

# The limits of cyberattacks in eroding political trust: A tripartite survey experiment

The British Journal of Politics and  
International Relations  
2024, Vol. 26(4) 1033–1054  
© The Author(s) 2023



Article reuse guidelines:  
sagepub.com/journals-permissions  
DOI: 10.1177/13691481231210383  
journals.sagepub.com/home/bpi



Sharon Matzkin<sup>1</sup> , Ryan Shandler<sup>2</sup>   
and Daphna Canetti<sup>1</sup>

## Abstract

To what extent do security threats – such as cyberattacks – undermine trust in government? Fears have emerged that cyberattacks undercut public trust in government and sow doubt in democratic institutions heavily dependent on digitised systems. Nevertheless, the logic of this threat remains untested. This article presents survey experiments conducted in the United States ( $n=607$ ), the United Kingdom ( $n=594$ ), and Israel ( $n=627$ ) that examine whether cyberattacks on critical infrastructure truly undermine public trust in government and, if so, by what psychological mechanism. We exposed participants to simulations of cyberattacks against critical infrastructure before measuring the psychological and political outcomes. Our results reveal that cyberattacks do not undermine voters' trust in the government's ability to protect them. Furthermore, in the United States, exposure to cyberattacks heightens public trust by amplifying anger. Our findings inject a missing comparative component to the theoretical discussion of when, why, and how cyberattacks affect public trust in government.

## Keywords

cyberattacks, exposure to terrorism, national security threats, psychological distress, public trust in government, survey experiment

## Introduction

Cyberattacks on critical infrastructure have become a significant concern in the realm of cybersecurity and, recently, for political scientists. These attacks target vital systems and networks that are essential for the functioning of a country's economy, security, public safety, and democratic stability. Therefore, it is inevitable that political scientists and cyber scholars alike have zoomed in on an insidious threat: the ability of cyberattacks to undermine public trust and sow doubt in democratic institutions. The logic of this insidious threat works as follows: With critical infrastructures, elections, healthcare, news

---

<sup>1</sup>School of Political Sciences, University of Haifa, Haifa, Israel

<sup>2</sup>Georgia Institute of Technology, Atlanta, GA, USA

### Corresponding author:

Sharon Matzkin, School of Political Sciences, University of Haifa, Haifa 3103301, Israel.

Email: sharona.work@gmail.com

media, finance, and government bureaucracy all relying on digital networks, the occurrence of cyberattacks by seemingly omniscient and invulnerable actors undercuts the government's guarantee of personal security and the integrity of democratic institutions (Schneider, 2022; Shandler and Gomez, 2023). If cyberspace, a central pillar underpinning critical infrastructure in modern society, is perceived as vulnerable, the public will reevaluate their trust in the government. Yet despite the intuitive plausibility of the claim that cyberattacks erode public trust, its logic remains undertested, and the psychological mechanism at its heart remains unknown. Therefore, this article presents a rigorous, multi-country experimental analysis that tests whether cyberattacks undermine public trust in government and, if so, by what psychological mechanism they do so.

The idea that cyberattacks can result in political consequences has been reinforced by recent empirical studies demonstrating how cyberattacks influence voters' attitudes and behaviours. Public exposure to digital attacks has been found to promote militaristic political attitudes, encourage escalation of violence, and amplify public demands for strict new security policies that undermine privacy (Kreps and Schneider, 2019; Leal and Musgrave, 2023b; Snider et al., 2021). Such consequences – as cyber scholars and pundits posit – are liable to subvert the pillars of democratic societies. These effects are thought to manifest as a consequence of the psychological distress that cyberattacks evoke in the public (Shandler et al., 2023a; Shandler and Gomez, 2023).

Be that as it may, scepticism of a cyber-political link persists. Why should the public be swayed by cyberattacks, which lack the visual and explosive spectacle of conventional warfare or terrorism? The idea that voters will respond to political violence by reducing their public trust in government – specifically, the public's trust in the government's ability to mitigate future attacks – clashes with a historical line of research depicting the public responding to external threats by rallying behind their political leaders (Mueller, 1970). Moreover, research has shown that civilians typically become resilient to political violence if the effects are constrained, and as cyberattacks become ubiquitous, habituation theory holds that the public is expected to become emotionally inured to ongoing political violence (Bitton and Laufer, 2018; Muldoon, 2003; Nussio, 2020; Waxman, 2011). Therefore, as the novelty surrounding cyber threats fades, an alternative logic dictates that cyberattacks should arouse no discernible effect on public trust in government or perhaps even evoke heightened trust in government as with physical violence. We are thus faced with two competing theories arguing that public exposure to cyberattacks should either amplify or undermine public trust in political leaders and government institutions more broadly.

To isolate the political effects of cyberattacks, we employed a multi-country survey experiment that simulated public exposure to different forms of cyberattacks compared to conventional terrorism. We sampled participants from the United States ( $n = 607$ ), the United Kingdom ( $n = 594$ ), and Israel ( $n = 627$ ) and exposed them to professionally produced original media news reports of threatening cyber-terror attacks on critical infrastructure. Within this experimental framework, we mimicked the style and framing of media coverage, intentionally using exaggerated descriptors such as cyber-terrorism, which are the terms that media convey to the public when reporting about cyberattacks (Jarvis et al., 2017; Shandler et al., 2023b). Participants were randomly assigned to view professionally created video treatments depicting cyberattacks or conventional terror attacks on railway infrastructure, with the attacks either causing lethal outcomes or financial damage. We employed an experimental  $2 \times 2$ -factorial design with a pure control group. We collected psychological responses and data on political attitudes to examine

whether and how cyberattacks on critical infrastructure produce political consequences to understand the psychological mechanism by which the cyber-political link operates.

Our findings suggest that contrary to recent cyber threat assessments, cyberattacks on critical infrastructure do not directly erode public trust in government – a null finding we obtained in all three cases sampled. Because our literature a priori dictated an emotional mediating mechanism, we followed recommendations by Memon et al. (2018) and Zhao et al. (2010) and tested for mediation regardless of a direct effect. Our empirical evidence corroborates that in the United States (but not in the United Kingdom or Israel), exposure to cyberattacks can increase public trust by generating anger at a common outgroup enemy. We theorise that the suddenness and the isolation of cyberattacks on critical infrastructure play a role in the formation of a rally effect as a result of cyberattacks with lethal outcomes.

As the political science and political psychology literature grapples with the question of how to incorporate cybersecurity within a psycho-political framework, our findings demonstrate that in one regard, at least, cyberattacks do not diverge from classical models, which predict higher public trust in government following shocking and sudden national events. We conclude this article by discussing further avenues of research that cyber scholars should consider in their examination of the cyber-political link.

## **Exposure to cyberattacks and public trust in government**

Stemming from a broadly debated crisis of public trust in government during the last decade, public trust in government has become one of the most debated topics of research in the political sciences. Ranging from discussions about the definition and conceptualisation of public trust in government (see, for example, Hardin, 2002) through the empirical operationalisation and classification of public trust (see the debate between Fisher et al., 2010, 2011 and Hooghe, 2011 about dimensions of public trust in this journal), and theorising the nature and origins of public trust in government (Brody and Shapiro, 1991; Mueller, 1970; Zaller, 1992) – research on public trust is burgeoning. The subject of public trust spans far back to the core roots of democratic governance. In its essence, the paradigmatic idea in scholarly literature considers political trust in government to be an imperative prerequisite for democratic rule and institutional integrity (Ben-Nun Bloom and Arikan, 2013; Crozier et al., 1975).

Although the definition of public trust is still a matter of scholarly debate, the opinion held by most scholars views public trust in government as the perceived ability of governments and law enforcement agencies to produce an expected and publicly desired outcome (see Horne, 2017 for definitions and taxonomy of public trust). As such, public trust in government is a subjective assessment fed by two components – an authority in which trust is placed – the government, and a subject to which trust refers – the public (Berry et al., 2008; Van der Meer, 2017). Essentially, the public is more likely to comply with laws and engage in democratic activity when they trust the government and other democratic institutions (Scholz and Lubell, 1998). From a government perspective, high public trust allows for policy reforms and higher risk-taking. In contrast, lowered trust has been found to compromise government stability and hinder public legitimacy of government (Bianco, 1994).

Thus, public trust in government is fundamental to a thriving democratic society (OECD, 2022). Trust reinforces compliance with various public policies, such as health regulations and the tax system. It also promotes political participation, strengthens social

capital, and nurtures institutional legitimacy (Hetherington, 1998). Trust is associated with support for democracy (Ben-Nun Bloom and Arikian, 2013) and is pivotal for community and national resilience (Kimhi, 2016; Kimhi et al., 2020). Therefore, the preservation of public trust in government becomes more salient as modern societies digitise (Wang et al., 2023; You and Wang, 2020). Citizens must be able to trust that the government can manage and regulate digitised systems to mitigate the recurrence of cyberattacks that exploit structural digital vulnerabilities (Maschmeyer, 2023). Because regulatory regimes rely on digitised networks almost exclusively, Haber and Reichman (2020) argue that the state can be understood as a networked entity. Hence, public trust in government is particularly sensitive to new digital and systematic vulnerabilities and exploits.

Prior to the digital era, research on political violence and public trust in government primarily focused on the ‘rally ‘round the flag’ effect (Perrin and Smolek, 2009; Woods, 2011). As Mueller (1970) explained, exposure to sudden violence by external forces, such as international terrorism, causes voters to rally behind political leaders. Theoretical approaches to the nature and origins of the rally effect have resulted in two primary schools of thought. The first – what Brody and Shapiro (1991) referred to as Mueller’s ‘patriotism’ explanation – posits that in times of national threat, the public will uncritically unite behind the political incumbent for fear of hindering the nation’s success in recovery. According to the ‘rally’ view, the public relates to the commander-in-chief as an ‘anthropomorphic symbol of national unity – a kind of living flag’ (Hetherington and Nelson, 2003: 37). Hetherington and Nelson’s account of a rally effect can be viewed as a political reflex, in which the public responds to a national event without more profound consideration of preexisting experiences with the government’s past responses or policies. Another account for the rally phenomenon – what Brody and Shapiro (1991) and Zaller (1992) refer to as the ‘opinion leadership’ interpretation – posits that a rally effect, to the extent that a rally effect forms (but see Baker and Oneal, 2001; Feinstein, 2018, 2022) is not dissimilar to any other political phenomena. According to the ‘opinion leadership’ view, when the public is given the opportunity to consider the government’s performance, the public will do so based on preexisting information about government performance and policies and the availability of new information as relayed by the media.

Nevertheless, cyber scholars argue that growing public dependence upon the cyber domain for everyday activities introduces unprecedented political vulnerabilities. But if sudden external threats have historically caused surges in political trust, why should cyberattacks produce an opposite set of political effects? Cyber scholars posit that the importance of the answer to this question lies within the ever-changing social and political landscape consequent to the rapid progression of the information highway and, inevitably, the rapid digitisation of states (Maschmeyer, 2023; Schneider, 2022). Cyber scholars’ divergence from traditional models that explain public trust following political violence is premised on cyberspace-specific factors. As opposed to the physical sphere, cyberspace enables enhanced speed and distance of coercive action (Kuehl, 2007) and greater anonymity that complicates the process of attributing attackers (Egloff and Wenger, 2019; Finlay and Payne, 2019; Libicki, 2009; Lynn, 2010), and is regularly depicted by the mass media in hyperbolic images of mass destruction, which amplify fear and threat perception within the public (Jarvis et al., 2017; Lawson, 2019). Furthermore, recent work on the political effects of cyberattacks reveals that assumptions about cyber assailants and uncertainty about perpetrators’ identity can bear with them political consequences (Egloff and Dunn Cavelti, 2021; Gartzke, 2021). In turn, uncertainty about the nature of an attack can lead decision-makers to (erroneously or not) rely on heuristics in

responding to them (Gomez and Villar, 2018). Owing to the uncertainties surrounding cyberattacks and the identity of perpetrators, authorities must often guess what the most effective policy response should be (Gomez and Villar, 2018). From a public perspective, the uncertainty associated with cyberattacks generates a sense of dread (Gomez and Villar, 2018; Van Schaik et al., 2017), which leads governments to adopt restrained responses that differ from those employed in response to non-cybernetic violence (Gomez, 2019; Kaminska, 2021; Leal and Musgrave, 2022).

Congruent to these cyber-specific factors, empirical works have demonstrated that cyberattacks generate distinct political effects that differ from classical theories that predict political behaviour. For example, research has found that cyberattacks arouse more robust public demands for an escalation of government responses (Schneider, 2020; Valeriano and Jenson, 2019). These include a heightened desire for military retaliation (Gross et al., 2017), public calls for enhanced protective measures (Canetti et al., 2021), and a willingness to sacrifice civil liberties for the sake of enhanced personal and national security (Snider et al., 2021). Furthermore, distinct to cyberattacks is that shifting political preferences hinge on a lethality threshold, suggesting that only certain types of cyberattacks generate strong political effects (Shandler and Gomez, 2023). It logically follows that trust evaluations following cyberattacks may plausibly be different from trust evaluations following conventional warfare and political violence.

## **Exploring the psychological mechanisms behind cyber-trust effects**

Overall, research on American political reactions to sudden terror attacks suggests that emotions can play a central role in the formation of political attitudes (Marcus et al., 2000; Vasilopoulos et al., 2019). Notwithstanding, studies on the role of emotions in driving political attitudes following cyberattacks remain understudied and provide conflicting evidence (Feinstein, 2022; Gomez and Whyte, 2021; Gross et al., 2009, 2017; McDermott, 2019; Shandler and Gomez, 2023; Snider et al., 2021).

To understand how emotional mechanisms interact with digital violence, we can draw on several decades of political psychology research that have studied the psychological effects of conventional terrorism and political violence. Underpinning state-level outcomes of terror attacks are the affective mechanisms that drive political outcomes (Snider et al., 2023). Research has indicated that terrorism affects the public psychologically: Terror can affect life satisfaction (Frey et al., 2009) and result in anxiety, sadness, anger, and dejection (Pliskin et al., 2020). Emotional responses to terrorism and political violence include identifying positive and negative emotional states. Research has found that terror evokes psychological distress such as anxiety (Canetti-Nisim et al., 2009; Liverant et al., 2004; Sinclair and LoCicero, 2007), fear (Ronen et al., 2003), and anger (Lerner et al., 2003) among other negative affective states. Of these, anger and anxiety are thought to generate the most politically consequential effects (Huddy et al., 2002, 2007, 2009; Huddy and Feldman, 2011).

Although anger and anxiety are considered ‘negative emotional states’, these emotions, when decoupled, give rise to vastly different political outcomes. In his definition of anger, Darwin (1872, 1993: 244) referred to anger as a state of mind that differs ‘... from rage only in degree, and there is no marked distinction in their characteristic signs’. Thus, Darwin implicitly defined anger as an emotional state that varies in intensity, from mild

irritation or annoyance to intense fury and rage. Anger is often experienced when people perceive themselves or those around them to have suffered a wrong, which arouses a desire to rectify the harm inflicted. Thus, anger acts as a motivating agent, and angry individuals experience moral outrage, denigration of the outgroup, and support hawkish national security policies (Huddy et al., 2009; Lerner and Tiedens, 2006). For instance, in the extensive research on the effects of public exposure to 9/11, it was found that people who predominantly experienced an anger response exhibited heightened trust in government (a rally response) because they perceived the nation to be under attack and in a state of perceived threat (Perrin and Smolek, 2009; Skocpol, 2002).

Distinctive from anger, anxiety is an emotional experience prompted by situations perceived as uncertain and lacking situational control (Lerner and Keltner, 2000, 2001). Once aroused, anxiety encourages pessimistic judgements and causes people to seek information to minimise future victimisation. Huddy and Feldman (2011) found that anxious people feel a sense of personal threat, seek ingroup enhancement, engage in reaffirmation of social values, and are less likely to support overseas military action. The aversive, information-seeking, threat-reducing behaviour aroused by anxiety differs from the active response elicited by anger, which causes people to seek retaliatory action to regain a sense of emotional equilibrium (Huddy et al., 2021).

Considering the distinct features of cyberspace, to what extent can the classical literature on the emotional effects of terrorism apply to new age digitised cyberattacks? To the extent that cyberattacks are simply a subgroup of the broader category of violence, then we could expect the prevailing theories to apply equally. Nevertheless, research has revealed that the qualities of cyberspace give rise to different emotional reactions to cyberattacks (Backhaus et al., 2020; Canetti et al., 2016). Other research has examined how emotional reactions to cyberattacks predict changes in public trust in government (Gross et al., 2017; Shandler and Gomez, 2023). Furthermore, studies have found that cyberattacks evoke dread, anxiety, anger, and heightened threat and risk perceptions (Kostyuk and Wayne, 2021). Gross et al. (2017) found a slight increase in public trust following cyberattacks, whereas Shandler and Gomez (2023) found the opposite: lowered trust due to a heightened sense of dread. Thus, based on the abovementioned literature, we hypothesise the following:

*H1.* Exposure to cyberattacks on critical infrastructure will result in heightened levels of anger and anxiety.

*H2(a).* Anger will mediate the relationship between exposure to cyberattacks and public trust in government, which will result in increased public trust.

*H2(b).* Anxiety will mediate the relationship between exposure to cyberattacks on critical infrastructure and public trust in government which will result in decreased public trust.

## **Methodology**

### *Procedure*

Prior to our main study, we ran a pilot experiment in the United States ( $n=50$ ) to verify the efficacy of our experimental manipulations, specifically, to confirm that exposure to media reports of terror attacks caused significant variance in both emotional and political responses. To this end, we concocted a New York Times article that reported different



types of terror attacks causing derailments on the Amtrak train network (see Supplemental Appendix B for the full procedure, results, and vignette).

Following the reaffirmation of our hypotheses in the pilot study, we conducted a multi-country experimental study to measure how cyberattacks influence trust in government and the psychological mechanism underlying such an effect. We surveyed 1828 participants in the United States ( $n=607$ ), the United Kingdom ( $n=594$ ), and Israel ( $n=627$ ; see Supplemental Appendix A for an analysis of power). Participants were recruited by Amazon Mechanical Turk in the United States, Prolific in the United Kingdom, and the Midgam Survey Company in Israel. We focused on these three countries for the following two main reasons: they are all strong democracies; therefore, public trust is a salient political matter, and they are all frequent victims of cyberattacks, increasing the experimental realism of the treatments. The selection of these countries also reflects a reality wherein the countries currently most susceptible to cyberattacks are the United States, Europe, and the West more broadly (Macdonald et al., 2022).

Participants were randomly assigned to one of five experimental conditions in each country, amounting to a  $2 \times 2$  design with a pure control group (see Supplemental Appendix D for balance checks). In each group, participants were asked to view realistic and professionally produced news coverage that simulated breaking news reports on television channels in three countries – NBC News in the United States, Sky News in the United Kingdom, and Channel Two in Israel. The news reports were prepared by industry professionals and used authentic footage and were 1:34 minutes to 1:36 minutes long. The video clips begin with introductory news music identical to NBC News in the United States, Sky News in the United Kingdom, and Channel Two in Israel. In the lethal-outcome conditions, a news reporter on the scene is providing voice-over media coverage of footage depicting ambulances near a derailed train and simultaneously running ribbons at the bottom of the screen, stating that a cyber/conventional terror attack by an unidentified perpetrator has resulted in a train derailment. The reporter continues to report that seven people have died due to the derailment, while 10 people have been severely injured and are being taken to a nearby hospital for medical treatment. The footage then cuts to a segment insert that shows a conference room holding a discussion among military personnel. All the lethal manipulations were adapted to local context so that the US manipulation depicted a US derailed train, the UK manipulation depicted a British derailment, and so forth.

In the financial outcome experimental conditions, the footage depicts a hooded perpetrator and the reporter's voice-over reporting that millions of dollars were stolen from the accounts of tens of thousands of passengers' credit cards. The footage is followed by the footage insert of the military personnel in the conference room, identical to the lethal-outcome manipulations. In terms of the identity of the perpetrators, we deliberately opted to leave the perpetrators anonymous in all the manipulations to reflect the attribution problem in cybersecurity (Finlay and Payne, 2019). Once a cyberattack is launched, attackers use a plethora of techniques to mask their identity and location, often routing an attack through several dispatching networks around the globe. Thus, the retrospective identification of a forensic link between a cyberattack and a possible perpetrator becomes cumbersome and lengthy for governments and security agencies. States are very careful in not attributing blame and pegging responsibility to perpetrators for fear of misattribution that could lead to escalation of an underlying conflict. The clips and news stories were kept identical in each country, subtly altered only to refer to local cities and railway organisations, and with the correct logo of each broadcaster (see Figure 1). Everything else remained constant – including the news presenter who reported in English in the US and UK news reports and Hebrew in the Israeli report.



**Figure 1.** Screenshots of the cyber-terror attack manipulation in the United States, the United Kingdom, and Israel.

The above figure depicts screenshots from the video manipulations in the three countries we sampled: the United States, the United Kingdom, and Israel.

Our manipulations resulted in the following four treatment groups: (1) conventional terror resulting in lethal outcome, (2) conventional terror resulting in financial outcome, (3) cyber-terror resulting in lethal outcome, and (4) cyber-terror resulting in financial outcome. A fifth group, the pure control group, was not assigned any manipulation but answered the survey questions. We opted to leave the control group as a pure group after careful deliberation about the nature of the control group. There are multiple ways to construct a control group, each with its advantages and disadvantages. The advantage of a pure control group, which we have employed, is that respondents are not subjected to any experimental stimuli that could affect their emotions. The disadvantage is that the control group is not identical to the treatment groups in all ways since treatment group members viewed experimental manipulation videos. Another possibility to construct a control group – one that we contemplated – was to provide respondents in the control group with a neutral video about trains. However, as emotions lie at the heart of our theory, we opted to leave the control group pure since we did not want to arouse any emotions (positive or negative) that could bias our results. Therefore, the assigned participants in the control group answered the questionnaire fully but did not view any videos.

In all cases, we adhered to the local language (e.g. subway in the United States, underground in the United Kingdom). Videos were originally produced and mimicked the style regarding logos and opening news segment music. The scripts were verified for consistency and language discrepancy in a blind back-translation process (see Supplemental Appendix C for video manipulation scripts and screenshots from the lethal and financial conditions).

### Variables

After viewing the video treatment, participants completed a detailed questionnaire to gauge their emotional state and political attitudes and to obtain demographic information.



To measure the dependent variable, *public trust in government*, we used the trust measure employed by Berry et al. (2008). A principal component analysis (PCA) revealed that all three variables were loaded onto one factor (see scree plot in Supplemental Appendix H). We constructed the dependent variable based on the mean score of the three items in the questionnaire. Participants were asked to report,

How confident are you that the government and law enforcement agencies can prevent a terror attack from taking place over the next six months? /How confident are you that the government and law enforcement agencies can prevent a terror attack from taking place over the next year? /How confident are you that the government and law enforcement agencies can prevent a terror attack from taking place over the next five years?

Cronbach's  $\alpha = .921$  resulted in an excellent measure of reliability.

Anger was measured using the four-item State-Trait Anger Expression Inventory (STAXI): 'Are you mad?/Do you feel irritated?/Do you feel angry?/Are you furious?' (Spielberger et al., 1983; Cronbach's  $\alpha = .962$ ). Anxiety was measured using the six-item short form Spielberger state-anxiety inventory (STAI): 'Do you feel tense?/Do you feel calm?/Do you feel relaxed?/Do you feel upset?/Do you feel content?/Do you feel worried?'<sup>1</sup> (Spielberger, 1972; Cronbach's  $\alpha = .905$ ). All questionnaire items were scored on a six-point Likert-type scale (1 = Not at all to 6 = Absolutely). In addition to these measures, we collected extensive socio-demographic information, including political orientation, age, gender, frequency of use of public transportation, and previous exposure to terror and cyberattacks. For the Israeli questionnaire, all survey items were professionally translated and independently back translated from English to Hebrew, and questions were adapted, where needed, to adhere to the local terms used in each country (e.g. subway in the United States vs underground in the United Kingdom).

### Analytical approach

Our proposed theoretical model predicts that exposure to various forms of cyberattacks would influence public trust in government through an indirect pathway encompassing the emotions of anger and anxiety. We therefore explore the possibility of a direct effect between cyberattacks and trust evaluations, as well as an indirect effect through the emotions of anger and anxiety. Following Memon et al. (2018) and Zhao et al. (2010), we regard direct and indirect effects as being independent irrespective of null effects. In keeping with Memon et al. (2018) and Zhao et al. (2010) even in the absence of a direct effect, 'researchers should test [the possibility of mediating effects] regardless of the significance of the relationship between X and Y' (Memon et al., 2018: v). The literature points to two negative emotions – anger and anxiety – each bearing discreet political outcomes. While anger results in people seeking retaliatory action to regain a sense of equilibrium, anxiety results in aversive, information-seeking, threat-reducing behaviour (Huddy et al., 2021). Considering that our theoretical foundation a priori dictated that these two emotions resulted in distinct political outcomes, we introduced them separately into the model to avoid opposing complementary and competitive mediation, which could have resulted in a null effect.

Because we expected participants to experience a range of emotions simultaneously in response to the experimental stimuli (Garcia and Rimé, 2019; Larsen and McGraw, 2011), we opted to use structural equation modelling (SEM) for the analysis of the results. Our choice of employing SEM in our analytical approach stems from our complex model,

which entails multiple different mediating variables (see Figure 2). We found the unique attributes of SEM to be superior at integrating multi-variable models into an easily understandable output.

## **Results**

### *Correlations and comparisons*

Before conducting the SEM test, we analysed the correlations between the variables of interest. In the United States, we found that public trust in government is significantly and positively correlated with anger, previous exposure to physical terror, and level of education. In Israel, public trust in government significantly and negatively correlated with previous exposure to cyberattacks and positively with age. We found no significant correlations between public trust in government and variables in the United Kingdom. Next, to examine whether there was a bivariate relationship, we conducted a series of independent samples t-tests for the independent variable (exposure to experimental stimuli) and the dependent variable (public trust in government). The results in all three countries revealed no direct relationship between trust in the government and the experimental treatments. The absence of a direct effect, however, does not rule out the possibility of mediation, especially considering that the public reacts to political violence through emotional channels (Garcia and Rimé, 2019; Getmansky and Zeitzoff, 2014; Hirsch-Hoefler et al., 2016; Hobfoll et al., 2006; Shandler et al., 2023a; see Supplemental Appendix E for the complete set of comparisons and correlations).

### *Structural equation model*

Structural equation modelling (SEM) is beneficial for simultaneously estimating multiple and mutual dependencies and for understanding the size and direction of direct and indirect effects. It is instrumental in experimental studies that require causal relationships (Lowry and Gaskin, 2014). SEM combines factor analysis and multiple regression analysis and is helpful in analysing the structural relationship between measured variables and latent constructs (Kline, 2015). A proposed model is acceptable in SEM according to a set of accepted fit indices. We embark on two distinct but related stages to establish whether specific paths are significant if the model is acceptable: first, the validation and estimation of suitability using a set of fit indicators. These indicators include the Incremental Fit Index (IFI), Comparative Fit Index (CFI), and Normed Fit Index (NFI). A model is acceptable if IFI, NFI, and CFI  $\geq .90$  (Byrne, 1994). The Root Mean Square Error of Approximation (RMSEA) is a 'badness-of-fit measure', yielding lower values for a better fit. An RMSEA  $\leq .06$  could be considered acceptable (Hu and Bentler, 1999). In addition to the fit indices, the chi-square test is unique among possible measures of fit in SEM because it is a test of statistical significance. The chi-square value tests the null hypothesis that the predicted model and observed data are equal. In other words, it measures whether the predictions match the actual data. Therefore, a null hypothesis indicates a good model fit for the chi-square test. As a measure of robustness, we opted to also run the data by employing a regression model (see Supplemental Appendix F for an OLS hierarchical regression table). We find that the main effects remain the same as the results in the structural equation model. This outcome gives confidence that our results are robust to the choice of analytical technique.

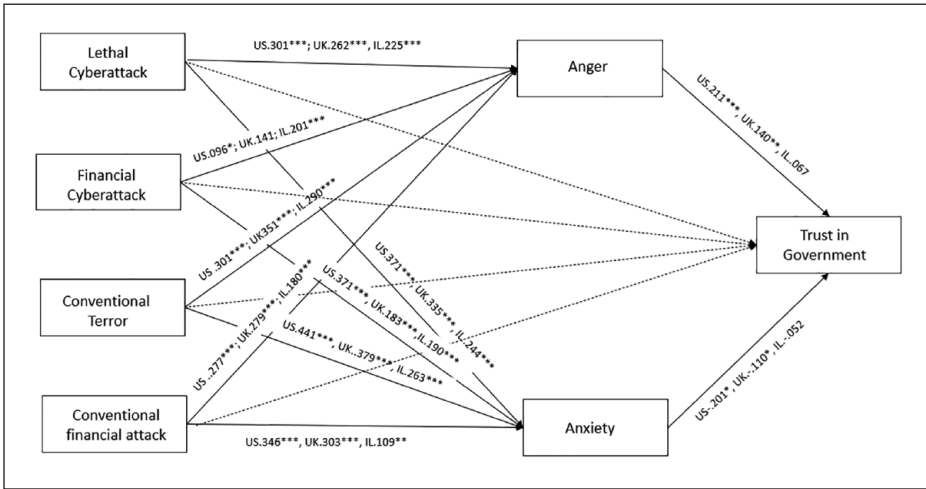


Figure 2. SEM.

For parsimony, we depict two structural equation models in one image while omitting demographic variables, although these were included in the analyses. N total = 1828 (United States (n = 607), the United Kingdom (n = 594), and Israel (n = 627)). The pure control group is not depicted but was modelled. The dotted lines indicate no direct effects.

\*p < .05; \*\*p < .01; \*\*\*p < .001.

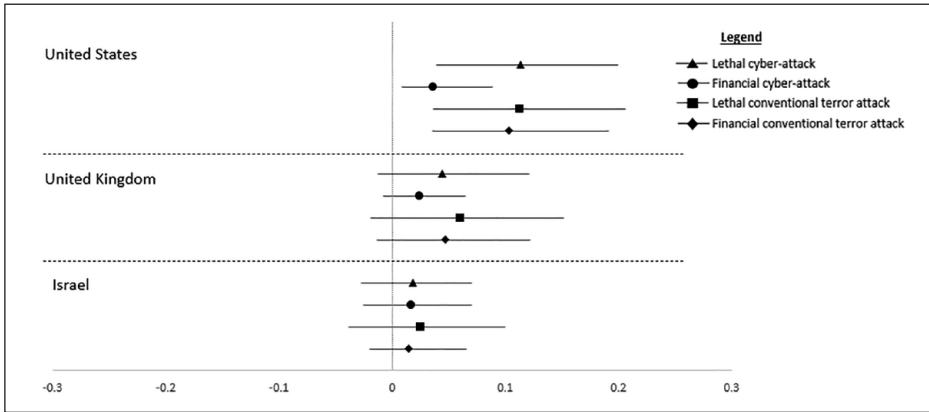
Direct effects

An initial validation test reveals that our proposed models achieved high goodness of fit (see Supplemental Appendix G for SEM goodness-of-fit indices). Having surpassed this preliminary threshold, we examined the direct effects. As illustrated in Figure 2, lethal and financial cyberattacks and lethal and financial terror attacks failed to directly predict public trust in government in any of our three country samples. Following the extensive support for the argument that mediating effects may exist despite no direct relationship (Memon et al., 2018; Zhao et al., 2010) we examined the mediating mechanism, which posits a role for anger and anxiety in driving attitudinal changes following exposure to cyberattacks.

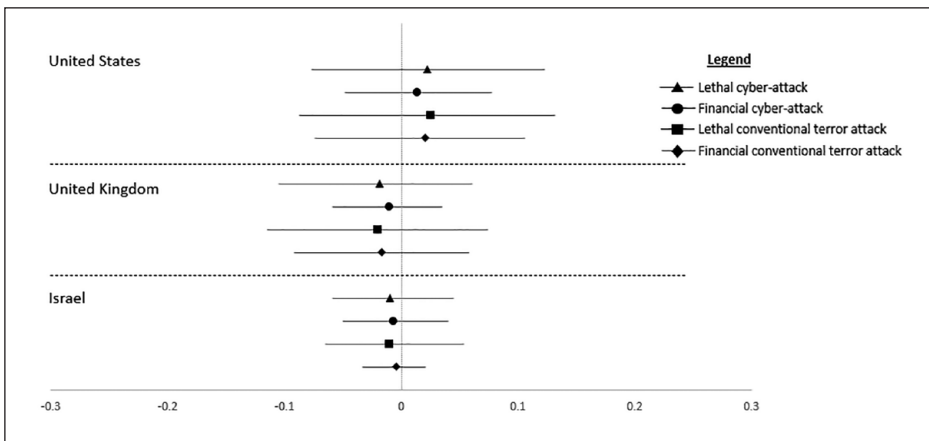
In the a-path of the SEM, we found that all forms of cyberattacks amplified anger and anxiety and that the effects were weaker for financial cyberattacks than for lethal ones. The b-path of this indirect model revealed that the relationship between negative emotions and trust in government was significant for anger in the United States but not in the United Kingdom or Israel. Anxiety did not predict any change in public trust evaluations of government in any of the countries we sampled.

Indirect effects

The absence of direct effects between the independent variables and the dependent variable, the significant relationships between the independent variables and the mediators, and between the mediators and the dependent variables pave the way for an examination of indirect mediation effects, as hypothesised in hypotheses 2(a) and 2(b) (Memon et al., 2018; Zhao et al., 2010).



**Figure 3.** Mediation effects of anger underpinning the independent variables and trust. This figure shows the mediation estimates of anger between the independent variables and public trust in government. Note that no significant indirect estimates exist in the United Kingdom and Israel cases. Legend: Triangle = Lethal cyberattack; Circle = Financial cyberattack; Square = Conventional lethal terror attack; Diamond = Conventional financial terror attack. 95% Confidence Intervals.



**Figure 4.** Mediation effects of anxiety underpinning the independent variables and trust. This figure shows the mediation estimates of anxiety between the independent variables and public trust in government. Note that anxiety has no significant mediation effects in any of the cases we sampled. Legend: Triangle = Lethal cyberattack; Circle = Financial cyberattack; Square = Conventional lethal terror attack; Diamond = Conventional financial terror attack. 95% Confidence Intervals.

Figures 3 and 4 show the results of the indirect analyses using anger and anxiety pathways, respectively. The indirect anger mechanism reveals that in the United States, anger fully and positively mediated the relationship between exposure to cyberattacks and public trust in government. The lethal scenarios elicited a far more potent effect than the non-lethal attacks. Consistent with the political psychology literature and the rally theory, exposure to violence indirectly raised trust evaluations, refuting the notion that trust in government suffers following cyberattacks. There was no significant indirect effect in the United Kingdom and Israel, and the heightened anger resulting from the experimental

treatments did not affect public trust in the government. This result supports hypothesis 2(a) in the United States but not in the United Kingdom or Israel.

As depicted in Figure 4, our results reveal that anxiety did not significantly mediate the relationship between experimental treatments and trust in government. This finding refutes hypothesis 2(b) in all three countries.

## Discussion

The primary focus of this research is to elucidate if and how the disruptive forces of technology can perhaps reshape the fragile balance between governance and citizen trust in the cyber era. Throughout history, the interaction between citizens and their governing bodies has undergone a dynamic balance between two fundamental elements: trust and scepticism in the government's ability to protect its citizens. Trust in government has been the cornerstone of social cohesion and democratic stability, while scepticism has served as a healthy check on government performance and concentration of power. By examining the relationship between cyberattacks and public trust in government, we report that the emergence of novel security threats – such as cyberattacks on critical infrastructures – can offer indispensable new insights into the malleable nature of public opinion in the cyber era. Stemming from this view, this delicate interplay has given rise to various theories that seek to uncover the origins and nature of trust in government and its evolution over time. Pundits and cyber scholars have suggested that cyberattacks create a crisis of trust and undermine the public's trust in democratic institutions (Bumiller and Shanker, 2012; Maschmeyer, 2023; Schneider, 2022). Nevertheless, the logic behind this theory remains untested, and the psychological mechanism at its heart is unexplored. To offer an empirical substantiation or repudiation of this claim, this article reported a tripartite survey experiment exposing 1828 participants in the United States, the United Kingdom, and Israel to simulated cyberattacks to identify the ensuing psychological distress and trust outcome.

We examine our research question through the prism of Mueller's (1970) rally theory and formulate our hypotheses on the vast literature revolving around the rally effect. Through a rigorous examination of the effect of cyberattacks on critical infrastructure, our results suggest that cyberattacks do not *directly* erode or amplify public trust in the government's ability to mitigate future cyberattacks on critical infrastructure. This null finding recurred in all three countries we sampled. Rather, to the extent that a cyber-political link occurred, the trust effects of cyberattacks manifested through an *indirect* psychological mechanism. We confirmed that cyberattacks on critical infrastructure uniformly evoked anger. While our manipulations were not focused on the theoretical aspects of a rally effect per se, we can assume that in the absence of a presidential statement about the event at hand, the public – in the United States at least, acted upon an emotional reflex that resulted in the formation of a political outcome. Our results reveal that this emotional reflex, in turn, heightened participants' trust in the government in the United States.

In this way, our findings align with Mueller's rally theory and resemble the many political psychology studies that explored the effects of exposure to terrorism and political violence (Huddy et al., 2007, 2009; Huddy and Feldman, 2011). This finding suggests that digital-era violence can be subsumed into earlier theoretical paradigms and that no new political theories are required to explain human behaviour or political tendencies in the face of novel digital threats. The emotional response generated by violent incidents depends on a range of internal factors, such as people's long-term emotional sentiment

about adversaries, values concerning conflict, and habitual emotional tendencies (Holland, 2021; Holland and Jarvis, 2014) and external factors, namely, news framing and subsequent government interventions (Halperin, 2014; Huddy et al., 2021).

By deliberately opting to leave the perpetrators anonymous in all the manipulations, we were able to reflect the attribution problem in cybersecurity (Finlay and Payne, 2019). Factors such as the Internet's borderless nature and state-sponsored actors' involvement further complicate attribution. Attackers can launch operations from different locations, exploiting legal and jurisdictional ambiguities. State-backed attacks introduce political considerations, making distinguishing between criminal hackers and government entities harder. Moreover, cyberattacks on critical infrastructure take place in an environment of technical complexity, resulting in a cumbersome task for governments to identify the perpetrators. This poses a difficult conundrum for states as they are conscientious not to misattribute perpetrators. At the same time, authorities try to maintain public trust in the government's ability to mitigate such attacks. Furthermore, the misattribution of cyberattacks could lead to an escalation of conflict. For cyberattacks specifically, the absence of an easily identifiable perpetrator as a target for the public's sentiment of anger does not seem to affect trust in the government. These findings echo other work that examined the desire for retaliation against possibly related targets when the identity of an attacker is unknown (Shandler et al., 2022).

We designed our comparative experimental framework to optimise external and internal validity, but the observed effects were inconsistent in the three countries we sampled. Although the present empirical setup does not provide a conclusive explanation for this inconsistency, several possibilities exist. First, a recent meta-analysis showed that rally effects were evident mainly in the United States (Godefroidt, 2023). Analysing several decades worth of rally experiments, the study concluded that they rarely manifested outside the United States and that Americans were more prone to rallying around their leader as an extension of the American flag in the aftermath of a conflict. This pattern recurred in our data as well.

An alternative explanation to our null finding suggests that we may be witnessing a habituation effect. On one hand, sudden and visceral acts of violence result in politically charged emotions. On the other hand, civilians living in ongoing conflict tend to become emotionally inured and habituated to a conflict situation as it evolves into a threshold of normalcy (Bitton and Laufer, 2018; Muldoon, 2003). Habituation literature reveals that civilians tend to adapt to conflict situations and become emotionally inured (Gelkopf et al., 2013; Hasler et al., 2023; Hobfoll et al., 2006; Itzhaky et al., 2017; Muldoon, 2003; Shechory Bitton and Silawi, 2019). This could explain why, in our findings, the emotional effects aroused from cyberattacks and the subsequent reduction or increase of public trust were milder in Israel and the United Kingdom. The two former nations have experienced prolonged conflict, while the latter has experienced sudden terror attacks. It is plausible that habituation effects caused by exposure to conventional terrorism and political violence can transfer to the cyber domain and cushion emotionally driven political effects caused by cyberattacks.

Our findings also have implications for the construct of public policy. First, cybersecurity seems to be a persistent 'cat-and-mouse' race as cyber threats to critical infrastructure vulnerabilities evolve and become more sophisticated. As perpetrators' technological sophistication advances, the government's role in cybersecurity will only become more complex. Governments must adapt to novel security threats, collaborate globally, and work closely with private sector partners to ensure the security and stability of the cyber



sphere. Moreover, politicians and policymakers seeking to advance proactive measures to mitigate future cyberattacks (e.g. a rollout of robust digital surveillance policies in the form of regulation) should account for the normative, social and conflict contexts in which they deploy their policies (Guillon and Kergall, 2020; Zhang et al., 2020).

Second, trust in government ebbs and flows differently in response to sudden exogenous shocks (Hetherington, 1998; Levi and Stoker, 2000) than in long-term events. Spikes in rally-around-the-flag effects have been observed following crises such as the Reagan assassination attempt (Ostrom Jr and Simon, 1989) and the 9/11 attacks (Huddy et al., 2002). The rally around the flag effect is short-term and tends to dissipate quickly (Baum, 2002). Although public trust in government and political leaders rises dramatically following national crises, this heightened state of public trust tends to return to baseline levels before the occurrence of the security threat (Kernell, 1978). This implies that a rally effect may not have a lasting impact on public opinion or political dynamics. Because government performance is hard to estimate in short-term events such as sudden cyberattacks, government performance becomes particularly salient and positively associated with political trust in situations where the public is exposed to long-term events such as prolonged conflicts (Van der Meer, 2017). It is possible that the uptick we found in trust in the government in the United States (mediated by anger) was a result of the suddenness of the cyberattack on critical infrastructure that participants witnessed. We anticipate that prologued exposure to cyberattacks, such as the Russian cyber-meddling in the 2016 US election or alleged meddling in Brexit, would result in a steady corrosion of public trust in government institutions if these are publicly perceived as unable to mitigate such attacks against core pillars of democracy.

Third, the emotions that cyberattacks evoke on critical infrastructure and their political outcomes imply that the cyber sphere is comparable to the physical domain. Scholars have theorised that cyberspace is an essential new arena in world politics because of its low cost, anonymity, and asymmetries in vulnerability (Nye, 2010). However, our results suggest that concerning emotionally charged political outcomes, lethal cyberattacks and conventional terror attacks are comparable in emotionally politically driven civilian responses.

## Conclusion

Classical and prominent theories elucidating trust in government considering shocking and sudden security threats have evolved, shedding light on this intricate dynamic (Mueller, 1970). As cyberattacks continue to present challenges to critical infrastructure vis-à-vis an acceleration of the digitisations of states around the world, pundits and cyber scholars have voiced growing concern about the integrity of public trust in government and, consequently, the stability of democratic institutions in the event of national and catastrophic cyberattacks. Although these concerns grow daily, empirical investigation into the ebbs and flows of public trust in government following exposure to cyberattacks remains scarce, with existing research providing conflicting evidence. On one hand, cyber scholars sound foreboding warnings about the impending erosion of core democratic pillars, such as trust in government and security institutions following exposure to cyberattacks (Schneider, 2022; Shandler and Gomez, 2023). On the other hand, established classical theory holds that sudden attacks result in heightened trust in government (Mueller, 1970). While a substantial number of empirical studies support Mueller's classical theory following conventional terror attacks, cybersecurity

scholarship still lacks substantial empirical evidence for a cyber-political outcome link essential for theory building. As a consequence, we know relatively little about the impact of exposure to sudden cyberattacks on critical infrastructure and the role of emotion in this context in the formation of public trust in government.

This article was intended to fill this gap by building upon a comparative survey-experiment framework designed to optimise external and internal validity. To this end, we performed survey experiments in three democracies: the United States, the United Kingdom, and Israel. We chose these case studies due to common attributes in cyberspace and comparable levels of trust in government. In contrast to recent cyber assessments, but in line with Mueller's (1970) classical rally theory, we find that cyberattacks on critical infrastructure do not erode trust in government. Furthermore, we find that emotions – primarily anger – play a pivotal role in *heightened* trust in the government in the United States (but not in the United Kingdom or Israel). While many possible theoretical explanations explain this phenomenon, we theorise that variance in the types of cyberattacks (e.g. sudden vs ongoing cyberattacks; see Leal and Musgrave, 2023a) and context of conflict (nations embroiled in short-term political violence vs ongoing conflict) in the three countries we sampled perhaps play a role in terms of the emotions of anger and anxiety and that these, in turn, then become politically charged as a result.

While our rigorous experimental design has paved the way for cybersecurity scholars to embrace classical theories, we have temporarily dampened the voices that claim that cyberattacks will uniformly precipitate an erosion of public trust in government, at least in terms of the impact of sudden cyberattacks on critical infrastructure. We believe that further avenues of exploration into the relationship between cyberattacks and public trust deserve scholarly examination. First, our time of sampling is somewhat of a 'betwixt-and-between'. While cyberattacks are no longer a novelty, they have still not become commonplace on critical infrastructure to a level of disruption to daily life. It is very plausible that as perpetrators become more technologically sophisticated in exposing and exploiting systematic vulnerabilities in trusted critical infrastructure used by the public daily, various types of cyberattacks would result in different outcomes in terms of public opinion in general and public trust in particular. Furthermore, prolonged exposure to ongoing cyberattacks (vs sudden and isolated incidents) would publicly implicate the government's inability to mitigate cyberattacks. Therefore, we believe that cyber scholars should make the distinction between sudden and isolated cyberattacks versus frequent or ongoing attacks that could result in the erosion of public trust in government and security institutions over time. Second, another avenue of research should examine the role of identified perpetrators. The attribution problem remains a complex and ongoing challenge in cybersecurity (Finlay and Payne, 2019). While pegging responsibility for a cyberattack is a lengthy and cumbersome task, scholars should examine how the identification of perpetrators affects public trust in government – for instance, an examination of Bandura's (2011) moral disengagement theory in relation to ingroup versus outgroup cyber perpetrators in ongoing conflict settings (Li et al., 2016) versus sudden cyberattacks. Third, we believe variance in cyberattack types could affect public trust differently. Logic dictates that cyberattacks against critical infrastructure that uphold core democratic processes, such as voting machines, would yield an immediate and acute anxiety response. Over time, as these types of cyberattacks proliferate, vis-à-vis the digitisation of critical systems, it is inevitable that public attention will be turned to the government to mitigate such attacks. Fourth, our trilateral survey experiment examined the roles of anger and anxiety as mediators. We urge political psychology scholars to introduce other emotions into their models. Some empirical work has examined the role of dread in the relationship

between exposure to cyberattacks and political outcomes (Gomez and Villar, 2018; Shandler and Gomez, 2023). Other emotions, such as hatred towards identified perpetrators, seeking revenge, and superstition towards government surveillance aimed at mitigating the recurrence of cyberattacks on critical infrastructure, could also bring with them lasting political outcomes.

Finally, we believe a deeper theoretical and empirical exploration into the nature of rally effects in general, and public trust in government in particular, is called for. As cyberattacks proliferate and states become digitised entities, the nature and origins of trust in government fit for a cyber era is a pressing issue. It is of utmost importance to examine whether a public facing national and threatening cyberattacks formulate their political opinion as a result of a deliberative weighing of administration's policies based on preexisting dispositions and media portrayals of the leadership (Baker and Oneal, 2001; Brody and Shapiro, 1991; Zaller, 1992) or whether the public formulate their political opinion as a mere emotionally charged political reflex (Hetherington and Nelson, 2003; Mueller, 1970).

## Acknowledgements

We extend a heartfelt thank you to Michael L. Gross, who supported the research efforts from their inception to conclusion, and to David Levi-Faur, Keren Levy-Ganany-Snider, and members of the Political Psychology Lab at the University of Haifa for their generous advice. This article benefited greatly from the feedback offered at a 2019 cyberterrorism symposium (Israel Institute) and a 2021 cyber conflict workshop (Israel Science Foundation) hosted by Daphna Canetti and Michael L. Gross at the University of Haifa. We appreciate the input of the article reviewers and the BJPIR editor, Jack Holland.

## Ethical standards


This study received IRB approval (235/18) from the University of Haifa Ethics Committee. In line with IRB requirements, respondents were first screened for past experiences of trauma. Respondents who reported post-traumatic stress symptoms or had recent experience with any form of trauma were excluded from the study.

## Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Israel Science Foundation (DC, grant number 594/15), the Center for Cyber Law & Policy at the University of Haifa in conjunction with the Israel National Cyber Directorate in the Prime Minister's Office (DC & RS), and the Maritime Policy & Strategy Research Center at the University of Haifa (SM), and a 270/21 and the ERC RegTrust /David Levi-Faur scholarship (SM).

## ORCID iDs

Sharon Matzkin  <https://orcid.org/0000-0002-8857-0133>

Ryan Shandler  <https://orcid.org/0000-0002-0931-2014>

## Supplemental material

Additional supplementary information may be found with the online version of this article.

Appendix A. Power analysis.

Appendix B. Pilot experiment – exposure to cyberattacks in newspaper vignettes.

Appendix C. Video manipulation scripts.

Appendix D. Balance checks for each terror condition in the United States, the United Kingdom, and Israel.

Appendix E. Comparisons, correlations, and estimates.

Appendix F. OLS hierarchical models of effect of attack type, anger and anxiety on trust in government.

Appendix G. SEM.

Appendix H. Scree plot and component matrix of the trust variable.

## Note

1. Items 2, 3, and 5 were reverse coded.

## References

- Backhaus S, Gross ML, Waismel-Manor I, et al. (2020) A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure. *Cyberpsychology, Behavior, and Social Networking* 23(9): 595–603.
- Baker WD and Oneal JR (2001) Patriotism or opinion leadership? The nature and origins of the ‘rally ’round the flag’ effect. *Journal of Conflict Resolution* 45(5): 661–687.
- Bandura A (2011) Moral disengagement. *The Encyclopedia of Peace Psychology*. Epub ahead of print 15 December. DOI: 10.1002/9780470672532.wbepp165.
- Baum MA (2002) The constituent foundations of the rally-round-the-flag phenomenon. *International Studies Quarterly* 46(2): 263–298.
- Ben-Nun Bloom P and Arikian G (2013) Religion and support for democracy: A cross-national test of the mediating mechanisms. *British Journal of Political Science* 43(2): 375–397.
- Berry MS, Baldwin ME, Samsa ME, et al. (2008) The effect of terrorism on public confidence: An exploratory study. *Argonne National Laboratory*. Available at: [https://papers.ssrn.com/sol3/papers.cfm?abstract\\_id=1337064](https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1337064) (accessed 30 October 2023).
- Bianco W (1994) *Trust: Representatives and Constituents*. Ann Arbor, MI: University of Michigan Press. Available at: [https://books.google.com/books?hl=en&lr=&id=d08d2Cy1IwC&oi=fnd&pg=PA1&ots=z nWnJ\\_9Tvy&sig=bEMFMdvTMexlMTCSOe1mumHRAEE](https://books.google.com/books?hl=en&lr=&id=d08d2Cy1IwC&oi=fnd&pg=PA1&ots=z nWnJ_9Tvy&sig=bEMFMdvTMexlMTCSOe1mumHRAEE) (accessed 30 October 2023).
- Bitton MS and Laufer A (2018) Children’s emotional and behavioral problems in the shadow of terrorism: The case of Israel. *Children and Youth Services Review* 86: 302–307.
- Brody RA and Shapiro CR (1991) The rally phenomenon in public opinion. In: Brody R (ed.) *Assessing the President: The Media, Elite Opinion, and Public Support*. Stanford, CA: Stanford University Press, pp.45–78.
- Bumiller E and Shanker T (2012) Panetta warns of dire threat of cyberattack on US. *The New York Times*, 11 October, p.A1.
- Byrne BM (1994) *Structural Equation Modeling with EQS and EQS/WINDOWS: Basic Concepts, Applications, and Programming*. Thousand Oaks, CA: Sage.
- Canetti D, Gross ML and Waismel-Manor I (2016) The psychological & physiological effects of cyberwar. In: Allhoff F, Henschke A and Strawser BJ (eds) *Binary Bullets: The Ethics of Cyberwarfare*. Oxford: Oxford University Press, pp.157–176.
- Canetti, D., Gubler, J., & Zeitzoff, T. (2021). Motives don’t matter? Motive attribution and counterterrorism policy. *Political Psychology* 42(3): 483–499.
- Canetti-Nisim D, Halperin E, Sharvit K, et al. (2009) A new stress-based model of political extremism: Personal exposure to terrorism, psychological distress, and exclusionist political attitudes. *Journal of Conflict Resolution* 53(3): 363–389.
- Crozier M, Huntington SP and Watanuki J (1975) *The Crisis of Democracy*, vol. 70. New York: New York University Press.
- Darwin C (1872) *The Expression of the Emotions in Man and Animals*. London: John Murray.
- Darwin C (1993) *The Portable Darwin*. London: Penguin Books, pp.364–393.
- Egloff F and Wenger A (2019) Public attribution of cyber incidents. *CSS Analyses in Security Policy* 244: 1–4.
- Egloff FJ and Dunn Cavelti M (2021) Attribution and knowledge creation assemblages in cybersecurity politics. *Journal of Cybersecurity* 7(1): tyab002.
- Feinstein Y (2018) One flag, two rallies: Mechanisms of public opinion in Israel during the 2014 Gaza war. *Social Science Research* 69: 65–82.
- Feinstein Y (2022) *Rally ’round the Flag: The Search for National Honor and Respect in Times of Crisis*. New York: Oxford University Press.
- Finlay L and Payne C (2019) The attribution problem and cyber armed attacks. *American Journal of International Law* 113: 202–206.
- Fisher J, Van Heerde-Hudson J and Tucker A (2011) Why both theory and empirics suggest there is more than one form of trust: A response to Hooghe. *British Journal of Politics and International Relations* 13(2): 276–281.
- Fisher J, Van Heerde J and Tucker A (2010) Does one trust judgement fit all? Linking theory and empirics. *British Journal of Politics and International Relations* 12(2): 161–188.
- Frey BS, Luechinger S and Stutzer A (2009) The life satisfaction approach to valuing public goods: The case of terrorism. *Public Choice* 138(3): 317–345.

- Garcia D and Rimé B (2019) Collective emotions and social resilience in the digital traces after a terrorist attack. *Psychological Science* 30(4): 617–628.
- Gartzke E (2021) Blood and robots: How remotely piloted vehicles and related technologies affect the politics of violence. *Journal of Strategic Studies* 44(7): 983–1013.
- Gelkopf M, Solomon Z and Bleich A (2013) A longitudinal study of changes in psychological responses to continuous terrorism. *Israel Journal of Psychiatry and Related Sciences* 50(2): 100–109.
- Getmansky A and Zeitoff T (2014) Terrorism and voting: The effect of rocket threat on voting in Israeli elections. *American Political Science Review* 108(3): 588–604.
- Godefroid A (2023) How terrorism does (and does not) affect citizens' political attitudes: A meta-analysis. *American Journal of Political Science* 67(1): 22–38.
- Gomez MA (2019) Past behavior and future judgements: Seizing and freezing in response to cyber operations. *Journal of Cybersecurity* 5(1): tyz012.
- Gomez MA and Villar EB (2018) Fear, uncertainty, and dread: Cognitive heuristics and cyber threats. *Politics and Governance* 6(2): 61–72.
- Gomez MA and Whyte C (2021) Breaking the myth of cyber doom: Securitization and normalization of novel threats. *International Studies Quarterly* 65(4): 1137–1150.
- Gross K, Brewer PR and Aday S (2009) Confidence in government and emotional responses to terrorism after September 11, 2001. *American Politics Research* 37(1): 107–128.
- Gross ML, Canetti D and Vashdi DR (2017) Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity* 3(1): 49–58.
- Guillon M and Kergall P (2020) Attitudes and opinions on quarantine and support for a contact-tracing application in France during the COVID-19 outbreak. *Public Health* 188: 21–31.
- Haber, E., & Reichman, A. (2020). The User, the Superuser, and the Regulator: Functional Separation of Powers and the Plurality of the State in Cyber. *Berkeley Tech. LJ* 35: 431.
- Halperin E (2014) Emotion, emotion regulation, and conflict resolution. *Emotion Review* 6(1): 68–76.
- Hardin R (2002) *Trust and Trustworthiness*. New York: Russell Sage Foundation.
- Hasler BS, Leshem OA, Hasson Y, et al. (2023) Young generations' hopelessness perpetuates long-term conflicts. *Scientific Reports* 13: 4926.
- Hetherington MJ (1998) The political relevance of political trust. *American Political Science Review* 92(4): 791–808.
- Hetherington MJ and Nelson M (2003) Anatomy of a rally effect: George W. Bush and the war on terrorism. *PS: Political Science & Politics* 36(1): 37–42.
- Hirsch-Hoefler S, Canetti D, Rapaport C, et al. (2016) Conflict will harden your heart: Exposure to violence, psychological distress, and peace barriers in Israel and Palestine. *British Journal of Political Science* 46(4): 845–859.
- Hobfoll SE, Canetti-Nisim D and Johnson RJ (2006) Exposure to terrorism, stress-related mental health symptoms, and defensive coping among Jews and Arabs in Israel. *Journal of Consulting and Clinical Psychology* 74(2): 207–218.
- Holland J (2021) 9/11 and critical terrorism studies – the emotion, culture, and discourse of the 'war on terror'. *Critical Studies on Terrorism* 14(4): 441–444.
- Holland J and Jarvis L (2014) 'Night fell on a different world': Experiencing, constructing and remembering 9/11. *Critical Studies on Terrorism* 7(2): 187–204.
- Hooghe M (2011) Why there is basically only one form of political trust. *British Journal of Politics and International Relations* 13(2): 269–275.
- Horne CM (2017) Trust and transitional justice. In: Horne CM (ed.) *Building Trust and Democracy: Transitional Justice in Post-Communist Countries* (Online Edition). New York: Oxford Academic, pp.23–55.
- Hu L and Bentler PM (1999) Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal* 6(1): 1–55.
- Huddy L and Feldman S (2011) Americans respond politically to 9/11: Understanding the impact of the terrorist attacks and their aftermath. *American Psychologist* 66(6): 455–467.
- Huddy L, Feldman S and Casese E (2009) 14 Terrorism, anxiety, and war. In: Stritzke W GK, Lewandowsky S and Denmark D (eds) *Terrorism and Torture*. Cambridge: Cambridge University Press, pp.290–312.
- Huddy L, Feldman S and Weber C (2007) The political consequences of perceived threat and felt insecurity. *The Annals of the American Academy of Political and Social Science* 614(1): 131–153.
- Huddy L, Khatib N and Capelos T (2002) Trends: Reactions to the terrorist attacks of September 11, 2001. *Public Opinion Quarterly* 66(3): 418–450.
- Huddy L, Smirnov O, Snider KLG, et al. (2021) Anger, anxiety, and selective exposure to terrorist violence. *Journal of Conflict Resolution* 65(10): 1764–1790.



- Itzhaky L, Gelkopf M, Levin Y, et al. (2017) Psychiatric reactions to continuous traumatic stress: A latent profile analysis of two Israeli samples. *Journal of Anxiety Disorders* 51: 94–100.
- Jarvis L, Macdonald S and Whiting A (2017) Unpacking cyberterrorism discourse: Specificity, status, and scale in news media constructions of threat. *European Journal of International Security* 2(1): 64–87.
- Kaminska M (2021) Restraint under conditions of uncertainty: Why the United States tolerates cyberattacks. *Journal of Cybersecurity* 7(1): tyab008.
- Kernell S (1978) Explaining presidential popularity: How ad hoc theorizing, misplaced emphasis, and insufficient care in measuring one's variables refuted common sense and led conventional wisdom down the path of anomalies. *American Political Science Review* 72(2): 506–522.
- Kimhi S (2016) Levels of resilience: Associations among individual, community, and national resilience. *Journal of Health Psychology* 21(2): 164–170.
- Kimhi S, Marciano H, Eshel Y, et al. (2020) Community and national resilience and their predictors in face of terror. *International Journal of Disaster Risk Reduction* 50: 101746.
- Kline RB (2015) *Principles and Practice of Structural Equation Modeling*. New York: Guilford publications.
- Kostyuk N and Wayne C (2021) The microfoundations of state cybersecurity: Cyber risk perceptions and the mass public. *Journal of Global Security Studies* 6(2): ogz077.
- Kreps S and Schneider J (2019) Escalation firebreaks in the cyber, conventional, and nuclear domains: Moving beyond effects-based logics. *Journal of Cybersecurity* 5(1): tyz007.
- Kuehl D (2007) The information revolution and the transformation of warfare. In: Bergstra J and de Leeuw K (eds) *The History of Information Security*. Amsterdam: Elsevier, pp.812–832.
- Larsen JT and McGraw AP (2011) Further evidence for mixed emotions. *Journal of Personality and Social Psychology* 100(6): 1095–1110.
- Lawson ST (2019) *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. London: Routledge.
- Leal M and Musgrave P (2022) Cheerleading in cyberspace: How the American public judges attribution claims for cyberattacks. *Foreign Policy Analysis* 18(2): orac003.
- Leal MM and Musgrave P (2023a) Backwards from zero: How the US public evaluates the use of zero-day vulnerabilities in cybersecurity. *Contemporary Security Policy* 44: 437–461.
- Leal M and Musgrave P (2023b) Hitting back or holding back in cyberspace: Experimental evidence regarding Americans' responses to cyberattacks. *Conflict Management and Peace Science* 40: 42–64.
- Lerner JS and Keltner D (2000) Beyond valence: Toward a model of emotion-specific influences on judgement and choice. *Cognition and Emotion* 14(4): 473–493.
- Lerner JS and Keltner D (2001) Fear, anger, and risk. *Journal of Personality and Social Psychology* 81(1): 146–159.
- Lerner JS and Tiedens LZ (2006) Portrait of the angry decision maker: How appraisal tendencies shape anger's influence on cognition. *Journal of Behavioral Decision Making* 19(2): 115–137.
- Lerner JS, Gonzalez RM, Small DA, et al. (2003) Effects of fear and anger on perceived risks of terrorism: A national field experiment. *Psychological Science* 14(2): 144–150.
- Levi M and Stoker L (2000) Political trust and trustworthiness. *Annual Review of Political Science* 3(1): 475–507.
- Li M, Leidner B, Fernandez-Campos S, et al. (2016) Stepping into perpetrators' shoes: How ingroup transgressions and victimization shape support for justice through perspective taking of perpetrators. *Personality and Social Psychology Bulletin* 46: 424–438.
- Libicki MC (2009) *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND corporation.
- Liverant GI, Hofmann SG and Litz BT (2004) Coping and anxiety in college students after the September 11th terrorist attacks. *Anxiety, Stress, & Coping* 17(2): 127–139.
- Lowry PB and Gaskin J (2014) Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication* 57(2): 123–146.
- Lynn IIIWF (2010) Defending a new domain-the Pentagon's cyberstrategy. *Foreign Affairs* 89: 97–108.
- Macdonald S, Jarvis L and Lavis SM (2022) Cyberterrorism today? Findings from a follow-on survey of researchers. *Studies in Conflict & Terrorism* 45: 727–752.
- Marcus GE, Neuman WR and MacKuen M (2000) *Affective Intelligence and Political Judgment*. Chicago, IL: University of Chicago Press.
- Maschmeyer L (2023) A new and better quiet option? Strategies of subversion and cyber conflict. *Journal of Strategic Studies* 46: 570–594.
- McDermott R (2019) Some emotional considerations in cyber conflict. *Journal of Cyber Policy* 4(3): 309–325.



- Memon MA, Jun HC, Ting H, et al. (2018) Mediation analysis issues and recommendations. *Journal of Applied Structural Equation Modeling* 2(1): i–ix.
- Mueller JE (1970) Presidential popularity from Truman to Johnson. *American Political Science Review* 64(1): 18–34.
- Muldoon O (2003) The psychological impact of protracted campaigns of political violence on societies. In: Silke A (ed.) *Terrorists, Victims and Society: Psychological Perspectives on Terrorism and Its Consequences*. Hoboken, NJ: John Wiley & Sons, pp.161–174.
- Nussio E (2020) Attitudinal and emotional consequences of Islamist terrorism: Evidence from the Berlin attack. *Political Psychology* 41(6): 1151–1171.
- Nye JS Jr (2010) *Cyber Power*. Cambridge MA: Belfer Center for Science and International Affairs, Harvard University.
- OECD (2022) *Building Trust to Reinforce Democracy*. Paris: OECD.
- Ostrom CW Jr and Simon DM (1989) The man in the Teflon suit? The environmental connection, political drama, and popular support in the Reagan presidency. *Public Opinion Quarterly* 53(3): 353–387.
- Perrin AJ and Smolek SJ (2009) Who trusts? *Race, gender, and the September 11 rally effect among young adults*. *Social Science Research* 38(1): 134–145.
- Pliskin R, Ruhrman A and Halperin E (2020) Proposing a multi-dimensional, context-sensitive approach to the study of ideological (a) symmetry in emotion. *Current Opinion in Behavioral Sciences* 34: 75–80.
- Ronen T, Rahav G and Appel N (2003) Adolescent stress responses to a single acute stress and to continuous external stress: Terrorist attacks. *Journal of Loss and Trauma* 8(4): 261–282.
- Schneider J (2020) A strategic cyber no-first-use policy? Addressing the US cyber strategy problem. *The Washington Quarterly* 43(2): 159–175.
- Schneider J (2022) A world without trust. *Foreign Affairs*. Available at: <https://www.foreignaffairs.com/articles/world/2021-12-14/world-without-trust> (accessed 15 April 2022).
- Scholz JT and Lubell M (1998) Trust and taxpaying: Testing the heuristic approach to collective action. *American Journal of Political Science* 42: 398–417.
- Shandler R and Gomez MA (2023) The hidden threat of cyber-attacks – Undermining public confidence in government. *Journal of Information Technology & Politics* 20: 359–374.
- Shandler R, Gross ML and Canetti D (2023a) Cyberattacks, psychological distress, and military escalation: An internal meta-analysis. *Journal of Global Security Studies* 8(1): ogac042.
- Shandler R, Gross ML, Backhaus S, et al. (2022) Cyber terrorism and public support for retaliation – A multi-country survey experiment. *British Journal of Political Science* 52: 850–868.
- Shandler R, Kostyuk N and Oppenheimer H (2023b) Public opinion and cyberterrorism. *Public Opinion Quarterly* 87(1): 92–119.
- Shechory Bitton M and Silawi Y (2019) Do Jews and Arabs differ in their fear of terrorism and crime? *Journal of Interpersonal Violence* 34(19): 4041–4060.
- Sinclair SJ and LoCicero A (2007) Fearing future terrorism: Development, validation, and psychometric testing of the Terrorism Catastrophizing Scale (TCS). *Traumatology* 13(4): 75–90.
- Skocpol T (2002) Will 9/11 and the war on terror revitalize American civic democracy? *PS: Political Science & Politics* 35(3): 537–540.
- Snider LGK, Shandler R and Zandani Shay Canetti D (2021) Cyber terrorism, cyber threats and attitudes toward cybersecurity policies. *Journal of Cybersecurity* 7: tyab019.
- Snider LGK, Shandler R, Matzkin S and Canetti D (2023) *The Political Psychology of Terrorism*. The Political Psychology of Terrorism. Oxford: Oxford University Press.
- Spielberger CD (1972) Anxiety as an emotional state. In: Spielberger CD (ed.) *Anxiety-Current Trends and Theory*. New York: Academic Press, pp.23–49.
- Spielberger CD, Jacobs G, Russell S, et al. (1983) Assessment of anger: The state-trait anger scale. *Advances in Personality Assessment* 2: 161–189.
- Valeriano BG and Jenson B (2019) The myth of the cyber offense: The case for cyber restraint. *Cato Institute Policy Analysis* 862: 1–16.
- Van der Meer TWG (2017) Political trust and the ‘crisis of democracy’. In: Thompson WR (ed.) *Oxford Research Encyclopedia of Politics*. Oxford: Oxford University Press, pp.1–23. Available at: <https://oxfordre.com/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-77> (accessed 16 November 2019).
- Van Schaik P, Jeske D, Onibokun J, et al. (2017) Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior* 75: 547–559.
- Vasilopoulos P, Marcus GE, Valentino NA, et al. (2019) Fear, anger, and voting for the far right: Evidence from the November 13, 2015 Paris terror attacks. *Political Psychology* 40(4): 679–704.

- Wang Z, Liu H, Li T, et al. (2023) The impact of internet use on citizens' trust in government: The mediating role of sense of security. *Systems* 11(1): 47.
- Waxman D (2011) Living with terror, not living in terror: The impact of chronic terrorism on Israeli society. *Perspectives on Terrorism* 5(5/6): 4–26.
- Woods J (2011) The 9/11 effect: Toward a social science of the terrorist threat. *The Social Science Journal* 48(1): 213–233.
- You Y and Wang Z (2020) The Internet, political trust, and regime types: A cross-national and multilevel analysis. *Japanese Journal of Political Science* 21(2): 68–89.
- Zaller J (1992) *The Nature and Origins of Mass Opinion*. Cambridge: Cambridge university press.
- Zhang B, Kreps S, McMurry N, et al. (2020) Americans' perceptions of privacy and surveillance in the COVID-19 pandemic. *PLoS ONE* 15(12): e0242652.
- Zhao X, Lynch Jr JG and Chen Q (2010) Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research* 37(2): 197–206.

Copyright of British Journal of Politics & International Relations is the property of Sage Publications Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.