

ARTICLE

Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment

Ryan Shandler^{1*} , Michael L. Gross¹ , Sophia Backhaus²  and Daphna Canetti¹ 

¹School of Political Sciences, University of Haifa, Haifa, Israel and ²Department of Psychology, University of Konstanz, Konstanz, Germany

*Corresponding author. E-mail: jshandler@staff.haifa.ac.il

(Received 14 May 2020; revised 15 September 2020; accepted 19 November 2020; first published online 10 February 2021)

Abstract

Does exposure to cyber terrorism prompt calls for retaliatory military strikes? By what psychological mechanism does it do so? Through a series of controlled, randomized experiments, this study exposed respondents ($n = 2,028$) to television news reports depicting cyber and conventional terror attacks against critical infrastructures in the United States, United Kingdom and Israel. The findings indicate that only *lethal* cyber terrorism triggers strong support for retaliation. Findings also confirm that anger bridges exposure to cyber terrorism and retaliation, rather than psychological mechanisms such as threat perception or anxiety as other studies propose. These findings extend to the cyber realm a recent trend that views anger as a primary mechanism linking exposure to terrorism with militant preferences. With cyber terrorism a mounting international concern, this study demonstrates how exposure to this threat can generate strong public support for retaliatory policies, depending on the lethality of the attack.

Keywords: cyber terrorism; terrorism; retaliatory strikes; foreign policy preferences; critical infrastructure; anger

Security officials have long warned of the foreboding threat posed by cyber terrorism. In recent years, following a spate of reports about next-generation cyber attacks causing real-world physical destruction, this threat has come of age. For example, a devastating cyber attack in 2020 on a German hospital led to the death of a patient who had to be urgently transferred to another hospital (Tidy 2020). Several months earlier, Iranian-affiliated operatives launched a cyber attack that successfully breached the control systems of Israel's civilian water infrastructure (Heller 2020), while Russian cyber operatives have frequently managed to digitally infiltrate power plants across the United States – attaining the ability to remotely control key components of the electricity grid (Sanger 2018). Scholars have thus heralded the dawn of 'Kinetic Cyber' – the 'credible capability to use cyber attacks to achieve kinetic effects' (Applegate 2013, 3).

The scope of the threat posed by this alarming new phenomenon, especially against critical infrastructure, was elucidated most prominently by former CIA Director and US Secretary of Defense Leon Panetta, when he insisted that the world was 'facing the possibility of a 'cyber-Pearl Harbor' [that] could dismantle the nation's power grid, transportation system, financial networks and government' (Bumiller and Shanker 2012). Even as skeptics question what is commonly viewed as a hyperbolic depiction of this threat (Lawson 2019; Gartzke 2013; Valeriano and Maness 2015), there is mounting evidence that terror organizations are adopting cyber tools to launch increasingly sophisticated attacks (Lee et al. forthcoming), and significant cyber attacks on critical infrastructure have increased tenfold during the last decade (Noguchi and Ueda 2019). In the shadow of this debate, the public continues to exhibit mounting

© The Author(s), 2021. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted re-use, distribution, and reproduction in any medium, provided the original work is properly cited.

trepidation about the destructive capacity of cyber terrorism. Recent Gallup polls find that the American public views cyber terrorism as the third-most critical threat to the United States over the next decade – ahead of Chinese military power, conflict in the Middle East or international (conventional) terrorism (McCarthy 2016; Norman 2018).

The rise of the phenomenon of a newly physically destructive cyber threat raises significant new questions for political science that are, unfortunately, likely to become increasingly relevant as this threat matures. How does exposure to cyber attacks affect political preferences and support for government actions? By what mechanism does exposure lead to shifts in political attitudes, and how does this differ from shifts stemming from conventional terrorism and political violence? New theories and models relating to cyber terrorism have been developed in the fields of law (Schmitt 2017), foreign policy and strategic studies (Clarke 2016; Herzog 2011) and psychology (Backhaus et al. 2020; Gross, Canetti and Vashdi 2018), yet equivalent models are conspicuously absent in political science.

An emerging body of research has begun to contemplate the political consequences of cyber attacks (Gross, Canetti and Vashdi 2017; 2016; Hua, Chen and Luo 2018), but it is still in its infancy. By contrast, it is well established that exposure to *conventional* terror attacks causes heightened threat perception (Berrebi and Klor 2008; Canetti et al. 2017a; Canetti et al. 2017b), anxiety (McDermott and Zimbardo 2007), in-group solidarity and out-group exclusion (Canetti-Nisim, Ariely and Halperin 2008), and increased demands for government protection and retaliatory policies to defend against future attacks (McDermott and Zimbardo 2007). However, there is limited evidence regarding whether individuals react to cyber terror attacks in the same way. It is reasonable to assume that conventional or cyber terror attacks that produce the same outcome will generate an equivalent reaction in victims. Alternatively, the specter of cyber terrorism may amplify the terror response due to the novelty of the form of attack, the omniscience often associated with cyber operators and uncertainty about the identity of cyber attackers. Still another prospect is that exposure to cyber terrorism may elicit a weaker political response than conventional terrorism due to the lack of historical fatalities associated with cyber attacks. The current study addresses this uncertainty by conducting a methodologically rigorous examination of how civilians experience cyber terrorism in its various forms.

Our empirical evidence verifies that cyber terrorism causes political shifts that are distinct from those generated by conventional terrorism. We examine the political effects of exposure to cyber terrorism using a series of randomized controlled experiments in three countries – the United States, United Kingdom and Israel. Following two experimental pilots, a culminating experiment exposed 1,848 respondents in the three countries to various forms of terror attacks. These controlled experiments tested how (1) the form of terrorism (conventional kinetic terror vs. cyber terror) and (2) the outcome of terrorism (lethal vs. non-lethal effects) influence support for military retaliation. The findings demonstrate that the level of support for retaliatory strikes differs significantly according to the type of terror to which respondents are exposed. Support for retaliatory strikes is substantially lower among participants who viewed cyber terror attacks as opposed to conventional terror attacks, but only when the consequences of the cyber attack are non-lethal. When cyber attacks do cause fatalities, then support for retaliation is just as high as with conventional terror attacks. We therefore observe a *lethality threshold* for cyber terrorism effects, wherein the outcome of the attack must meet a minimum level of destructiveness in order to produce political outcomes equivalent to those of conventional terrorism. Secondly, we confirm that the mechanism underpinning the relationship between exposure to cyber terrorism and support for retaliation is driven by a mediated model: exposure to terrorism causes anger, which in turn drives political support for retaliation. This conclusion extends to the cyber realm recent findings that view anger, and not anxiety or threat perception, as the predominant variable linking political violence and militant attitudes.

Political Consequences of Exposure to Cyber Terrorism

Two decades of research have thoroughly identified how exposure to political violence in general, and terrorism in particular, markedly shapes political preferences and behaviors. Moving beyond the early studies that used aggregate-level data to consider the effects of exposure to terrorism, newer studies now integrate the psychological and emotional consequences of exposure into political models that explain particular attitudinal shifts at the individual level. This research established that exposure to conventional terrorism undermines one's sense of security and heightens feelings of vulnerability (Huddy *et al.* 2005; Neria, DiGrande and Adams 2011; Silver *et al.* 2002), fosters a threatening worldview and increases support for hardline policies (Bleich, Gelkopf and Solomon 2003; Bonanno and Jost 2006), causes a rightward shift on security and privacy issues (Janoff-Bulman and Usoof-Thowfeek 2009) and leads to increased demands for governments to take strong military action against terror groups (McDermott 2010).

A recurring political effect of interest in the literature is public support for military retaliation against perpetrators. This variable is of interest since scholars have slowly come to agree that public opinion has at least a measurable impact on decisions about whether to engage in sustained military operations, and many international relations theories of conflict implicitly incorporate micro-level processes (Foyle 2004; Kertzer 2017; Klarevas 2002; Sobel 2001).

Yet the literature offers competing evidence about how exposure to political violence translates into support for retaliation. On the one hand, the fear and anxiety caused by exposure to terror attacks enhance support for precautionary (surveillance) policies, and lower support for military action (Huddy *et al.* 2005; Lerner *et al.* 2003). On the other hand, exposure to terrorism increases individuals' tendency to vote for right-wing candidates and to engage in risk-seeking behaviors (Berrebi and Klor 2008; Gould and Klor 2010; Jaeger and Paserman 2008; Montalvo 2011). These behaviors are reflected in the tendency to develop more negative out-group sentiments and to intensify demands on governments to initiate strong military action (Sadler *et al.* 2005). The differences in exposure effects reflect the multifaceted nature of political policy preferences. A person can simultaneously experience vulnerability and express support for precautionary policies, while at the same time advocate strong military responses out of a sense of injustice or anger. These ostensibly different findings reflect the particular focus of each study.

The variable of support for retaliation is of particular interest in analyzing the effects of cyber terrorism, since the characteristics of this form of terrorism may alter the findings traditionally associated with conventional exposure. One major difference is the difficulty associated with attributing responsibility, which is a characteristic of cyber attacks, and could dampen the effectiveness and attractiveness of retaliatory strikes (Brenner 2006; Lindsay 2015). Jardine and Porter (2020) found that the presence of ambiguity in attributing cyber attacks severely reduces public support for retaliatory options. Kreps and Das (2017) concluded that bipartisan assessments of attribution following cyber attacks can mitigate this lower support, while the consequences of cyber attacks are a key aspect of support for retaliatory airstrikes. Another major difference is that cyber terrorism has not hitherto threatened civilians' physical safety in the same way as conventional terrorism. The perceived lethality of the terror attack is critical for understanding its impact since most people are threatened by (rather than directly exposed to) the terror act, and the perception of lethality is an important factor in its individual-level impact (Getmansky and Zeitsoff 2014). The limited danger of cyber attacks has become a characteristic feature in discussions of the phenomenon, and it would make sense that cyber terrorism is experienced and perceived differently than other forms of terror acts that bear the possibility and even likelihood of fatal consequences. Finally, civilians could seek safety in their homes, bomb shelters or in other countries to attain a sense of security from traditional terror attacks. Yet similar attempts to protect oneself are less effective in the face of cyber attacks, where perpetrators can break into digital devices irrespective of geographic proximity.

The important factor in examining the public response to terror attacks is not the objective analysis of substantive differences between cyber terrorism and conventional terrorism, but the

manner in which they are *subjectively perceived* by citizens who are exposed to attacks. Research by Tomz and Weeks (2016) and Kreps and Schneider (2019) found that the public is loath to escalate aggressively in response to cyber attacks, even if the effect is equivalent to that of conventional attacks. Their research theorized that individuals experience cognitive dissonance following exposure to cyber attacks since the natural inclination for vengeance is counteracted by the virtual qualities of the cyber sphere that are associated with lower levels of threat. Our research builds on these foundational studies by concentrating on cyber terrorism in particular, rather than cyber attacks generally. This focus is important because the primary threat of exposure to destructive cyber attacks is via terrorism (Albahar 2019), and an individual's response to an external threat cannot be separated from the conceptualization of the attacker. Under this terror-centric framework, we take into account a number of competing variables, including the nature of the attack (cyber vs. conventional (kinetic) means) and its lethality. We advance the following two hypotheses:

HYPOTHESIS 1: People who are exposed to cyber terrorism will demand retaliation at lower levels than those exposed to kinetic terrorism.

HYPOTHESIS 2: People who are exposed to fatal terrorism will demand retaliation at higher levels than those who are exposed to non-fatal terrorism – regardless of the form of attack (cyber vs. conventional).

Theorizing Anger as a Mechanism

Anger is 'an emotional state that consists of feelings that vary in intensity, from mild irritation or annoyance to intense fury and rage' (Spielberger, Reheiser and Sydeman 1995). Anger is often driven by a desire to correct a perceived injustice or unfairness (Fischer and Roseman 2007; Halperin et al. 2011). Cyber and conventional terror attacks that directly transgress norms regarding the use of force are especially likely to evoke anger and a desire for retaliatory strikes – even if the threat was not experienced on a personal level.

The theory of emotionally driven foreign policy preferences in the aftermath of political violence is well established. In the aftermath of conventional terror attacks, we know that a variety of negative emotions (anger, rage, sadness, etc.) enhance support for aggressive foreign policy responses (Kupatadze and Zeitzoff 2019; Lerner et al. 2003; Small, Lerner and Fischhoff 2006). Yet how does this mechanism translate to the phenomenon of cyber terrorism specifically? It could be that cyber terrorism will cause high levels of emotional responses due to the novelty of this form of attack, lower levels due to low subjective predictions of the likelihood of harm, or the same level of anxiety due to a perceived equivalence between cyber and conventional terror.

Experimental research has identified causal pathways between exposure to terrorism and political outcomes with various intervening emotional variables such as fear and anxiety (Huddy et al. 2005; Lerner et al. 2003; Skitka et al. 2006), threat perception (Huddy et al. 2002; Kupatadze and Zeitzoff 2019; Stevens and Vaughan-Williams 2016; Wayne 2019) and sadness (Nussio 2020). While fear and anxiety are a common response to exposure to terrorism, these do not always translate into heightened support for military retaliation or other corrective political acts, since fear is elicited primarily by attacks that are personally experienced (Haidt 2003; Huddy et al. 2005). Likewise, the literature suggests that the intervening effect of threat perception is minimized in cases of limited information, such as with cyber terrorism (Egloff 2020). However, most recent research has identified that 'the dominant response of civilian populations to terror threat is not fear and a desire to reduce future personal risk, but rather anger and a desire for vengeance' (Wayne 2019, 5). Exposure to terror events is typically and understandably

accompanied by anger (Carver 2004; Hirsch-Hoefler *et al.* 2016; Lerner *et al.* 2003; Steele, Parker and Lickel 2015). In the case of terrorism especially, anger is more likely to intervene in any retaliation-centric mechanism since it is linked to more superficial and heuristic-based cognitive processing that is associated with aggressive policy options (Bodenhausen, Sheppard and Kramer 1994; Sirin and Geva 2013). Indeed, one recent multi-country study found that only respondents who expressed anger following exposure to a terrorist threat become more supportive of drone strikes against terrorists (Fisk, Merolla and Ramos 2019).

This literature poses a conceptual dilemma in applying its conclusions to the phenomenon of cyber terrorism due to the absence of physically present perpetrators and the difficulty of attributing attacks to a source. Anger is typically associated with wielding a sense of control, yet this raises questions about how people express their anger if the perpetrator is unknown – a common occurrence in the cyber realm. Cyber terrorism is certainly more nebulous, abstract, and difficult to connect cause with effect compared to conventional terrorism, of which there is typically visceral and direct evidence. Nonetheless, we assert that anger maintains its potency in regulating foreign policy preferences in these situations for the following reasons. A persuasive line of research has identified how anger can lead to a generalized desire for revenge and retribution – even when there is uncertainty as to the identity of the attacker, or when the target is symbolically similar to the perpetrator (Lieberman and Skitka 2017; Lieberman and Skitka 2019; Washburn and Skitka 2015). These findings draw on social psychological theories to demonstrate the political equivalent of ‘displaced aggression’ – a tendency to express heightened support for aggressive action against tangentially related third parties in the aftermath of attacks. Essentially, this theory demonstrates that anger can lead to a general increase in punitive inclinations, and that anger need not be directed against a specific target in order to heighten support for retaliation. This vicarious retribution theory is especially useful in analyzing exposure to cyber terrorism, where the identity of the attacker is often unknown or uncertain. The theory explains how the experience of anger translates into heightened general punitive impulses against unrelated offenders (Lieberman and Skitka 2019) or symbolically similar out-groups to whom responsibility is imputed (Lieberman and Skitka 2017; Washburn and Skitka 2015).

We assert that weighing these factors, the political effects of exposure to cyber terrorism are most closely related to the anger emotion and its association with aggressive policy preferences. Following this pathway, we hypothesize that:

HYPOTHESIS 3: Preferences for retaliatory strikes following both cyber and conventional terror attacks will be mediated by anger, and not by anxiety or a sense of perceived threat.

A Three-Country Survey Experiment

To test these hypotheses, we ran a series of controlled, randomized survey experiments that simulated television news reports about different forms of terror attacks in the United States, United Kingdom and Israel. The experimental manipulation relied on professionally produced original video clips that broadcast breaking news reports showing various forms of terror attacks on railway infrastructure. Recent experiments have shown that exposure to broadcast videos and media reports of terror attacks are sufficient to cause shifts in levels of anxiety, anger and political attitudes (Backhaus *et al.* 2020; Shandler, Gross and Canetti, 2021; Shoshani and Slone 2008). We further submit that high-quality, professionally produced television news reports are more ecologically valid and authentic than comparatively sterile vignettes that seem to be the norm in many survey experiments on terrorism and political violence. To further substantiate this belief, we ran a pilot experiment ($n = 180$) that affirmed that exposure to breaking news media reports depicting terror attacks against train networks causes substantial variance in emotional and political responses depending on the type of terror attack. (The analyses and media reports for this pilot dataset appear in Appendix A).




We randomly assigned respondents ($n = 1,848$ among the three countries) to one of five conditions in a 2×2 experimental design with a control group. There were four treatment conditions: (1) *Lethal Cyber Terrorism Condition* – a cyber terror attack by an as-yet-unidentified perpetrator caused a train to derail, killing seven passengers and critically injuring another ten; (2) *Lethal Conventional Terrorism Condition* – the same outcome was caused by a conventional terror attack; (3) *Non-Lethal Cyber Terrorism Condition* – a cyber terror attack by an as-yet-unidentified perpetrator targeted a railway network, leading to the theft of tens of millions of dollars from passengers' credit cards and (4) *Non-Lethal Conventional Terrorism Condition* – the same non-fatal outcome was perpetrated using conventional terror means. A fifth control condition did not utilize any news stories or refer to the train system in any way. The experiment therefore manipulates forms of terror attacks on two axes: the type of attack (cyber vs. conventional) and the consequences of the attack (lethal vs. financial). (See [Table 1](#) for an overview of the conditions, and [Appendix B](#) for complete scripts and screenshots). The hyper-realistic video news story was identical in each country, adapted only to refer to local cities and railway companies, and with the relevant introductory special alert animation and logo of the broadcaster. Every other element remained identical – including the news presenter.

The news clips purported to broadcast on local news stations in the three countries – NBC News in the United States, Sky News in the United Kingdom and Channel 2 in Israel. These outlets were selected due to their standing as nationally syndicated news outlets, with among the highest and most bipartisan levels of public trust. (Although it may be more accurate to describe them as possessing the least lousy levels of public trust). NBC News, for example, is one of only three nationally broadcast television news sources that is trusted by more than 30 per cent of both Republicans and Democrats (Pew Research Center 2020). Sky News, likewise, is ranked as one of the three most trusted UK news brands (Nielsen, Schulz and Fletcher 2020). Unlike the BBC, for example, which has significant variance in trust levels according to political identity, Sky News possesses highly consistent perceptions along the full ideological spectrum (Nielsen, Schulz and Fletcher 2020). In Israel, a smaller media market, there is less scholarship on public trust in the various media outlets. Yet Channel 2, before it was split into competing broadcasters, was the largest and most authoritative news source with an audience share of above 20 per cent – double the next highest national news network (Dorot 2020).

While acknowledging the thriving literature on partisanship in the ascription of trustworthiness in media outlets, we note that this methodology abides by the highest levels of ecological validity in that the public is exposed to terror attacks via news reports that are not devoid of pre-conceived notions of credibility. We contend with this challenge by controlling for relevant variables that influence trust (political identity, age, etc.) and work to minimize these effects by abiding by the principle of specificity in producing the news reports, a feature that is associated with accuracy and eliciting high levels of concern in cyber terrorism reporting (Jarvis, Macdonald and Whiting 2017). We are further comforted by prior empirical research emphasizing the fact that professionalism and expertise in the production of television news segments is a more significant factor in imputing credibility and emotional resonance than the broadcaster label (Tewksbury, Jensen and Coe 2011). The script was translated and back translated to ensure cross-language consistency.

After viewing the video treatment, respondents completed a detailed questionnaire exploring their emotional state, political attitudes and demographic information. The dependent variable of interest in this study was support for retaliation policies, which was measured using an adapted six-item summative index from Graves, Acquisti and Anderson (2014). Respondents were asked to indicate their support for various military and diplomatic responses to attacks on the soil of their respective countries. Retaliatory options included cyber and conventional military attacks on military and civilian targets, economic sanctions and diplomatic maneuvers. (For example, 'To what extent do you support missile strikes against military targets of the attacker? To what extent do you support freezing the attackers' bank accounts and imposing economic sanctions?')

Table 1. Description of treatment conditions

Treatment condition	Method of attack	Consequences of attack	Screenshot from breaking news report
Lethal cyber terrorism	Cyber attack	The attack caused a train to derail causing the deaths of 7 passengers and causing injuries to an additional 10 passengers	 <p>A screenshot from a news report showing a train derailed on a track. A carriage is tilted at a steep angle. The news banner at the bottom reads "BREAKING NEWS CYBER TERROR ATTACK ON NATIONAL RAIL; 7 DEAD".</p>
Non-lethal cyber terrorism	Cyber attack	The attack targeted railway headquarters leading to the theft of tens of millions of dollars from passengers' credit cards.	 <p>A screenshot from a news report showing the interior of a railway station. A large sign for "Krnib" is visible. The news banner at the bottom reads "BREAKING NEWS CYBER TERROR ATTACK ON NATIONAL RAIL; MILLIONS STOLEN".</p>
Lethal conventional terrorism	Conventional attack	The attack caused a train to derail causing the deaths of 7 passengers and causing injuries to an additional 10 passengers	 <p>A screenshot from a news report showing a train derailed on a track. A carriage is tilted at a steep angle. The news banner at the bottom reads "BREAKING NEWS TERROR ATTACK ON NATIONAL RAIL; 7 DEAD".</p>
Non-lethal conventional terrorism	Conventional attack	The attack targeted railway headquarters leading to the theft of tens of millions of dollars from passengers' credit cards.	 <p>A screenshot from a news report showing the interior of a railway station. A large sign for "Krnib" is visible. The news banner at the bottom reads "BREAKING NEWS TERROR ATTACK ON NATIONAL RAIL; MILLIONS STOLEN".</p>
Control	N/A	Did not view any video	Did not view any video

Note: screenshots are taken from the UK news reports.

All questions were rated on a scale of 1 (not at all) to 6 (absolutely), and post-hoc analyses showed the scale to be highly reliable (Cronbach's $\alpha = 0.80$).

Anger, the hypothesized mediating variable, was measured with the shortened version of the commonly used STAXI measure (State-Trait Anger Expression Inventory, Spielberger 1988), comprised of four items that assess the intensity of anger at a particular moment in time. Respondents rated items on a scale of 1–6 (1 = not at all; 6 = absolutely). The inventory is scored as the total mean of all items, with higher scores reflecting higher levels of anger (Cronbach's $\alpha = 0.96$).

Anxiety was measured using the short-form Spielberger state-anxiety inventory-6 (Marteau and Bekker 1992; Spielberger 1970). This commonly used six-item index measures both state (extrinsic) and trait (intrinsic) anxiety. Respondents were asked to rate on a scale of 1–6 (1 = not at all; 6 = absolutely) the extent to which their feelings 'at the moment' corresponded to different items. Half of the items represented negative feelings and emotions (for example, 'I feel upset', 'I feel worried') and the other half represented positive feelings and emotions (for example, 'I feel relaxed', 'I feel content') (Cronbach's $\alpha = 0.88$).

In accordance with standard methodological practices, and to avoid the pitfalls of confound and unseen interaction effects, the dependent variable measures were placed in the survey immediately after respondents were exposed to the experimental treatment. Other covariates collected included age, gender, level of education, political self-identification, family income, average daily Internet usage, computer literacy and usage of public transportation. All demographic covariates were collected at the end of the survey.

Participants and Countries

The questionnaires were distributed simultaneously in the three countries from 14–17 October 2018. The survey was distributed using three Internet survey platforms – Amazon Turk, Prolific and Midgam – in the US, UK and Israel, respectively. (See Appendix C for a discussion of the advantages and shortcomings of the selected survey panels). At the outset of the surveys, respondents were told that they were to view an authentic video news story and answer several questions. In line with restraints imposed by the Institutional Review Board (IRB), respondents diagnosed with post-traumatic stress disorder symptoms or having experienced trauma during the preceding two years were excluded from participating in the survey. An attention check was conducted following the video manipulation, leading to the exclusion of sixteen respondents (0.8 per cent of the total). During the debriefing, we communicated to the respondents that the videos were scripted and did not reflect real-world events.

The study participants represented a cross-section of the general adult population in each country: US ($N = 607$, mean age = 37 years, $SD = 10.31$), UK ($N = 597$, mean age = 37 years, $SD = 11.93$) and Israel ($N = 644$, mean age = 39, $SD = 13.16$). The distribution of the political orientation of the sample in Israel skewed more right wing than in the US and UK, and the UK sample had a higher portion of female respondents than the US and Israel. Appendix D presents the detailed statistics of the sample and balance checks across the conditions.

We chose to focus on the United States, United Kingdom and Israel since they share several features in common. First, each of these countries is among the short list of states that have been exposed to publicly reported cyber attacks on critical infrastructure. Secondly, all three are ranked within the same decile in terms of the social and economic impact of terrorism as measured by the Global Terrorism Index. Thirdly, each of the countries has high levels of Internet penetration and publicly renowned levels of cybersecurity preparedness to deal with cyber attacks on critical infrastructure. While the quality of past terrorism exposure is likely to be different (Israel is exposed to more persistent and repeated terror attacks, while the US and UK have experienced fewer but larger attacks), all three register high levels of perceived threat from terrorism. The full comparative data appear in Table 2. The selection of these countries additionally reflects a

Table 2. Comparative analyses of factors relevant to cyber terrorism exposure in the United States, United Kingdom and Israel

	United States	United Kingdom	Israel
Global Terrorism Index Ranking (impact of terrorism on country) ^a	Ranked 32 of 130 countries	Ranked 35 of 130 countries	Ranked 36 of 130 countries
Ranking of cyber security preparedness to deal with cyber attacks on critical infrastructure ^b	1 (highest) out of 195 countries	5 out of 195 countries	6 out of 195 countries
Percentage of population fearing that a major terror event will take place ^c	51%	65%	70%
Reported instances of cyber attacks on critical infrastructure ^d	14	2	1

Sources: a: Institute for Economics and Peace 2017; b: Shafqat and Masood 2016; c: Bulman 2018; Israel Democracy Institute 2016; d: Critifence 2018.

reality in which the countries currently most susceptible to cyber terror attacks are the United States, Europe and the West more broadly (Macdonald, Jarvis and Lavis 2019). This Western-centric emphasis is explained by the disproportionately heavy reliance on digital systems that accompanies economic development, as well as the natural tendency to use terrorist tactics in asymmetric conflicts against more conventionally powerful states (Macdonald, Jarvis and Lavis 2019). We note, however, that new research has revealed that cyber terror attacks are increasingly targeting developing countries in the Middle East, Africa and South America as the threshold for obtaining destructive cyber tools becomes gradually lower (Lee *et al.* forthcoming).

Main Results

A preliminary step of our analysis strategy was to verify the emotional effects of exposure to the various terror conditions. This approach allows us to test the efficacy of the experimental manipulation by confirming differential responses among the different conditions. We tested this by running two one-way analyses of variances tests with the type of terror attack as the independent variable and anxiety and anger as the respective dependent variables. The results (see Figure 1) reveal clear differences among the conditions for both anxiety ($F(4, 1,827) = 48.459$, $p < 0.000$) and anger ($F(4, 1,827) = 37.113$, $p < 0.000$). Post-hoc analysis using the Tukey HST statistic revealed that for both anxiety and anger, each of the four terrorism exposure conditions reported statistically significantly higher levels of anxiety and anger than the control condition at the 0.000 significance level for each data point. This result held for the combined sample ($n = 1,832$) and each individual country sample.

The next step of our analysis strategy was to explore any variance in the political effects of exposure to the distinctive terror conditions, using support for retaliatory strikes against the perpetrator of a terror attack as the dependent variable. As described above, this variable was measured using multi-item summative scales with high internal validity. After conducting an exploratory factor analysis, we removed two items from the six-point retaliation measure, which distinguished between military strikes and diplomatic retaliatory responses. The final scale comprises four items asking about cyber strikes or missile strikes against military or civilian targets. Table 3 summarizes the mean scores for each of the variables of interest, showing how each country responded to the various terror conditions to which they were exposed.

To test how exposure to terror affects support for retaliatory strikes, we ran a series of ordinary least squares (OLS) regression analyses (see Table 4). The four models show the collective and country-level effects of each experimental terror condition compared to the *lethal conventional terrorism* group, which acts as the reference condition. We used this subset as the reference condition since lethal conventional terrorism is the classic and emblematic form of terrorism against which we are comparing the new form of cyber terrorism in all of its guises. Since this form of

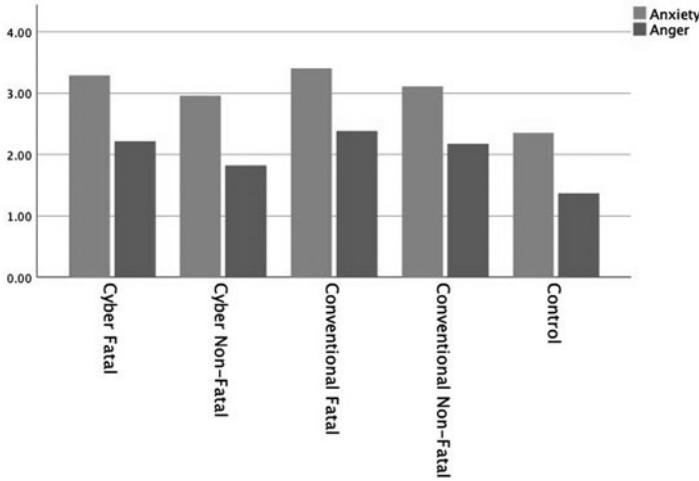


Figure 1. Levels of anxiety and anger by exposure to terror conditions

Table 3. Means for participants on political and emotional measures

Country	Treatment condition	N	Support for retaliatory strikes	Level of anxiety	Level of anger
United States	Cyber terror – Fatal	118	3.24	3.43	2.71
	Cyber terror – Non-fatal	119	2.95	2.98	1.90
	Conventional terror – Fatal	119	3.21	3.55	2.68
	Conventional terror – Non fatal	116	3.07	3.10	2.30
	Control	125	3.45	2.21	1.54
United Kingdom	Cyber terror – Fatal	120	2.55	3.31	2.04
	Cyber terror – Non-fatal	119	2.40	2.90	1.68
	Conventional terror – Fatal	118	2.80	3.44	2.32
	Conventional terror – Non fatal	120	2.53	3.22	2.09
	Control	120	2.61	2.39	1.23
Israel	Cyber terror – Fatal	125	3.98	3.14	1.93
	Cyber terror – Non-fatal	130	3.64	2.99	1.88
	Conventional terror – Fatal	122	4.23	3.22	2.16
	Conventional terror – Non-fatal	123	4.07	2.79	1.86
	Control	138	4.23	2.45	1.32
Combined countries	Cyber terror – Fatal	363	3.26	3.29	2.21
	Cyber terror – Non-fatal	368	3.02	2.96	1.82
	Conventional terror – fatal	359	3.42	3.40	2.38
	Conventional terror – Non-fatal	359	3.23	3.11	2.17
	Control	383	3.33	2.35	1.36

Note: all measures are scored from 1 (lowest) to 6 (highest).

terrorism elicited the highest levels of demand for retaliation, we can easily observe the extent to which the other types of terrorism lowered the demand for retaliatory strikes. The cyber non-fatal terror condition exhibits the strongest effect, with the lowest support for retaliation (approximately 0.4 scale points lower than the control group; $p = 0.000$). This effect suggests that cyber attacks may require a physically destructive element to trigger emotional responses akin to other terror responses. The effects hold while controlling for basic demographic variables and other related variables such as previous exposure to terror incidents and regular use of public transportation. Two covariates had a particularly strong effect on retaliatory preferences. First, as would be expected, political orientation is a key predictor of support for retaliation. A one-point increase on a 1 (left wing) to 7 (right wing) scale of political attitudes increased respondents' support for retaliation by 0.2–0.3 points. This effect is significant at the 0.000 level

Table 4. OLS regression models of support for retaliation policies – individual terror conditions

	1 Three countries	2 US	3 U.K.	4 Israel
Cyber terror (Fatal) condition – Dummy variable	–0.153 [0.079]	0.045 [0.773]	–0.281 [0.054]	–0.278 [0.059]
Cyber terror (Non-Fatal) condition – Dummy variable	–0.393*** [0.000]	–0.179 [0.249]	–0.355* [0.016]	–0.626*** [0.000]
Conventional terror (Non-Fatal) condition – Dummy variable	–0.172* [0.048]	–0.077 [0.622]	–0.235 [0.107]	–0.209 [0.159]
Control condition – Dummy variable	0.031 [0.713]	0.264 [0.086]	–0.157 [0.279]	–0.001 [0.995]
Political orientation (1 = very left wing, 7 = very right wing)	0.245*** [0.000]	0.218*** [0.000]	0.211*** [0.000]	0.294*** [0.000]
Age	0.000 [0.618]	–0.004 [0.429]	–0.005 [0.205]	0.000 [0.578]
Gender (0 = male; 1 = female)	–0.384*** [0.000]	–0.246* [0.016]	–0.517*** [0.000]	–0.365*** [0.000]
Previous exposure to terror attacks (0 = no exposure, 1 = exposure)	0.096 [0.081]	–0.020 [0.840]	0.044 [0.635]	0.244** [0.008]
Regular user of public transportation (0 = no or low use, 1 = regular use)	0.198*** [0.001]	0.612*** [0.000]	–0.037 [0.719]	0.069 [0.474]
Parental status (0 = no children, 1 = children)	0.294*** [0.000]	0.384*** [0.000]	0.197 [0.062]	0.131 [0.193]
Country dummies	Yes	No	No	No
Observations	1,832	597	598	638
R-Squared	0.309	0.215	0.134	0.166
Adjusted R-Squared	0.304	0.201	0.119	0.153

Note: regression coefficients with p-values in brackets. * p < 0.05; ** p < 0.01; *** p < 0.001.

among all countries and in the collective sample. Likewise, gender has a uniformly predictive effect in our model: men are more likely than women to support retaliation against terror groups in all models. Breaking down these findings by country reveals that the combined effects are driven primarily by the Israeli and United Kingdom samples; the United States shows no variance in retaliatory preferences compared to the control group.

Two additional sets of regression analyses further substantiate the difference between the cyber and non-cyber, and fatal and non-fatal forms of terror attacks (see Table 5). We first combined the two cyber terror conditions into one group and the two conventional terror conditions into another group – ignoring the fatality of the strikes and focusing purely on the form of the terror attack. In this analysis, conventional terrorism was the reference group, against which the effects of exposure to cyber terrorism were compared (Table 5, Model 1). In the second analysis, we combined the two fatal terror conditions and the two non-fatal terror conditions into separate groups – disregarding the form of the terror attack and focusing purely on its consequences. In this analysis, fatal terrorism was the reference group, against which the effects of exposure to non-fatal terrorism were compared (Table 5, Model 2). We then ran the same regression analyses to test the effect on retaliation preferences while controlling for the same covariates as above. These analyses reveal a number of interesting findings. First, when focusing only on the *type* of terror attack, respondents exposed to cyber attacks were significantly less likely to demand retaliation than those exposed to conventional attacks. Secondly, concentrating only on the *consequences* of terror attacks yielded an equally strong effect: non-fatal attacks were considerably less likely than fatal attacks to evoke strong demands for retaliation. This supports Hypothesis 2, that the fatality of a terror attack will be a significant predictor of support for retaliatory strikes. These findings additionally illuminate the negligible effect of non-fatal cyber terrorism depicted in Table 4; this form of terrorism appears to suffer from two deficits, lacking both conventional form as well as lethal outcome.

Table 5. OLS regression models of support for retaliation policies – grouped terror conditions

Predictor variables ↓ Reference condition →	1 Conventional (Kinetic) Terrorism	2 Fatal Terrorism
Cyber terror conditions – Dummy variable	-0.187** [0.002]	-
Control condition – Dummy variable	0.118 [0.111]	0.108 [0.143]
Non-fatal terror conditions – Dummy variable	-	-0.208*** [0.001]
Demographic variables as appearing in Table 3	Yes	Yes
Country Dummies	Yes	Yes
Observations	1,832	1,832
R-Squared	0.304	0.305
Adjusted R-Squared	0.300	0.301

Note: regression coefficients with p-values in brackets. * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

We note an unanticipated finding – that the control (reference) group exhibited an equally high level of support for retaliation as the conventional terrorism and fatal terrorism conditions. This is explained by the fact that control group respondents, who did not view any video, were asked to indicate their support for military strikes in response to an unviewed attack – a fact that evoked the worst possible scenario (that is, a high casualty terror attack). We ran a post-hoc experiment to test this theory with a new dataset ($n = 737$ respondents among all three countries) and found that respondents in the control group did indeed envision a high-casualty terror incident – akin to the conventional fatal terror group. The full analysis of this post-hoc evidence appears in Appendix E.

Anger Mechanism Estimation

We hypothesized that increased levels of anger would mediate and explain a substantial portion of the relationship between exposure to cyber and conventional terrorism with retaliation preferences. This is based on the theory that the dominant response of civilian populations to terror threats is anger and a desire for vengeance (Fisk, Merolla and Ramos 2019; Wayne 2019). This anger-driven mechanism can be reflected in a basic mediation model explaining attitudes towards retaliatory strikes following terror attacks. In this case, T reflects exposure to a terror attack, Y is the level of support for retaliatory strikes and M is the anger caused by exposure to the terror attack – the mediator variable. We expect that it is not the mere fact of exposure that causes a demand for retaliation, but rather that exposure leads to anger, which in turn makes respondents more likely to support retaliatory strikes.

To estimate this mediation effect, we employ the accepted technique developed by Imai et al. (2011). This technique requires that we estimate two equations and then perform a bootstrap simulation.

$$M_i = \alpha_1 + \lambda_1 T_i + x\beta + \epsilon_i \quad (1)$$

$$Y_i = \alpha_2 + \lambda_2 T_i + \gamma M_i + x\beta + \epsilon_i \quad (2)$$

Each equation runs a least-squares regression, appearing in Table 6. The dependent variable in Equation 1 (M) is anger, while for Equation 2, the dependent variable (Y) is the support for retaliatory strikes variable. The right-hand sides of the equations contain the exposure to terrorism variable (T) plus a vector of control variables (x) that were collected before the treatment was administered. Equation 2 also includes the mediating anger variable. Having calculated the

Table 6. Mediation regression analyses

Independent binary T variable:	1. Exposure to cyber terrorism vs. Control group		2. Exposure to conventional terrorism vs. Control group	
	Equation (1)	Equation (2)	Equation (1)	Equation (2)
	(Mi) 1.1	(Yi) 1.2	(Mi) 2.1	(Yi) 2.2
Anger		0.153 *** (0.030)		0.120 *** (0.028)
Exposure to type of terror attack (T Variable)	0.658 *** (0.073)	-0.410 *** (0.076)	0.910 *** (0.078)	-0.225 ** (0.078)
Country = United States (dummy variable)	0.441 *** (0.087)	-0.696 *** (0.089)	0.610 *** (0.094)	-0.804 *** (0.090)
Country = United Kingdom (dummy variable)	0.093 (0.090)	-1.107 *** (0.091)	0.249 ** (0.097)	-1.176 *** (0.091)
Political Orientation	0.111 *** (0.023)	0.218 *** (0.023)	0.139 *** (0.025)	0.255 *** (0.024)
Age	0.000 (0.000)	0.000 (0.000)	0.000 (0.000)	0.000 (0.000)
Gender	-0.043 (0.070)	-0.255 *** (0.070)	0.091 (0.076)	-0.431 *** (0.072)
Constant	1.268 *** (0.394)	3.467 *** (0.399)	0.993 * (0.480)	3.460 *** (0.452)
ACME	0.100 *** [0.052, 0.15]		0.109 *** [0.056, 0.17]	
Direct Effect	-0.410 *** [-0.558, -0.26]		-0.225 *** [-0.382, -0.08]	
Total Effect	-0.309 ** [-0.455, -0.16]		-0.115 [-0.258, 0.02]	
N	1,114		1,101	

Notes: entries in rows with variable name labels are least-squares regression coefficients with standard errors in parentheses. Shaded cells reflect the main parameters of interest that must be significant to substantiate a mediation finding (a path, b path, and average causal mediation effect). * = $p < 0.05$, ** = $p < 0.01$, *** = $p < 0.001$. All statistical significance tests are two-tailed.

coefficients and standard errors from these two equations, the Imai procedure then computes the average causal mediation effect (ACME), which is the estimate of the effect that the exposure to terror treatment (*T*) exerted on support for retaliation (*Y*) through the mediator variable (*M*). Due to the weakness of this procedure in integrating multicategorical independent variables, we convert the exposure to terror variable into a binary paradigm and run the analysis twice. The first analysis equates exposure to cyber terrorism as 1 and the control group as 0. The second analysis equates exposure to conventional terrorism as 1 and the control group as 0. Appendix F contains further information on meeting the sequential ignorability assumption required to effectively estimate the true mediation effect.

Table 6 reports the findings of the two mediation analyses on the experimental data, with the main parameters of interest shaded in grey. Each of the different stipulations required to prove a mediation effect is present. First, both treatment effects (exposure to cyber or conventional terror) have a positive effect on the anger variable, as captured by the shaded coefficients in Columns 1.1 and 2.1. The second condition is that the anger mediator exerts an effect on the dependent variable, a fact that is shown in the shaded coefficients in Columns 1.2 and 2.2. In both cases, the anger variable is a strong predictor of support for retaliatory strikes. The final and most important condition is that the ACME is nonzero. The shaded figure at the bottom of the table indicates that the causal mediation effect is 0.100 ($p = 0.000$) and 0.109 ($p = 0.000$), respectively. Contrasting these figures to the total effects illustrates that a substantial portion of the increased support for retaliatory strikes following cyber and conventional terror strikes is due to the anger evoked by the strike.

While the findings seem to be consistent with our theoretical expectations, the fickleness of mediation analyses requires us to thoroughly examine their robustness. We do so by running

two robustness checks. First, we tested the fit of the model by replacing the mediating variable with other prospective intervening variables. Alternative causal mechanisms that could theoretically mediate the relationship between exposure to terrorism and support for retaliation include anxiety and perceived threat. We do not hypothesize that either of these variables will intervene since most recent research suggests that anger is the dominant response of civilian populations to terror threats (Wayne 2019), and that the low-information features of cyber attacks are likely to mitigate the influence of perceived threat as a mediator (Egloff 2020). Still, mediation analyses replacing anger with anxiety, and replacing anxiety with threat perception, confirm that our model is robust to related variables (see Appendix F for full analyses).¹ Secondly, we run a sensitivity analysis to assess whether our mediation is susceptible to a violation of the sequential ignorability principle – that is, whether our mediation results are robust against potentially confounding pre-treatment covariates. The results of this sensitivity analysis (see Appendix F) confirm that the positive ACME findings would require an implausibly large omitted variable to disqualify the positive findings.

Discussion

Terrorism has many faces – the latest of which is digital. In this article we demonstrate how even a digital form of terrorism – cyber terrorism – can have a considerable impact on public support for retaliatory policies. Empirical research on the effects of cyber terrorism is still in its infancy, and the field is characterized by the absence of systematic, methodologically sound data collection and analysis (Dunn Cavelti 2018). This study employed methodologically rigorous analyses of how civilians experience cyber terrorism, and how this influences their policy preferences pertaining to retaliation. Several key findings emerge from these analyses that have practical implications for governments' foreign and cyber policies.

First, civilians respond politically to cyber terrorism in the same way as conventional kinetic terrorism, but only when a cyber terror attack results in fatal consequences. The fatal/non-fatal distinction appears to be the threshold for the onset of strong political effects. This accords with research by Kreps and Das (2017), who identified that the lethality of cyber attacks is a key factor in explaining support for military airstrikes. One way to explain the weak support for retaliation following non-fatal cyber terror attacks is that they may be more associated with cyber *crime*. According to this rationale, the absence of fatal consequences and the lack of any immediately identifiable perpetrators cloud the scope and intent of the attack, which is an important indicator in the public's ascription of terrorism (Huff and Kertzer 2018). The need for death and destruction in ascribing a terrorist label to cyber attacks may pose challenges for governments, since there will be diminished public support for activating the full scope of anti-terror tools in response to non-fatal cyber attacks that otherwise meet every definition of terrorism. For example, non-fatal cyber terror attacks that target critical infrastructure – such as electricity stations or financial networks – can cause highly damaging consequences, yet would not be sufficient to arouse public demands for retaliatory strikes in the same way that a conventional attack would.

Secondly, cyber and conventional terror attacks operate through a similar psychological mechanism, with anger as an intervening variable. We tested a series of possible intervening variables with similar affect, and found that only anger succeeded in explaining the pathway by which exposure to terrorism influenced support for retaliatory policies. This pathway held for both conventional and cyber terrorism. The data support this finding through a robustly tested mediation mechanism, and the fact that the 95 per cent confidence intervals of the ACME overlap for both

¹We measured threat perception using a three-item scale that looks at the realistic and symbolic aspects of perceived threat. Each participant was asked whether and to what extent (1 = not at all; 6 = absolutely) a terror attack threatened their and their family's economic situation, personal safety and values. Internal reliability was high.

the cyber and conventional models (0.052, 0.15 / 0.056, 0.17) indicates that the strength and direction of the model is essentially identical. We acknowledge that even as this resolves some questions, it raises others. Most striking of these is the question of where feelings of anger are directed in instances of cyber terrorism where attribution is uncertain. We propose that the vicarious retribution theory offers an astute solution to this dilemma by drawing on social psychological theories to explain how exposure to violence, even where the identity of an attacker is unknown, can still trigger a punitive mindset and a heightened drive for vengeance against ostensibly related targets (Lieberman and Skitka 2017; Lieberman and Skitka 2019; Washburn and Skitka 2015). While some empirical research has begun to examine how political preferences form when the perpetrator of cyber attacks is unknown (Jardine and Porter 2020), we encourage additional research to focus on this topic.

This study instructs governments interested in pursuing retaliatory strikes following cyber terror attacks to rouse and emphasize public anger. Likewise, governments looking to exercise restraint should attempt to minimize the flame of anger, and instead engage with the public's fear and anxiety. While governments cannot dictate complex societal emotions, especially in the aftermath of crises events, research has indicated that public addresses by leaders can have a significant effect on public anger (Yoo and Jin 2017). From a comparative foreign policy perspective, the question of inflaming and diminishing anger raises interesting questions about cross-cultural emotional dispositions. Does the renowned stoicism of the British public give the government more flexibility in setting foreign policy in the aftermath of attacks compared to the perceived emotional volatility of Israelis and Americans (Meyer 2014), whose heightened anger may encourage retaliation? Research in the aftermath of the 7/7 attack in London identified a strategic invocation of British stoicism as a way of minimizing the emotionally laden response to the attacks in a way that offered the government maximum flexibility (Bean, Keränen and Durfy 2011).

A third and unexpected revelation in the data is the country-specific effects. The observed effect of exposure to cyber terrorism on political attitudes was primarily driven by Israeli and UK respondents; American respondents displayed only minor variation in retaliatory attitudes. We selected countries with equivalent levels of susceptibility to cyber terror attacks, similar levels of cyber security preparedness, and comparable levels of civilian fears of terrorism, but some country-level variables appear to contribute to differential responses in the countries. One possible explanation for this phenomenon, which is beyond the scope of this article, is that Israeli respondents may have more readily available potential perpetrators at the forefront of their minds due to the ongoing conflicts being waged, and so are able to better imagine how (and against whom) retaliation could take place. Another possible explanation is the national appetite for war and the use of force, which is shaped by core national beliefs about revenge, and which varies across countries (Stein 2015). In Stein's study, which did not include Israel, the percentage of UK respondents endorsing revenge was substantially lower than in the United States, which is in line with our findings. We encourage future research to probe country-level variables that influence these cyber terrorism models.

We offer two small case studies that illustrate the applicability of this study. In 2020, Israeli authorities announced that they had successfully repelled a sophisticated cyber attack that sought to surreptitiously add chlorine to the country's water supply. The authorities succeeded in resisting the cyber terror attack, purportedly launched by Iranian-connected attackers, and no casualties were recorded (Heller 2020). A few years earlier, the United States Department of Homeland Security reported that Russian cyber operatives had successfully infiltrated the control rooms of power plants across the United States – an attack that could have led to significant first- and second-order casualties (Sanger 2018). In both these cases, the governments sufficed with token, or at least, public muted military responses – a far cry from what would surely have been demanded had Russian or Iranian operatives been caught physically entering the critical infrastructure sites. These cases – though far from providing conclusive evidence – offer

anecdotal support for our theory that only lethal or destructive cyber terror attacks will give rise to strong public demands for retaliation; conventional terrorism does not have such a conditional threshold.

Myriam Dunn Cavelty's (2007) decade-old statement about the scarcity of verified instances of cyber terror attacks causing fatal consequences is still apt. Yet we anticipate that it is but a matter of time until a paradigmatic case is publicly acknowledged. When this occurs, we will need to understand how exposure to cyber terrorism influences political preferences. This study affirms that cyber terrorism can indeed trigger strong public support for retaliatory military action – but only when it causes fatalities. This is a significant finding since it confirms for the first time that the new phenomenon of cyber terrorism can strongly influence support for policy positions. More so, it reveals that exposure to cyber terrorism causes different responses to conventional terrorism, validating the need for new or adapted political models for digital forms of terrorism. We also confirm that anger is the key underlying variable bridging the relationship between cyber terrorism and preferences regarding retaliation policies. This extends to the cyber realm the recent trend that views anger as the salient mechanism linking exposure to terrorism with militant preferences.

Supplementary material. Online appendices are available at: <https://doi.org/10.1017/S0007123420000812>.

Data availability statement. Data replication files are available in Harvard Dataverse at: <https://doi.org/10.7910/DVN/SACJHE>.

Acknowledgements. The authors gratefully acknowledge Dana Vashdi and Valentin Vancak for their invaluable assistance in analyzing the research data, and Ofer Ravid for his video production and editing. We extend a heartfelt thank you to Sharon Matzkin, who supported the research efforts from their inception to conclusion, and to Miguel Gomez and Keren Snider for their generous advice. This article benefited greatly from the feedback offered at a 2019 colloquium hosted by Myriam Dunn Cavelty at the ETH Zurich Center for Security Studies, and a 2019 cyber-terrorism symposium at the University of Haifa. We appreciate the input of the article reviewers, and the *BJPoS* editor, René Lindstädt.

Financial support. 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, and the Idit Doctoral Fellowship Program at the University of Haifa.

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.

References

- Albahar M** (2019) Cyber attacks and terrorism: a twenty-first century conundrum. *Science and Engineering Ethics* 25(4), 993–1006.
- Applegate SD** (2013) The dawn of kinetic cyber. In *Cyber Conflict (CyCon)*, 2013 5th International Conference. IEEE, pp. 1–15.
- Backhaus S et al.** (2020) A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure. *Cyberpsychology, Behavior, and Social Networking* 23(9), 595–603.
- Bean H, Keränen L and Durfy M** (2011) 'This is London': cosmopolitan nationalism and the discourse of resilience in the case of the 7/7 terrorist attacks. *Rhetoric & Public Affairs* 14(3), 427–464.
- Berrebi C and Klor EF** (2008) Are voters sensitive to terrorism? Direct evidence from the Israeli electorate. *American Political Science Review* 102(3), 279–301.
- Bleich A, Gelkopf M and Solomon Z** (2003) Exposure to terrorism, stress-related mental health symptoms, and coping behaviors among a nationally representative sample in Israel. *JAMA* 290(5), 612–620.
- Bodenhausen GV, Sheppard LA and Kramer GP** (1994) Negative affect and social judgment: the differential impact of anger and sadness. *European Journal of Social Psychology* 24(1), 45–62.
- Bonanno GA and Jost JT** (2006) Conservative shift among high-exposure survivors of the September 11th terrorist attacks. *Basic and Applied Social Psychology* 28(4), 311–323.
- Brenner SW** (2006) At light speed: attribution and response to cybercrime/terrorism/warfare. *Journal of Criminal Law & Criminology* 97, 379–475.

- Bulman M** (2018) UK more concerned about terror than any other country, finds study. *The Independent*, 8 January.
- Bumiller E and Shanker T** (2012) Panetta Warns of Dire Threat of Cyberattack on US *New York Times*, 11 October.
- Canetti D et al.** (2017a) Exposure to violence, ethos of conflict, and support for compromise: surveys in Israel, East Jerusalem, West Bank, and Gaza. *Journal of Conflict Resolution* **61**(1), 84–113.
- Canetti D et al.** (2017b) How cyberattacks terrorize: cortisol and personal insecurity jump in the wake of cyberattacks. *Cyberpsychology, Behavior, and Social Networking* **20**(2), 72–77.
- Canetti-Nisim D, Ariely G and Halperin E** (2008) Life, pocketbook, or culture: the role of perceived security threats in promoting exclusionist political attitudes toward minorities in Israel. *Political Research Quarterly* **61**(1), 90–103.
- Carver CS** (2004) Negative affects deriving from the behavioral approach system. *Emotion* **4**(1), 3–2.
- Cavelty MD** (2007) *Cyber-security and Threat Politics: US Efforts to Secure the Information Age*. Abingdon: Routledge.
- Clarke RA** (2016) The risk of cyber war and cyber terrorism. *Journal of International Affairs* **70**(1), 179–181.
- Critifence** (2018) 2018 critical infrastructure cyber attack timeline. Available from <http://www.critifence.com/papers/attack-timeline/files/SCADA%20Cyber%20Attacks%20Timeline> (accessed 18 May 2020).
- Dorot R** (2020) Media influence matrix: Israel. CEU Center for Media, Data and Society. Available from <https://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/basicpage/1860/mimisraelfunding.pdf> (accessed 20 August 2020).
- Dunn Cavelty M** (2018) Thomas rid, cyber war will not take place. *ERIS–European Review of International Studies* **5**(1), 131–134.
- Egloff FJ** (2020) Contested public attributions of cyber incidents and the role of academia. *Contemporary Security Policy* **41**(1), 55–81.
- Fischer AH and Roseman IJ** (2007) Beat them or ban them: the characteristics and social functions of anger and contempt. *Journal of Personality and Social Psychology* **93**(1), 103–115.
- Fisk K, Merolla JL and Ramos JM** (2019) Emotions, terrorist threat, and drones: anger drives support for drone strikes. *Journal of Conflict Resolution* **63**(4), 976–1000.
- Foyle DC** (2004) Leading the public to war? The influence of American public opinion on the Bush administration's decision to go to war in Iraq. *International Journal of Public Opinion Research* **16**(3), 269–294.
- Gartzke E** (2013) The myth of cyberwar: bringing war in cyberspace back down to earth. *International Security* **38**(2), 41–73.
- Getmansky A and Zeitzoff T** (2014) Terrorism and voting: the effect of rocket threat on voting in Israeli elections. *American Political Science Review* **108**(3), 588–604.
- Gould ED and Klor EF** (2010) Does terrorism work? *The Quarterly Journal of Economics* **125**(4), 1459–1510.
- Graves J, Acquisti A and Anderson R** (2014) Experimental measurement of attitudes regarding cybercrime. In 13th Annual Workshop on the Economics of Information Security. Pennsylvania State University.
- Gross ML, Canetti D and Vashdi DR** (2016) The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists* **72**(5), 284–291.
- 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.
- Gross ML, Canetti D and Vashdi DR** (2018) Cyber terrorism: its effects on psychological well-being, public confidence, and political attitudes. In Lin H and Zegart A (eds), *Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations*. Washington, DC: Brookings Institution Press, pp. 235–264.
- Haidt J** (2003) The moral emotions. *Handbook of Affective Sciences* **11**(2003), 852–870.
- Halperin E et al.** (2011) Anger, hatred, and the quest for peace: anger can be constructive in the absence of hatred. *Journal of Conflict Resolution* **55**(2), 274–291.
- Heller A** (2020) Israeli cyber chief: Major attack on water systems thwarted. *The Washington Post*, 28 May. Available from https://www.washingtonpost.com/world/middle_east/israeli-cyber-chief-major-attack-on-water-systems-thwarted/2020/05/28/5a923fa0-a0b5-11ea-be06-af5514ee0385_story.html.
- Herzog S** (2011) Revisiting the Estonian cyber attacks: digital threats and multinational responses. *Journal of Strategic Security* **4**(2), 49–60.
- Hirsch-Hoefler S 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.
- Hua J, Chen Y and Luo XR** (2018). Are we ready for cyberterrorist attacks? —Examining the role of individual resilience. *Information & Management* **55**(7), 928–938.
- Huddy L et al.** (2002) The consequences of terrorism: disentangling the effects of personal and national threat. *Political Psychology* **23**(3), 485–509.
- Huddy L et al.** (2005) Threat, anxiety, and support of antiterrorism policies. *American Journal of Political Science* **49**(3), 593–608.
- Huff C and Kertzer JD** (2018) How the public defines terrorism. *American Journal of Political Science* **62**(1), 55–71.
- Imai K et al.** (2011) Unpacking the black box of causality: learning about causal mechanisms from experimental and observational studies. *American Political Science Review* **105**(4), 765–789.

- Institute for Economics & Peace** (2017) Global terrorism index: measuring and understanding the impact of terrorism. Institute for Economics & Peace. Available from <http://economicsandpeace.org/wp-content/uploads/2015/11/Global-Terrorism-Index-2015.pdf> (accessed 6 May 2020).
- Israel Democracy Institute** (2016) Peace index poll: 1/3 of Jews say Jewish terrorists should be handled differently than Palestinian terrorists [Press release]. Available from <https://en.idi.org.il/press-releases/12728> (accessed 12 June 2019).
- Jaeger DA and Paserman MD** (2008) The cycle of violence? An empirical analysis of fatalities in the Palestinian–Israeli conflict. *American Economic Review* **98**(4), 1591–1604.
- Janoff-Bulman R and Usoof-Thowfeek R** (2009) Shifting moralities: post-9/11 responses to shattered national assumptions. In Morgan MJ (ed.), *The Impact of 9/11 on Psychology and Education*. New York: Palgrave Macmillan, pp. 81–96.
- Jardine E and Porter ND** (2020) Pick your poison: the attribution paradox in cyberwar. Available from osf.io/preprints/socarxiv/etb72
- Jarvis K, 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.
- Kertzer JD** (2017) Microfoundations in international relations. *Conflict Management and Peace Science* **34**(1), 81–97.
- Klarevas L** (2002) The ‘essential domino’ of military operations: American public opinion and the use of force. *International Studies Perspectives* **3**(4), 417–437.
- Kreps S and Das S** (2017) Warring from the virtual to the real: assessing the public’s threshold for war over cyber security. *Research & Politics* **4**(2), 2053168017715930.
- 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.
- Kupatadze A and Zeitzoff T** (2019) In the shadow of conflict: how emotions, threat perceptions and victimization influence foreign policy attitudes. *British Journal of Political Science*, 1–22. Doi: 10.1017/S0007123418000479.
- Lawson ST** (2019) *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. Abingdon: Routledge.
- Lee C et al.** (forthcoming) Mapping global cyberterror networks: an empirical study of al-Qaeda and ISIS cyberterrorism events. *Journal of Contemporary Criminal Justice*.
- Lerner JS et al.** (2003) Effects of fear and anger on perceived risks of terrorism: a national field experiment. *Psychological Science* **14**(2), 144–150.
- Lieberman P and Skitka LJ** (2017) Revenge in US public support for war against Iraq. *Public Opinion Quarterly* **81**(3), 636–660.
- Lieberman P and Skitka LJ** (2019) Vicarious retribution in US public support for war against Iraq. *Security Studies* 1–27.
- Lindsay JR** (2015) Tipping the scales: the attribution problem and the feasibility of deterrence against cyberattack. *Journal of Cybersecurity* **1**(1), 53–67.
- Macdonald S, Jarvis L and Lavis SM** (2019) Cyberterrorism today? Findings from a follow-on survey of researchers. *Studies in Conflict & Terrorism*, 1–26.
- Marteau TM and Bekker H** (1992) The development of a six-item short-form of the state scale of the Spielberger State – Trait Anxiety Inventory (STAI). *British Journal of Clinical Psychology* **31**(3), 301–306.
- McCarthy J** (2016) Americans cite cyberterrorism among top three threats to US Gallup. 10 February. Available from <https://news.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx>.
- McDermott R** (2010) Decision making under uncertainty. Proceedings of a Workshop Detering Cyberattacks: Informing Strategies and Developing Options for US Policy. National Academies Press, Washington, DC. pp. 227–241.
- McDermott R and Zimbardo PG** (2007) The psychological consequences of terrorist alerts. In Bongar B, Brown LM and Beutler LE, et al. (eds), *Psychology of Terrorism*. Oxford: Oxford University Press, pp. 357–370.
- Meyer E** (2014) *The Culture Map: Breaking Through the Invisible Boundaries of Global Business*. New York: Public Affairs.
- Montalvo JG** (2011) Voting after the bombings: a natural experiment on the effect of terrorist attacks on democratic elections. *Review of Economics and Statistics* **93**(4), 1146–1154.
- Neria Y, DiGrande L and Adams BG** (2011) Posttraumatic stress disorder following the September 11, 2001, terrorist attacks: a review of the literature among highly exposed populations. *American Psychologist* **66**(6), 429–446.
- Nielsen RK, Schulz A and Fletcher R** (2020) The BBC is under scrutiny. Here’s what research tells about its role in the UK. Reuters Institute and University of Oxford. Available from <https://reutersinstitute.politics.ox.ac.uk/risj-review/bbc-under-scrutiny-heres-what-research-tells-about-its-role-uk> (accessed 19 August 2020).
- Noguchi M and Ueda H** (2019) An analysis of the actual status of recent cyberattacks on critical infrastructures. *NEC Technical Journal, Special Issue Cybersecurity* **12**(2), 19–24.
- Norman J** (2018) North Korea, cyberterrorism top threats to US Gallup. 5 March. Available from <https://news.gallup.com/poll/228437/north-korea-cyberterrorism-top-threats.aspx>.
- Nussio E** (2020) Attitudinal and emotional consequences of Islamist terrorism. Evidence from the Berlin attack. *Political Psychology* **41**(6), 1151–1171.
- Pew Research Center** (2020) US media polarization and the 2020 election: a nation divided. Available from <https://www.journalism.org/2020/01/24/democrats-report-much-higher-levels-of-trust-in-a-number-of-news-sources-than-republicans/>.

- Sadler MS et al.** (2005) Emotions, attributions, and policy endorsement in response to the September 11th terrorist attacks. *Basic and Applied Social Psychology* 27(3), 249–258.
- Sanger DE** (2018) Russian hackers appear to shift focus to US power grid. *The New York Times*, 27 July.
- Schmitt MN** (2017) *Tallinn Manual 2.0 on the International law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.
- Shafiqat N and Masood A** (2016) Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security* 14(1), 129–136.
- Shandler R, Gross ML, Backhaus S, Canetti D** (2021) “Replication Data for: Cyber Terrorism and Public Support for Retaliation - A Multi-Country Survey Experiment”, <https://doi.org/10.7910/DVN/SACJHE>, Harvard Dataverse, V1.
- Shandler R, Gross ML and Canetti D** (2021) A fragile public preference for cyber strikes: Evidence from survey experiments in the United States, United Kingdom, and Israel. *Contemporary Security Policy*, 1–28.
- Shoshani A and Slone M** (2008) The drama of media coverage of terrorism: emotional and attitudinal impact on the audience. *Studies in Conflict & Terrorism* 31(7), 627–640.
- Silver RC et al.** (2002) Nationwide longitudinal study of psychological responses to September 11. *JAMA* 288(1), 1235–1244.
- Sirin CV and Geva N** (2013) Examining the distinct effects of emotive triggers on public reactions to international terrorism. *Terrorism and Political Violence* 25(5), 709–733.
- Skitka LJ et al.** (2006) Confrontational and preventative policy responses to terrorism: anger wants a fight and fear wants ‘them’ to go away. *Basic and Applied Social Psychology* 28(4), 375–384.
- Small DA, Lerner JS and Fischhoff B** (2006) Emotion priming and attributions for terrorism: Americans’ reactions in a national field experiment. *Political Psychology* 27(2), 289–298.
- Sobel R** (2001) *Impact of Public Opinion on US Foreign Policy Since Vietnam*. New York: Oxford University Press.
- Spielberger CD** (1970) STAI Manual for the state-trait anxiety inventory. *Self-Evaluation Questionnaire*: 1–24.
- Spielberger CD** (1988) *Manual for the State-Trait Anger Expression Scale (STAXI)*. Odessa, FL: Psychological Assessment Resources.
- Spielberger CD, Reheiser EC and Sydeman SJ** (1995) Measuring the experience, expression, and control of anger. *Issues in Comprehensive Pediatric Nursing* 18(3), 207–232.
- Steele RR, Parker MT and Lickel B** (2015) Bias within because of threat from outside: the effects of an external call for terrorism on anti-Muslim attitudes in the United States. *Social Psychological and Personality Science* 6(2), 193–200.
- Stein RM** (2015) War and revenge: explaining conflict initiation by democracies. *American Political Science Review* 109(3), 556–573.
- Stevens D and Vaughan-Williams N** (2016) Citizens and security threats: issues, perceptions and consequences beyond the national frame. *British Journal of Political Science* 46(1), 149–175.
- Tewksbury D, Jensen J and Coe K** (2011) Video news releases and the public: the impact of source labeling on the perceived credibility of television news. *Journal of Communication* 61(2), 328–348.
- Tidy J** (2020) Police launch homicide inquiry after German hospital hack. BBC, 18 September. Available from <https://www.bbc.com/news/technology-54204356>.
- Tomz M and Weeks JLP** (2016) Public opinion and foreign electoral intervention. *American Political Science Review* 114(3), 856–873.
- Valeriano B and Maness RC** (2015) *Cyber War versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press.
- Washburn AN and Skitka LJ** (2015) Motivated and displaced revenge: remembering 9/11 suppresses opposition to military intervention in Syria (for some). *Analyses of Social Issues and Public Policy* 15(1), 89–104.
- Wayne C** (2019) *Risk or Retribution: The Micro-foundations of State Responses to Terror* (Doctoral dissertation).
- Yoo JW and Jin YJ** (2017) The effects of tearful presidential appeals on public anger relief and government reputation. *Corporate Reputation Review* 20(1), 40–56.