampling Plan

Study Design: Our survey experiment will comprise a panel study that takes place across two waves. The first wave will take place approximately 6 weeks before the presidential election. The second wave will take place approximately 2 weeks after the election has concluded.

Survey Wave 1 (the pre-election wave) will take place approx. 6 weeks before the presidential elections, and a representative sample of 4,400 voters will be surveyed. Respondents will answer a battery of questions about the perceived integrity of the election results, and baseline political attitudes, psychological predispositions, and technology attitudes will be measured. Participants will be randomly assigned to one of four groups (described below), and at this stage, members of the Inoculation Group will view a professionally produced educational video describing how risk-limiting audits protect the integrity of US elections in jurisdictions using election technolgies. This inoculation video is fielded before the election to test whether it is effective at mitigating the later effect of our cyber threat treatments.

Survey Wave 2 (the post-election wave) will take place approx. two weeks after the election. This survey will return to the same participants as in the previous wave (aspiring for a retention rate of 75%). At this time, survey participants will view an experimental treatment that differs for each of the four treatment groups.

A. Cyber Threat Group 1 – Members of this group will be asked to view a professionally produced breaking news television segment describing cyberattacks against critical US energy infrastructure.

B. Cyber Threat Group 2 – Members of this group will be asked to view a professionally produced breaking news television segment describing cyberattacks against US election infrastructure.

C. Inoculation Group – Members of this group (who already viewed the inoculation video during wave 1) will receive a refresher of the inoculation content, before they view the same breaking news television segment as in cyber threat group 1 or 2 describing cyberattacks against critical US energy / election infrastructure.

D. Neutral Control Group – Members of this group will not receive any experimental treatment.

Following the experimental stimuli, participants will again answer a series of survey questions about political attitudes, electoral and democratic trust, and cyber threat perception.

We collaborated with a team of actors and video producers to construct the videos. The two cyber threat videos appear as vivid, professionally produced 80-second television news segments that simulate a live breaking report on ABC News. The clips include realistic cutaway clips and chyrons to maximize external validity. The reports depict either a drone attack against the U.S. power grid, or election infrastructure. The scenarios reflect real world instances of attacks against critical infrastructure, and the videos mimic both the facts of such attacks and the tone of reporting about them.

The inoculation group video was produced by Verified Voting, an American nonprofit 501(c)(4) corporation that lobbies for reliable and publicly verifiable election systems. Its mission is to strengthen democracy for all voters by promoting the responsible use of technology in elections. The 79-second

video clip provides information about risk-limiting audits (RLAs). The video explains how RLAs work and how they can instill confidence in election outcomes.

Survey Variables: In wave 1, all participants will answer a series of survey questions that measures their beliefs in election integrity, asks about their perception of threat associated with cyberspace, media consumption habits, political attitudes, psychological predispositions, and socio-demographic data. The purpose of this preliminary wave of data collection is to collect baseline data on our core dependent variables. Furthermore, the use of a dedicated survey wave to collect dispositional and socio-political variables avoids the concern of these variables priming participants (were they to be collected immediately prior to the experimental treatments), and steers clear of the possibility of their being influenced by the treatments (were they to be fielded after the experimental stimuli).

Variables to be collected during this wave include:

a) Perceived integrity and accuracy of elections at state and federal levels

b) Perceptions about the prevalence of vote fraud

c) Perceptions about the prevalence of illegal voting

d) The vulnerability of the election system to cyber threats

e) Support for online / technologically-mediated voting procedures

f) Digital literacy

g) Cyber threat perception (national and personal)

h) Trust in government

i) Past exposure to cyber threats

j) Perceived electoral reliance on technology

k) Trust in institutions

l) Understanding of electoral processes

m) Conspiratorial thinking

n) Political and partisan identity

o) Media consumption habits

In waves 2 and 3, following the experimental stimuli, we will measure the following mediating and dependent variables (a through e), along with additional variables that ask about people's experiences during the immediately preceding elections:

a) Perceived integrity and accuracy of elections at state and federal levels

b) Perceptions about the prevalence of vote fraud

c) Perceptions about the prevalence of illegal voting

d) The vulnerability of the election system to cyber threats

e) Support for online / technologically-mediated voting procedures

f) Emotional responses – anger, anxiety

g) Voting choices

h) Voting method (mailing, in-person, drop-box, etc.)

i) Voting experience (positive, negative, etc.)

j) Exposure to circulating conspiracy theories

Data: As of the date of submission, the data collection has not been started and none of the data has been quantified, constructed, observed, or reported by the researcher.

Data Collection Procedures: Respondents will be recruited in the United States through YouGov. The benefit of using this survey company is that we can attain a higher retention rate across waves, obtain a more representative sample, and guarantee the absence of bots.

In wave 1, we will obtain a representative sample of 4,400 US respondents. Representative respondent pools are constructed using a quota system that matched the sample demographics to the national population on the basis of gender, age, income, and ethnicity. During wave 2, we aspire for a retention rate of 75% per wave, and subsequent tests will confirm that the attrition rate across waves is not correlated with any socio-demographic variables or treatment assignment allocations. The sample will comprise adults – above the age of 18 – who are residents and citizens of the United States. It is the responsibility of the survey company to ensure that the respondents abide by the conditions of service, including providing accurate residency information.

Sample Size Rationale: The sample size is mainly driven by power considerations. Since an experiment is included in this survey, there must be enough observations in each of the treatment conditions. Currently, assuming an even distribution of respondents among the four treatment conditions, we can expect to see approximately 1,100 respondents in each group in wave 1, and 800 per group in wave 2. This sample size offers a sufficiently large number to enable sub-group analyses that will need to account for treatment assignment and Republicans and Democrats.

Stopping Rule: Sampling will stop once the targeted number of observations is reached. The data will not be examined prior to the completion of the collection.

Blinding: Respondents will not know the purpose of the study beyond a general introductory statement requesting that they participate in a survey about foreign policy. Respondents will not be aware of the random allocation of treatment groups.

Theory and Hypotheses

This project identifies an additional reason why voters exhibit such ingrained mistrust in election systems. The distrust is not, as long presumed, only a product of increasingly bitter partisanship and motivated reasoning. Rather, there is a component whereby voters are evaluating the security of technological systems, and inferring flawed yet understandable conclusions about the susceptibility of electoral systems to cyber threats.

Until now, the literature has discussed the idea that rampant cyber threats create a culture of mistrust. If everything is digitally connected, and everything that's digitally connected is vulnerable, then nothing can be trusted. Yet this logic has been rather amorphous – focusing on a generalized

mistrust without any concrete manifestations. This project seeks to show how this mistrust translates into concrete democratic / electoral harms.

We divide our hypotheses by voters who belong to the winning and losing parties.

> **Hypothesis 1**: *Winners* will increase their trust in the integrity of elections, and *losers* will decrease their trust in the integrity of elections (basic motivated reasoning hypothesis)
>
> **Hypothesis 2**: *Losers* who are exposed to the *cyber threat treatment* groups will reduce their trust in the integrity of elections even more than losers in the control condition. (motivated reasoning X cyber threat hypothesis)
>
> **Hypothesis 3**: We expect that the inoculation treatment will confer a palliative effect against digital election threats. Specifically, *losers* who are exposed to the *inoculation treatment groups* will reduce their trust in the integrity of elections less so than losers in the cyber threat treatment groups. (motivated reasoning X inoculation hypothesis)

Among those partisans whose vote accorded with the winning party:

> **Hypothesis 4**: *Winners* will increase their trust in the integrity of elections due to motivated reasoning.
>
> **Hypothesis 5**: *Winners* who are exposed to the *cyber threat treatment* will increase their trust less than winners in the control condition.

Analysis Strategy

Balance and randomization tests: To mitigate against biased estimates of our treatment effects, we intend to run balance checks to confirm that the random allocation of respondents to the treatment groups did not result in skewed sub-groups on the basis of key covariates. In the case of unequal treatment distribution, we will run a robustness test that employs entropy balancing to reweight the data to population parameters. Through this analysis, we can show that the substantive conclusions remain the same regardless of whether weights are used. We will check randomization by running logit regressions that estimate the effect of pre-treatment covariates on treatment assignment.

Treatment effect estimations: We will run OLS regression analyses to observe how allocation to treatment groups influences the dependent variables of interest. We will run models with and without the following covariates in our models to account for the known effect of demographic and attitudinal factors in guiding political beliefs: age, gender, education, and income.

Our longitudinal analyses that observe shifts from wave 1 to wave 2 will utilize within-subject analytical techniques to observe how outcome variable scores change over time as a function of treatment assignment. To measure changes in the dependent variables of interest between waves, we will use repeated measure analyses of variance, together with a series of paired T-tests with adjustments for repeated measures.

We will test hypotheses relating to the mediating effect of emotions using the mediation technique developed by Imai et al. (2011). This technique requires that we estimate two equations relating to the A' and B' pathways, and then perform a bootstrap simulation. Each equation runs a least-squares regression. The dependent variable in equation 1 (M) is anger, while for equation 2, the dependent variable (Y) is either support for redistribution or regulation.