




Public Opinion and Cyberterrorism

Ryan Shandler^{1*} , Nadiya Kostyuk² , Harry Oppenheimer³ 

¹Postdoctoral Research Fellow, Blavatnik School of Government and Nuffield College, University of Oxford, Oxford, UK

²Assistant Professor, School of Public Policy and the School of Cybersecurity and Privacy, Georgia Institute of Technology, Atlanta, GA, US

³PhD candidate, Department of Government, Harvard University, Cambridge, MA, US

Abstract Research into cyber-conflict, public opinion, and international security is burgeoning, yet the field suffers from an absence of conceptual agreement about key terms. For instance, every time a cyberattack takes place, a public debate erupts as to whether it constitutes *cyberterrorism*. This debate bears significant consequences, seeing as the ascription of a “terrorism” label enables the application of heavy-handed counterterrorism powers and heightens the level of perceived threat among the public. In light of widespread conceptual disagreement in cyberspace, we assert that public opinion plays a heightened role in understanding the nature of cyber threats. We construct a typological framework to illuminate the attributes that drive the public classification of an attack as cyberterrorism, which we test through a ratings-based conjoint experiment in the United States, the United Kingdom, and Israel (N = 21,238 observations). We find that the public (1) refrains from labeling attacks by unknown actors or hacker collectives as cyberterrorism; and (2) classifies attacks that disseminate sensitive data as terrorism to a greater extent even than physically explosive attacks. Importantly, the uniform public perspectives across the three countries challenge a foundational tenet of public opinion and international relations scholarship that divided views among elites on foreign policy matters will be reflected by a divided public. This study concludes by providing a definitive conceptual baseline to support future research on the topic.

According to a 2021 Gallup study, the US public ranked “cyberterrorism” as the single most critical threat facing the nation—more even than Russian aggression, the spread of COVID, or the development of nuclear weapons by

*Corresponding author: Ryan Shandler, Blavatnik School of Government, University of Oxford, Radcliffe Observatory Quarter, Woodstock Road, Oxford OX2 6GG, UK; email: ryan.shandler@bsg.ox.ac.uk.

Advance Access publication April 3, 2023

© The Author(s) 2023. Published by Oxford University Press on behalf of American Association for Public Opinion Research.

This is an Open Access article distributed under the terms of the Creative Commons Attribution License (<https://creativecommons.org/licenses/by/4.0/>), which permits unrestricted reuse, distribution, and reproduction in any medium, provided the original work is properly cited.

<https://doi.org/10.1093/poq/nfad006>

Iran (Brenan 2021). Some experts seem to share the public's concern over a potent, even apocalyptic threat of cyberterrorism (Gross, Canetti, and Vashdi 2016, 2017; Henschke 2021), while others view this issue as a hyperbolic depiction of a still developing phenomenon (Valeriano and Maness 2015; Lawson 2019; Gomez and Whyte 2021). Yet what attacks are people afraid of? Which attacks fall under the heading of cyberterrorism, and do the public and elites share the same view of this phenomenon?

The dilemma of whether attacks constitute cyberterrorism is becoming increasingly common as cyberattacks proliferate. In the aftermath of the 2021 Colonial Pipeline cyberattack that triggered gas shortages throughout the United States, a vigorous public debate erupted as to whether this and similar attacks should be treated as terrorism. Some politicians excoriated the Biden administration's characterization of the attack as merely criminal, declaring it a clear act of cyberterrorism that demands a commensurate response (Chamberlain 2021). Other public voices defended classifying the attack as cyber-crime, claiming that the facts do not warrant the application of a terrorist label, which should be reserved for a very specific subset of threats (Sanger and Perlroth 2021). This pattern recurs each time an attack is launched, with supporters pointing to the major consequences of the attack (Stroobants 2018), and detractors insisting on the absence of sufficient political intent (Rid 2013). The decision about whether to label a cyberattack as cyberterrorism bears significant implications, with the application of a terrorism label activating far-reaching counter-terrorism powers, and amplifying public fear and anger (Canetti-Nisim et al. 2009; Zeitzoff 2014; Snider et al. 2021).

In this article, we adopt experimental methods to explore the perception of cyberterrorism from the perspective of the wider public. While previous research has mapped the attitudes of the media (Zeri and Noordin 2017) and the positions of cybersecurity experts (Jarvis and Macdonald 2015), the views of the public remain understudied. This is surprising due to the central role that public opinion plays in understanding the effectiveness of terrorism (Enders and Sandler 2011). If a primary goal of terrorists is to spread fear and draw attention to their cause, then the public perception of what constitutes cyberterrorism is prerequisite to gauging its effects. In addition to entering this theoretical debate, this manuscript aims to generate a level of conceptual consistency to guide future research. Empirical and theoretical research into cyber-conflict, public opinion, and international security is burgeoning, yet the field suffers from an absence of conceptual agreement about key terms (Branch 2021). This article seeks to provide a definitive baseline to support the wave of research on the topic.

To probe the factors that underlie the decision to designate a cyberattack as cyberterrorism, we employ a ratings-based conjoint experimental design with 3,036 respondents in three countries—the United States, United

Kingdom, and Israel. We begin by constructing a typology of key variables that we hypothesize will drive the public perception of cyberterrorism. We then employ a conjoint structure to isolate the effect of each attribute on the decision to classify various scenarios as cyberterrorism. Building on this base, we take advantage of our multi-country dataset to examine whether the attributes that drive the designation of cyberterrorism are uniform across borders. This design sets our paper apart as the most comprehensive comparative study of public opinion in response to cyberattacks.

We identify several definitive features that guide the public classification of cyber incidents. First, we find that the public is disinclined to label attacks by unknown actors as cyberterrorism, which is striking due to the difficulty of attributing cyberattacks. Second, we observe a clear reticence to associate attacks by individuals or hacker collectives as cyberterrorism, regardless of the consequences of such attacks. Third, we detect a readiness to associate attacks that steal and disseminate sensitive data with cyberterrorism, to the extent that the public views these attacks just as seriously as attacks causing major physical explosions. Overall, our results demonstrate a highly stable view of cyberterrorism, which transcends national boundaries, and which starkly differs from elite-driven understandings of terrorism. Given the absence of conceptual uniformity among domain experts (Jarvis and Macdonald 2015), we conclude by arguing that the public perspective on cyberterrorism may constrain policy elites due to the robust public consensus that has formed.

Why Is Public Opinion Important in Understanding Cyberterrorism?

Historically, the public was viewed as holding inconsistent and incoherent views on national security and foreign policy, which led to policymakers ignoring their views and limited their influence over policy (Almond 1950; Baum and Potter 2015). However, scholars have come to understand that the public has increasingly nuanced views on matters of national security, and that public opinion can influence elite decision-making (Lin-Greenberg 2021; Sevenans 2021). While we do not go so far as to claim that public views can definitively resolve technical policy debates, we offer four reasons why civilian responsiveness to cyberattacks is important.

First, the public perception of an attack as terrorism has political and electoral consequences. Leaders frequently take advantage of the ambiguity inherent in terrorism to designate the acts of out-group members as terrorism and reap political benefits (Geis and Wunderlich 2014). Similarly, the public often demands that politicians label acts of domestic violence as terrorism due to the normative weight of the label. A seminal example of this is the

acrimonious public debate in the United States about applying the terrorist tag to acts by white-nationalist groups (Ackerman 2012). In addition to the normative significance of this labeling act, designating an out-group as terrorists strongly impacts voting behavior and election outcomes (Montalvo 2011). The extent to which the public will accept or expect such designations in the realm of cyber is still open to question.

Second, the subjective perception of an act as terrorism can influence political attitudes ranging from support for military action to shifts in political orientation (Getmansky and Zeitzoff 2014). These political effects are mediated by the subjective perception of threat (Huddy et al. 2005; Snider et al. 2022). For instance, perceiving an attack as terrorism rather than crime leads to distinct levels of anxiety and fear (Shechory-Bitton and Cohen-Louck 2018), which in turn shifts political attitudes such as militaristic tendencies, and willingness to sacrifice civil liberties for security (Snider et al. 2021). Applying this to cyberspace, it may well be that the public perception of an attack as cyberterrorism rather than cyber-crime or cyber-vandalism will likewise bear an outsize effect on political behavior.

Third, the media regularly has to make decisions about how to frame acts of political violence. This often takes place before the authorities have made a public determination about whether an act formally meets the designation of terrorism. With the diffusion of media from a centralized elite to independent reporters, bloggers, and influencers operating through social media, this framing decision is moving from professional editors to individual actors (Konow-Lund and Olsson 2017). Seeing as the framing of an act as terrorism can significantly raise the profile of an attack and influence the public's response (Baum and Groeling 2010), it becomes important to understand the factors that drive journalists and thought leaders to designate an attack as terrorism.

Finally, there is often greater room for public input in policy areas lacking broad consensus, since elites are more willing to follow popular views in these cases (Kreps and Das 2017). This situation can be aptly observed in the case of cyberterrorism, where elites have demonstrated that they are attuned to public views regarding cyberterrorism. For instance, Congress members in the United States and parliamentarians in the United Kingdom have made speeches on the floors of their respective houses that specifically referred to the views of their constituents about the nature and gravity of the cyberterrorism threat (U.S. Congress 2016).

In summary, we assert that the public is a central actor in shaping the normative and political significance of cyberterrorism. It is well established that public opinion plays a tangible albeit limited role when it comes to traditional foreign policy issues, and we expect that this role will be greater still when it comes to novel cyber-threats where the absence of established norms

and the absence of an elite consensus on the definition of cyberterrorism open the door to greater public influence.

When Do Cyberattacks Become Cyberterrorism in the Eyes of the Public?

A number of studies over the years have sought to define cyberterrorism, yet what emerges chiefly from these analyses is the complete lack of consensus about the term (Luijckx 2014). Jarvis, Nouri, and Whiting (2014) explain the contestability of this phenomenon by pointing to the still-evolving nature of cyberspace and the collective fear of omniscient attackers whose destructive power is inflated in the public discourse. In the absence of consistent policy guidance, which attributes does the public rely on in classifying a cyberattack as cyberterrorism?

Insofar as cyberterrorism is just a methodological subset of terrorism, the public may search for characteristics it associates with conventional terrorism. Yet while cyberterrorism is unquestionably related, research has shown that it is substantively different from conventional terrorism in its practice and effects (Backhaus et al. 2020; Shandler, Snider, and Canetti 2022; Shandler and Gomez 2022; Shandler et al., 2023). We therefore hypothesize that there will be several distinguishing predictive features that are unique to cyberterrorism.

To identify these features, we draw on an enduring debate in the literature about whether the focal cyber component of cyberterrorism refers to the ends or means of an attack. Specifically, Denning (2000) suggested that cyberterrorism should be generally understood to mean unlawful attacks and threats thereof against computer networks. This view of cyberterrorism gained traction with supporters who extrapolated that cyberterrorism refers to digital political acts as varied as unauthorized deletions and denial-of-service attacks (Luijckx 2014). These scholars stress the importance of a digital *target* for an act to be designated as cyberterrorism. By contrast, most researchers today subscribe to a broader conception of the term that views any attack predominantly utilizing digital means as meeting the cyber-threshold of cyberterrorism, even if the final target is not digital (Murray et al. 2019). For these scholars, a digital *method* is a priority.

In addition to the “target” and “method” classes, we also distinguish three additional categories—outcome, agent, and motivation—which form cues that help people classify attacks. We explain each of the five categories below and how they contribute to the public ascription of cyberterrorism. We end this section by hypothesizing about the cross-national peculiarities that might contribute to diverging views of cyberterrorism among countries.

Factors Guiding the Public Ascription of Cyberterrorism

Method of attack

The form of the perpetrated violence is a central variable in attributing an attack as terrorism. Referring to our definitional dilemma, we first distinguish whether an attacker uses digital or non-digital means to execute an attack. Following Murray et al. (2019), we hypothesize that an attack utilizing digital means should increase the public perception of an attack as cyberterrorism more than an attack utilizing non-digital means. Yet we also differentiate between different types of digital attacks. Studies of conventional terrorism show that the method of attack matters, with bombings perceived as most highly associated with terrorism, followed by less destructive methods such as shootings and stabbings (Huff and Kertzer 2018). Even though we substitute these kinetic methods with digital equivalents such as malware, computer viruses, and Trojan horses, we expect that the particular digital method of attack will not be predictive of an attack's classification as an instance of cyberterrorism, since no one attack type is considered more dangerous or destructive than another.

Target of attack

We differentiate between the targets of an attack in two ways. First, relating to abovementioned definitional dilemma, we distinguish whether the digital element of cyberterrorism must be the means of attack or the target of attack. Following Denning (2000), we hypothesize that digital targets (i.e., network servers) should increase the public ascription of cyberterrorism more than non-digital targets. Second, and following the literature on conventional terrorism, we distinguish between military and noncombatant targets. The public view of terrorism typically accords with the *jus in bello* perspective that recognizes the legitimacy of attacks on combatants, and only views attacks against noncombatants as terrorism. Yet the advent of cyber-capabilities has complicated this balancing act, since cyber-operations can deliver major advantages without causing fatalities, a fact that should minimize the stigma against targeting noncombatants (Gross 2018).

Outcome of attack

The question of whether cyberattacks need to cause real-world physical destruction is central to our debate on perceptions of cyberterrorism. Previous research has shown that cyber-terror acts must result in physical destruction to trigger strong public support for military retaliation (Shandler, Gross, and Canetti 2021; Shandler et al. 2022). As such, we expect that the "outcome of attack" attribute will be significant in predicting whether the public ascribes

a terrorism label to a cyberattack—attacks that cause physical destruction will be classified as terrorism, while those with an outcome of financial theft will not.

Agent of attack/attacker identity

Most definitions of terrorism require that the perpetrator be either conducted or inspired by an organization with an identifiable chain of command (Hoffman 2006). Previous research suggests that the public is more likely to consider an organizationally linked attack as terrorism compared to attacks by individuals (Huff and Kertzer 2018). Cyber-attackers can be divided in the same way, and so we expect that the involvement of organized groups will be predictive of a cyberterrorism label, compared with individual hackers (D’Orazio and Salehyan 2018). But, in contrast to kinetic attacks, the identities of cyber-attackers often remain unknown since the particular characteristics of cyberspace allow actors to obfuscate their identity (Rid and Buchanan 2015). The literature is divided on the effects of this uncertainty in attribution on public attitudes. Drawing on theories of risk perception, several scholars have theorized that the view of digital actors as omniscient, invisible perpetrators will heighten threat perception (Jarvis, Nouri, and Whiting 2014; Dunn Cavelti 2019; Kostyuk and Wayne 2021). But recent research suggests that the absence of definitive attribution will decrease the likelihood that the attack will be perceived as terrorism (Bada and Nurse 2020). In line with the latter logic, we expect that the public will view attacks with unattributed perpetrators as less likely to be a cyberterrorism event.

Motivation of attack

The motivation attribute can be considered as a subjective determination since it requires the public to explore the underlying intent of another person. Yet the public intuitively relies on assumptions about attacker motivation in forming opinions (Kimhi, Canetti-Nisim, and Hirschberger 2009). Therefore, we argue that the public will take note of the intent behind an attack as a factor in how the attack is perceived (Canetti, Gubler, and Zeitzoff 2021). Common motivations associated with terrorism include political, social, and religiously driven attempts to influence public policy, though states have begun to broaden the definition of terrorism with new laws that equate individual hate crimes with domestic terrorism. Furthermore, we note that in contrast to conventional terror attacks, the motivation of cyberattackers often remains unknown (Rid and Buchanan 2015). In line with this logic, we expect that the public will view attacks with unknown motivations as less likely to be a cyberterrorism event.

Country-level effects

To what extent will public views transcend national borders? We suggest that the above attributes will regulate the public perception of cyberterrorism across countries. The reason for this is that the public is exposed to extensive discourse on cyber-threats via the media and popular culture—which tends to be homogeneous in its depictions of cyberterrorism (Zeri and Noordin 2017).¹ To the extent that the media adopts a consistent approach to reporting about cyberterrorism, then any elite variance will not necessarily filter down to the public (Groeling and Baum 2008; Kertzer and Zeitsoff 2017). If this is indeed the case, we should see a consistent view of cyberterrorism within and among the three countries in our research sample—the United States, United Kingdom, and Israel.

Nevertheless, despite our expectation of a consistent perception of cyberterrorism, we do expect that there will be some level of country-level divergence based on the distinctive experiences of particular countries. For example, distinct to the United States is the politicization of database breaches by individual hackers. Seminal examples include the Snowden leaks, and the dissemination of troves of emails from the Democratic National Committee during the 2016 national election. The highly public response to these hacks has led to a charged public debate about information theft, cyberattacks, and treason. We therefore expect that American respondents will perceive cyberattacks by individual hackers as cyberterrorism to a greater extent than other countries. Likewise, we expect a Jihadi attacker identity to be significantly predictive of the application of a cyberterrorism label in all countries (D'Orazio and Salehyan 2018), yet we anticipate that this will be strongest in Israel, where religious violence is most salient.

Method

Our analytical strategy involves estimating the causal effects of specific incident attributes on the public ascription of an attack as cyberterrorism. To do so, we use a conjoint experiment design that works by building randomly generated scenarios with interchangeable attributes that are drawn from a pre-populated list. After viewing a randomly generated scenario, populated with one item drawn from each of the five incident attributes explained in our theory section, participants responded whether they would or would not classify the incident as cyberterrorism. We use a conjoint design because it: (1) allows us to hold fixed a multitude of attributes—something that would not be possible with observational studies due to the inability to isolate the

1. While Jarvis, Macdonald, and Whiting (2017) identify diversity in media discourse, they confirm that the most apprehensive international media accounts of cyberterrorism are presented in a uniform manner as cataclysmic threats targeting “the West” or the entire world.

Scenario 1 of 7

An attack has taken place using a malicious software program.
 The attack was carried out against an electricity power station.
 The attack caused a major explosion.
 The attack was carried out by an organization with ties to a foreign government.
 Authorities have declared that the incident was motivated by the goal of changing government policy.

In your opinion, does this scenario describe a cyber-terrorism attack?

Yes – this is cyber-terrorism | No – this is not cyber-terrorism

Figure 1. An example conjoint scenario.

variables of interest, and (2) gives us the ability to study the effect of each attribute, which would not be possible with traditional factorial experiments due to the statistical power constraints. We consider a ratings-based conjoint better suited to this study than a choice-conjoint structure since citizens assess the status of each attack as they appear, rather than comparing the merits of two attacks against one another. Figure 1 illustrates how a randomly generated vignette appeared to participants.

Survey Instrument

In this section, we explain the five-attribute typology which we employ in our conjoint design.² Table 1 summarizes the conjoint attributes, values, and reference conditions.

Attribute #1: agent of attack

Following the literature on conventional terrorism, we distinguish between terror organizations (independent versus state-sponsored) and lone-wolf attacks (Weimann 2012). We also add a new digital-centric category of “loosely affiliated hacker group” in recognition of the prominent hacktivist groups that are responsible for widely reported cyberattacks and which do not fit into classical actor categories. Finally, since many cyberattacks lack attribution, we label them as an “unknown actor.” We use a “foreign country” as our baseline.³

2. The research design and all hypotheses were preregistered. The pre-analysis plan can be accessed at <https://osf.io/d69k3>.

3. As a rule, neutral or status-quo items are selected as the baseline conditions against which the effect of substituting for other items are contrasted. In a subsequent analysis, we employ a marginal means technique which avoids the distorting effect of a reference condition (Leeper, Hobolt, and Tilley 2020).

Table 1. Attributes for cyberterrorism classification scenarios in conjoint experiment.

Attributes	Values
Agent of attack	A foreign country (baseline) A group of hackers with ties to a foreign government A Jihadi Islamic group An organization with ties to a foreign government An unaffiliated group of hackers An individual hacker An unknown actor
Method of attack	A cyberattack has taken place (baseline) An attack has taken place An attack has taken place through the insertion of an infected USB disc An attack has taken place using an email that tricked employees into sharing their passwords and usernames An attack has taken place using a malicious software program
Motivation of attack	The incident was motivated by revenge (baseline) The incident was motivated by the goal of overthrowing the government The incident was motivated by the goal of changing government policy The motivation for the incident remains unknown
Outcome of attack	No casualties or property damage were reported in the attack (baseline) The attack caused a major explosion Sensitive personal and organizational data was stolen and publicly released in the attack The attack caused a minor explosion Millions of dollars were stolen in the attack
Target of attack	A military facility (baseline) Online databases (containing personal information about citizens) A government office building An electricity power station A shopping mall

Note: This table shows the attributes and attribute values that are used to generate the cyberterrorism scenarios for the conjoint methodology. For the purposes of statistical comparisons, one value in each attribute category is marked as the “baseline item” against which all of the other items are measured.

Attribute #2: method of attack

The method of attack attribute distinguishes between purely external intrusions such as malware, spear-phishing attacks, and insider-facilitated intrusions such as an infected USB drive plugged into a target site. We included the above categories because they constitute common forms of cyberattacks that are often discussed in the public sphere. A generic unspecified “cyberattack” was inserted as a baseline condition.

Attribute #3: motivation of attack

The public often takes note of the intent behind an attack as a factor in how the attack is perceived (Canetti, Gubler, and Zeitzoff 2021). Potential motivations included in our typology range from an explicit desire to overthrow the government, to a somewhat softer intent to alter government policy, or to a simple revenge motive, which we use as our reference condition. Since many cyberattacks lack attribution, we also include an unknown motivation behind an attack.

Attribute #4: outcome of attack

The existence and the extent of casualties in the aftermath of attacks attract significant public attention. While this outcome variable is usually measured on a continuum of no casualties to mass casualties, we intend to consider several other nonlethal outcomes that relate to the particular nature of cyberterrorism. These include the theft of sensitive personal or organizational data, and financial theft. A baseline option was included whereby the attack caused no casualties or property damage.

Attribute #5: target of attack

We differentiate between the targets of an attack in two ways. First, to consider whether the digital element of cyberterrorism must be the means of attack or the target of attack, we include both digital targets (e.g., databases) and traditional concrete targets (e.g., malls or power stations). Second, we distinguish between military (e.g., a military facility) and noncombatant (e.g., a shopping mall) targets. Similarly, we employ this distinction because each of these types of targets are frequently the subject of cyberattacks (e.g., Wheeler and Schneier 2021). Military targets are used as a baseline condition.

Adopting best practices in conjoint experiments in the political sciences (see Hainmueller and Hopkins 2015), we minimize the number of design constraints, adding only two constraints within the randomization protocols to avoid implausible combinations of scenario attributes. Specifically, we

excluded scenarios depicting an attack on information databases causing a major or a minor explosion. In total, there are 3,220 unique ways to build a scenario by substituting the different values in each attribute.

Survey Sample and Design

The study was fielded simultaneously in the three countries on 26 August 2020, during which time we recruited 3,242 respondents (United States, $N = 1,077$; United Kingdom, $N = 1,042$; Israel, $N = 1,123$). Surveys were distributed via Amazon Mechanical Turk, Prolific, and the Midgam Survey company in the United States, the United Kingdom, and Israel, respectively. Participants were required to have an approval rating of 96 percent, and reCAPTCHA technology was used to weed out potential bots. We retain only the 3,036 respondents who completed all of the conjoint questions and who passed the reCAPTCHA test. This amounts to a total non-completion rate of 6.35 percent—a rate that compares favorably to completion metrics in other web-based surveys (Liu and Wronski 2018). Following best practice, we refrain from removing speeders (Greszki, Meyer, and Schoen 2015).⁴

We elect to focus on three countries to demonstrate that our hypothesized effects transcend borders. Even though cultural differences often precipitate distinct national responses to security crises, we hypothesized that public opinion regarding cyber threats should be stable cross-nationally. We focus on these three countries since they possess certain features in common. Importantly, they are all technologically advanced countries with a history of publicly reported cyberattacks on critical infrastructure (Critifence 2018). Additionally, they are all democracies, where public opinion can have a greater effect on policy. In the Discussion section, we consider the generalizability of these scope conditions. With 3,036 participants classifying seven incidents each, the following analyses include classifications of 21,238 different randomly generated scenarios.

The following analyses are carried out using the R Statistical Computing language (v4.2.1, R Core Team 2022), and RStudio Version 1.2.1335. The conjoint analyses were carried out using a combination of functions from the *Cregg* and *Cjoint* packages, respectively (Barari et al. 2018; Leeper 2020). We cluster all standard errors by respondent, seeing as rating outcomes are not independent across the multiple scenarios rated by each respondent. A codebook with details of all collected variables appears in [Supplementary Material section 1](#).

4. Detailed balance checks and an extended discussion of the recruitment strategy and sample quality appear in [Supplementary Material section 2](#).

Results

We begin by analyzing which attack attributes heighten the likelihood of a cyber incident being perceived as cyberterrorism. We then proceed to disaggregate the results across countries.

Effects of Attack Attributes on Classification of Incidents as Cyberterrorism

Our analysis strategy involves assessing the relative importance of each attribute by calculating the average marginal component effects (AMCE). This draws on an estimation strategy developed by [Hainmueller, Hopkins, and Yamamoto \(2014\)](#), which has since become the norm in conjoint analyses in the political sciences ([Hainmueller and Hopkins 2015](#)).⁵ The AMCE figure quantifies the differential likelihood of a scenario being classified as cyberterrorism when comparing two attribute values while controlling for all other permutations of the remaining attributes. [Figure 2](#) displays the results for each of the five attributes among the full multicountry sample.⁶ The lines indicate 95 percent confidence intervals for the AMCE of each attribute value—reflecting the change in the probability that respondents will classify a scenario containing that value as cyberterrorism. The upper items in each category denote the reference item for that attribute against which the other values are compared.

A number of trends immediately emerge from [figure 2](#). Taking note of the effect of the *attack agent*, we can observe a clear reticence to associate non-governmental actors with cyberterrorism. Compared to the baseline (foreign country), the presence of an individual hacker or an unaffiliated group of hackers significantly decreased the likelihood that an attack would be classified as cyberterrorism by 7.3 percentage points ($SE = 1.2$) and 4.1 percentage points ($SE = 1.1$), respectively. This means that, all else being equal, the wider public is likely to eschew the label of cyberterrorism when assessing the actions of an unaffiliated hacker collective like Anonymous. By contrast, the public appears to be willing to make accusations on the basis of circumstantial evidence, and will label attacks as cyberterrorism if ostensibly independent hackers maintain ties with a foreign government. This reinforces new research by [Canfil \(2022\)](#) that overturned the fallacy of a widespread and successful use of non-state proxies to obscure attribution in cyberspace. Notably, the presence of an unknown actor significantly diminishes the

5. We discuss whether and how our design abides by the assumptions required to conduct ratings-based conjoint analysis in [Supplementary Material section 5](#).

6. The full coefficient table for [Figure 2](#) appears in [Appendix A](#).

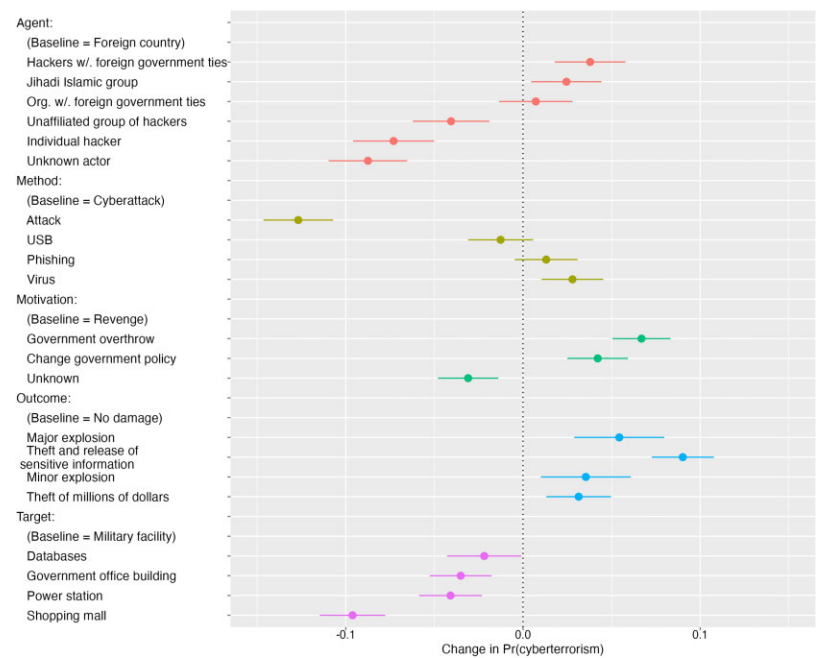


Figure 2. Effects of incident attributes on probability of being classified as cyberterrorism. This plot depicts estimates of the effects of each randomly assigned attribute values on the probability of a scenario being classified as cyberterrorism. Estimates are based on the AMCE model with respondent-clustered standard errors. Bars represent 95 percent confidence intervals. This plot reveals a pooled estimate for the full multicountry sample ($N = 21,238$ observations from 3,036 unique respondents).

likelihood that an incident will be labeled as cyberterrorism in the eyes of the public (8.7 percentage points; $SE = 1.1$).

Turning to the *method of attack*, we can immediately see a clear division between non-cyber-specific items (an attack), and attack descriptors that convey that a cyber-technique was employed (phishing attack, virus, etc.). Describing the methodology of an incident as “an attack” significantly lowers the likelihood of an incident being designated as cyberterrorism by 12.7 percentage points ($SE = 1.0$) compared to a “cyberattack” description. What is noteworthy here is that there is conspicuously little difference between the various cyber methodologies. Even a generic “cyberattack” is sufficient to invoke the cyber connection that the public ostensibly seeks. This tells us that the public does not differentiate between alternate cyberattack routes when

classifying an incident. The public responds in the same way whether an attack utilizes a phishing technique or an infected USB key.

We also find evidence that *attacker motivation* matters, with actions spurred by a desire to change government policy or overthrow the government leading, naturally, to a significantly higher probability of incidents being classified as cyberterrorism compared to revenge as the motivation (4.2 percentage points; SE = 0.9 and 6.7 percentage points; SE = 0.8). This abides by the same internal logic that drives the definition of conventional terrorism, requiring some underlying political motive. What stands out is the contractionary effect of the perpetrator's motivation being unknown. Similarly to the presence of an unknown attacker, the lack of specificity in an attacker's motivation significantly reduces the perception of an attack as constituting cyberterrorism (3.1 percentage points; SE = 0.9) when compared to a vengeance motivation, which is not typically associated with terrorism.

Looking at the *outcome of an attack*, we can see that attacks causing minor or major physical destruction will significantly increase the likelihood of an incident being designated as cyberterrorism compared to an attack that leads to no damage by 3.5 and 5.4 percentage points, respectively. This confirms prior research by Shandler et al. (2022), which emphasized the importance of tangible physical effects in shifting public opinion following strikes in the cyber domain. Yet our findings reveal that the public views the theft and dissemination of sensitive personal and organization data as an even graver consequence, significantly increasing the likelihood of a cyberterrorism classification by 9.0 percentage points (SE = 0.9) compared to the baseline. This may reflect a mounting comprehension of the damage that can be wreaked by the dissemination of personal data, and the continual exposure to reports of foreign actors targeting sensitive data in the context of national elections (Zubiaga, Procter, and Maple 2018). By contrast, an outcome of monetary theft is not nearly as likely to invoke the specter of cyberterrorism compared to major physical destruction and data acquisition.

Finally, the *attack target* attribute reveals the limits of the public's comprehension of terrorism, with military facilities being most highly associated with cyberterrorism, more than government office buildings, power stations, or shopping malls. One of the rare features that is shared among all definitions of terrorism and cyberterrorism is that it must target civilians—not combatants. As such, it is surprising to see that attacks against civilian infrastructure such as shopping malls significantly lowered the likelihood that an incident would be classified as cyberterrorism by some 9.6 percentage points (SE = 0.9) compared to an attack on a military facility. A possible explanation is that the vast majority of high-profile cyberattacks that have been reported in the media have been attacks against the state itself (Jarvis, Macdonald, and Whiting 2017). By contrast, reports of cyberterrorism attacks targeting civilian

infrastructure have only begun to emerge in the last three years (Sanger and Perlroth 2021), and so the public may simply not have paradigmatic examples of cyberterrorism targeting civilians in mind. Alternatively, Young and Findley (2011) have raised the possibility that attacks against military targets—conducted during peacetime—might reasonably qualify for the category of terrorism. For example, the bombing of the USS *Cole* in 2000, and the September 11 plane attack on the Pentagon, are both commonly referred to as terrorism, even though the attacks were conducted against military targets. In our conjoint study, the participants received no hint that any attack took place in the context of active military operations, and so it is natural that they would view unprovoked attacks on the military as terrorism.

Comparing Cyberterrorism Classifications across Country Samples

In figure 3, we display the results for each of the five attributes again, but this time broken down by country. Each line indicates the 95 percent confidence interval for the AMCE of an attribute value—reflecting the relative probability that respondents will classify a scenario containing that value as cyberterrorism.⁷ It is immediately apparent that there is a high level of consistency between countries in how each attribute affects the classification of an incident as cyberterrorism.

To identify the extent of any between-country differences, we utilize a technique developed by Leeper, Hobolt, and Tilley (2020) that examines subgroup differences using conditional marginal means by highlighting the similarities and dissimilarities between subgroups without the distorting effect of a reference condition. This dyadic analysis appears in figure 4, and the full cross-country estimates appear in Supplementary Material section 3.

The key result to emerge from this analysis is that there is an extremely high degree of similarity across countries in how each attribute affects the public designation of an incident as cyberterrorism. Comparing between the United States and Israel, for example, there are only 4 of 26 attribute values that are statistically different at the 5 percent-level across the samples. It appears that despite the absence of clear top-down guidance, the publics in multiple countries have coalesced in their views of what constitutes cyberterrorism.

While the estimates across countries reveal a high degree of similarity, there are several isolated attributes where the effects do vary between countries. For instance, as we hypothesized, the US respondents were significantly less likely to label an attack by an individual hacker as cyberterrorism, compared to the

7. The full tabular results for this analysis are in Appendix B.

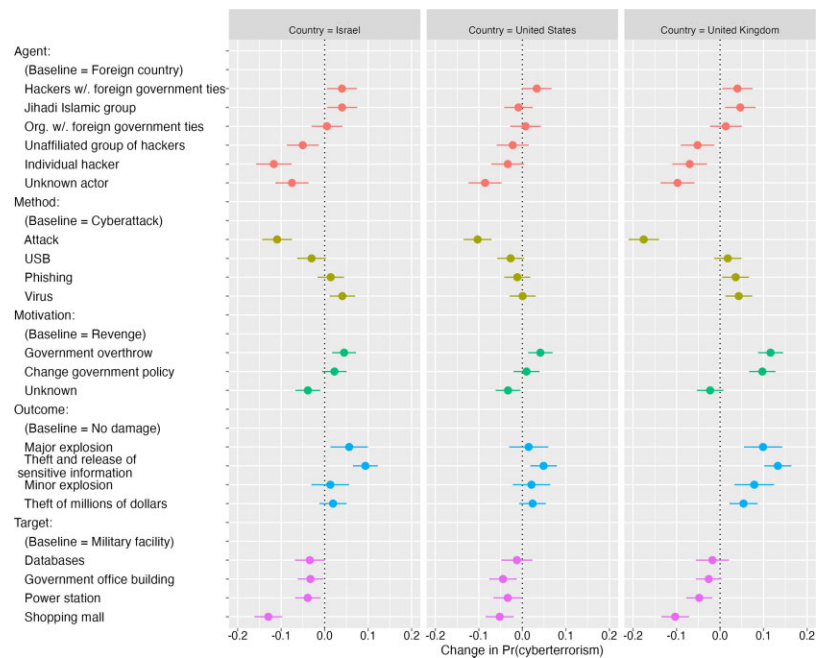


Figure 3. Effects of incident attributes on probability of being classified as cyberterrorism—by country. This plot depicts estimates of the effects of each randomly assigned attribute value on the probability of a scenario being classified as cyberterrorism. Estimates are based on the AMCE model with clustered standard errors. Bars represent 95 percent confidence intervals. This plot exhibits a pooled estimate for each country sample (N = 7,084 observations from 1,012 respondents in the United States; 7,070 observations from 1,010 respondents in the United Kingdom; and 7,098 observations from 1,014 respondents in Israel).

United Kingdom ($p < .001$) and Israel ($p < .001$). British respondents were slightly more attuned to the motivation of the attackers, with revenge motivations and unknown motivations both significantly lowering the chances of an attack being classified as cyberterrorism compared to American ($p < .001$ for revenge and $p < .001$ for unknown motivation) and Israeli ($p < .001$ for revenge and $p < .005$ for unknown motivation) respondents.⁸

8. In addition to examining country effects, we also measure the interaction between respondents' partisan beliefs and computer literacy (Supplementary Material section 4). We find that: (1) liberals rely more on the presence or absence of particular features in applying a terroristic label; and (2) highly digital literate respondents are more attuned to the gravity of particular types of attack.

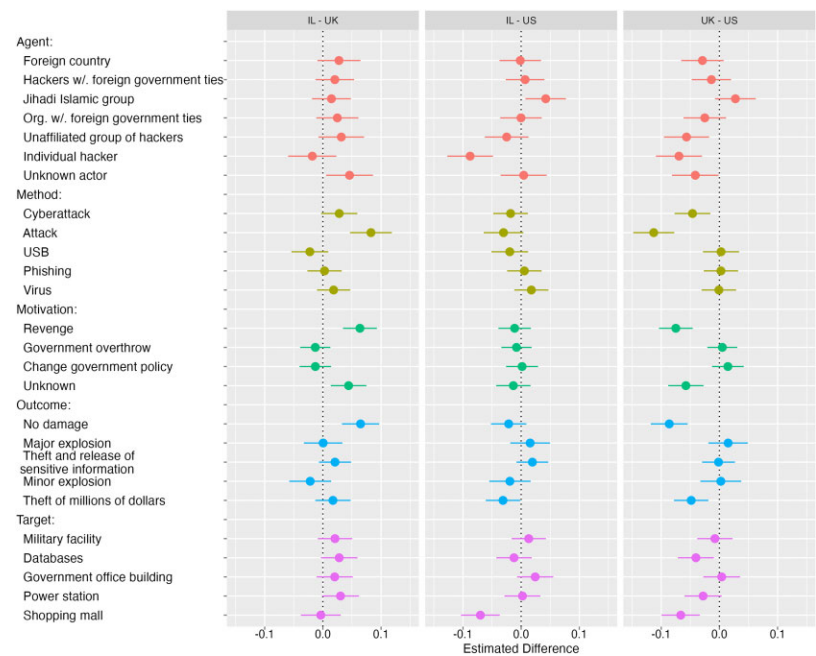


Figure 4. Marginal means differences by country. This figure contains a plot of the difference in marginal mean levels cyberterrorism attribution by treatment category with 95 percent confidence intervals. The country that appears first in the title is the reference condition, against which the country listed second is compared. For example, attributing the motivation of an attack to revenge has a more positive effect on attribution for American respondents than Israeli or British respondents. IL: Israel; UK: United Kingdom; US: United States.

Discussion

This study stems from the premise that there is substantial disagreement over what constitutes various cyber-threats. We witness this confusion in the aftermath of each cyber incident, with public debate flaring over whether to label the incident as cyberterrorism, cybercrime, cyber-vandalism, or something else entirely. We elected to focus on the wider public since the public designation of an act as terrorism has broad political consequences. If an objectively criminal attack is perceived as cyberterrorism by the general public, then this can heighten public fear and distort public confidence in law enforcement. By contrast, if a cyberattack by a terrorist organization is not

perceived as cyberterrorism, then this minimizes the effectiveness of an attack.

Using a rating-based conjoint experimental mechanism, we isolated the extent to which specific incident attributes contribute to the ascription of an attack as cyberterrorism. We take note of several key findings that emerged from the study. Collectively, these results can settle much of the ingrained ambiguity about public opinion and cyberterrorism, and serve as the basis for future research.

Specifically, we observe a clear reticence to associate attacks by non-institutional actors with cyberterrorism. Though it resembles a semantic truism, cyberterrorism is waged by terrorist organizations in the eyes of the public, or at least by a hierarchical organization with ties to a foreign power. By contrast, attacks by individual hackers or loose collectives of hackers do not resemble terrorist attacks. This finding is likely to tamp down the prevalence of the cyberterrorism label, since traditional terrorist organizations have been slow to adopt cyberspace as an attack platform (Gartzke 2013).

Next, we note that even more than for individual hackers, the public is wary of labeling attacks by unknown actors as cyberterrorism. This circumspection is further amplified when the motivation of the attack is unknown. While it was once theorized that seemingly omniscient cyber-perpetrators would terrorize a hapless public, it is now accepted that the absence of any definitive attribution is likely to have the opposite effect, seeing as terrorists crave attention compared to mere cybercriminals that tend to operate in the shadows (Bada and Nurse 2020). This finding offers guidance for governments that increasingly view the public attribution of cyber perpetrators as a strategic decision—and who can “name and shame” an offender to heighten the likelihood that the public will view the attack as terrorism (Egloff 2020).

Our findings partially corroborate past research that identified that only cyberattacks causing physically destructive outcomes would rise to the level of cyberterrorism in terms of the political effects it levies on the public (Shandler et al. 2022). While destructive outcomes substantially increased the likelihood of an attack being viewed as cyberterrorism, surprisingly, the public viewed the dissemination of sensitive digital data as an even graver consequence, and freely attached the label of cyberterrorism to attacks of this sort. This reinforces recent findings that the public views attacks that disseminate sensitive data as seriously as physically destructive attacks (Zubiaga, Procter, and Maple 2018).

This study also revealed that no single cyber instrument (i.e., malware attacks, phishing attacks, etc.) is more reflective of cyberterrorism than any

other. Even reports of a generic “cyberattack” are sufficient to meet the minimum threshold required to raise the specter of cyberterrorism. This finding is a key point of departure from public attitudes to conventional terrorism, where there is an innate ranking of terroristic methods (i.e., bombings imply terrorism, stabbings do not) (Huff and Kertzer 2018).

Finally, our findings speak more broadly to the public opinion literature relating to the overlap between elite guidance and public opinion pertaining to international security (Kertzer and Zeitzoff 2017). A tenet of public opinion and international relations scholarship holds that the public follows elite opinion in developing views on foreign policy and national security issues. We demonstrate that views on cyber issues, where elite guidance is divided, diverge from this classical model. Somehow, despite elite divisions, the public has formed a cohesive cross-national view of cyberterrorism. This finding bears important policy implications—since the uniform public perspective on cyber terrorism may constrain policy elites at the national and international levels in formulating policy due to the robust public norms that have already formed in this area.

Is it pertinent that media coverage of an attack may oftentimes fail to accurately depict the objective facts of an incident? We remain agnostic about this question given that our treatments reflect real-world reports of the kind that readers must frequently evaluate. Since the credibility of an information source can influence decision-making processes, future research would do well to explore the effect of source trustworthiness upon the ascription of an attack as cyberterrorism.

Our multicountry empirical sweep gives us confidence that our findings are not the product of any one mass public, and that the results are robust to national idiosyncrasies. We acknowledge that our empirics focus heavily on Western, democratic, and technologically advanced countries. While this offers a broad set of scope conditions, we must be wary of overbroad generalizations. We conclude by noting that we have identified a highly stable view of cyberterrorism among our cross-national sample, and this perspective diverges from the objective and elite-driven definition of terrorism. As such, this paper reinforces the emergence of a new relationship between public opinion and security issues when it comes to cybersecurity. As cyber-threats become ever more salient, this cleavage is poised to elevate the role of public opinion.

Appendixes

Appendix A. Pooled Results

Table A1 contains the full AMCE results for the pooled sample analysis that appears in figure 2.

Table A1. Average marginal component effect for pooled sample.

Attribute	Level	Estimate	Std. err	z value	p
Agent	Hackers with foreign government ties	0.038	0.010	3.731	.000
Agent	Jihadi Islamic group	0.024	0.010	2.420	.016
Agent	Organization with foreign government ties	0.007	0.011	0.684	.494
Agent	Unaffiliated group of hackers	−0.041	0.011	−3.680	.000
Agent	Individual hacker	−0.073	0.012	−6.257	.000
Agent	Unknown actor	−0.087	0.011	−7.725	.000
Method	Attack	−0.127	0.010	−12.627	.000
Method	USB	−0.013	0.009	−1.347	.178
Method	Phishing	0.013	0.009	1.447	.148
Method	Virus	0.028	0.009	3.141	.002
Motivation	Government overthrow	0.067	0.008	8.015	.000
Motivation	Change government policy	0.042	0.009	4.839	.000
Motivation	Unknown	−0.031	0.009	−3.569	.000
Outcome	Major explosion	0.054	0.013	4.204	.000
Outcome	Theft and release of sensitive information	0.090	0.009	10.106	.000
Outcome	Minor explosion	0.035	0.013	2.743	.006
Outcome	Theft of millions of dollars	0.031	0.009	3.372	.001
Target	Databases	−0.022	0.011	−2.056	.040
Target	Government office building	−0.035	0.009	−3.945	.000
Target	Power station	−0.041	0.009	−4.528	.000
Target	Shopping mall	−0.096	0.009	−10.195	.000

Note: All tests are two-tailed, and all standard errors are clustered at the respondent level.
ACME baseline levels for attributes: Agent = Foreign country; Method = Cyberattack; Motivation = Revenge; Outcome = No damage; Target = Military facility.

Appendix B. Country-Level Results

Appendix B contains the disaggregated country-level AMCE results for analyses appearing in figure 3. Full results associated with the marginal means analyses can be found in Supplementary Material section 3.

Table B1. Average marginal component effect for US sample.

Attribute	Level	Estimate	Std. err	z value	p
Agent	Hackers with foreign government ties	0.033	0.017	1.908	.056
Agent	Jihadi Islamic group	−0.009	0.017	−0.532	.595
Agent	Organization with foreign government ties	0.007	0.018	0.410	.682
Agent	Unaffiliated group of hackers	−0.022	0.019	−1.179	.239
Agent	Individual hacker	−0.034	0.019	−1.759	.079
Agent	Unknown actor	−0.086	0.019	−4.425	.000
Method	Attack	−0.103	0.016	−6.245	.000
Method	USB	−0.027	0.016	−1.722	.085
Method	Phishing	−0.012	0.015	−0.757	.449
Method	Virus	0.001	0.015	0.036	.972
Motivation	Government overthrow	0.041	0.014	2.864	.004
Motivation	Change government policy	0.010	0.015	0.627	.531
Motivation	Unknown	−0.033	0.015	−2.251	.024
Outcome	Major explosion	0.015	0.023	0.634	.526
Outcome	Theft and release of sensitive information	0.049	0.016	3.119	.002
Outcome	Minor explosion	0.021	0.022	0.957	.338
Outcome	Theft of millions of dollars	0.023	0.016	1.497	.135
Target	Databases	−0.013	0.018	−0.693	.488
Target	Government office building	−0.045	0.016	−2.734	.006
Target	Power station	−0.034	0.017	−2.009	.044
Target	Shopping mall	−0.052	0.016	−3.157	.002

Note: All tests are two-tailed, and all standard errors are clustered at the respondent level.
ACME baseline levels for attributes: Agent = Foreign country; Method = Cyberattack; Motivation = Revenge; Outcome = No damage; Target = Military facility.

Table B2. Average marginal component effect for UK sample.

Attribute	Level	Estimate	Std. err	z value	p
Agent	Hackers with foreign government ties	0.040	0.018	2.260	.024
Agent	Jihadi Islamic group	0.047	0.018	2.580	.010
Agent	Organization with foreign government ties	0.013	0.019	0.707	.480
Agent	Unaffiliated group of hackers	-0.052	0.020	-2.630	.009
Agent	Individual hacker	-0.070	0.020	-3.417	.001
Agent	Unknown actor	-0.098	0.020	-4.935	.000
Method	Attack	-0.175	0.018	-9.785	.000
Method	USB	0.018	0.016	1.099	.272
Method	Phishing	0.036	0.016	2.264	.024
Method	Virus	0.043	0.016	2.726	.006
Motivation	Government overthrow	0.116	0.015	7.859	.000
Motivation	Change government policy	0.097	0.015	6.292	.000
Motivation	Unknown	-0.023	0.016	-1.460	.144
Outcome	Major explosion	0.099	0.022	4.414	.000
Outcome	Theft and release of sensitive information	0.133	0.016	8.369	.000
Outcome	Minor explosion	0.079	0.023	3.386	.001
Outcome	Theft of millions of dollars	0.054	0.016	3.278	.001
Target	Databases	-0.018	0.019	-0.906	.365
Target	Government office building	-0.026	0.015	-1.718	.086
Target	Power station	-0.048	0.015	-3.120	.002
Target	Shopping mall	-0.103	0.016	-6.361	.000

Note: All tests are two-tailed, and all standard errors are clustered at the respondent level.

ACME baseline levels for attributes: Agent = Foreign country; Method = Cyberattack; Motivation = Revenge; Outcome = No damage; Target = Military facility.

Table B3. Average marginal component effect for Israel sample.

Attribute	Level	Estimate	Std. err	z value	p
Agent	Hackers with foreign government ties	0.040	0.018	2.260	.024
Agent	Jihadi Islamic group	0.040	0.018	2.259	.024
Agent	Organization with foreign government ties	0.005	0.018	0.290	.772
Agent	Unaffiliated group of hackers	−0.050	0.019	−2.674	.008
Agent	Individual hacker	−0.117	0.021	−5.597	.000
Agent	Unknown actor	−0.075	0.020	−3.843	.000
Method	Attack	−0.109	0.018	−6.244	.000
Method	USB	−0.030	0.017	−1.779	.075
Method	Phishing	0.014	0.016	0.899	.369
Method	Virus	0.041	0.015	2.714	.007
Motivation	Government overthrow	0.045	0.014	3.197	.001
Motivation	Change government policy	0.023	0.014	1.567	.117
Motivation	Unknown	−0.039	0.015	−2.636	.008
Outcome	Major explosion	0.056	0.022	2.574	.010
Outcome	Theft and release of sensitive information	0.094	0.015	6.380	.000
Outcome	Minor explosion	0.013	0.022	0.591	.555
Outcome	Theft of millions of dollars	0.019	0.016	1.200	.230
Target	Databases	−0.034	0.017	−1.955	.051
Target	Government office building	−0.033	0.015	−2.177	.029
Target	Power station	−0.039	0.015	−2.596	.009
Target	Shopping mall	−0.130	0.016	−7.914	.000

Note: All tests are two-tailed, and all standard errors are clustered at the respondent level.
ACME baseline levels for attributes: Agent = Foreign country; Method = Cyberattack; Motivation = Revenge; Outcome = No damage; Target = Military facility.

Supplementary Material

Supplementary Material may be found in the online version of this article: <https://doi.org/10.1093/poq/nfad006>.

Acknowledgements

This article benefited greatly from feedback at the 2021 Annual Conference of the International Studies Association, and a 2021 workshop on Original Policy Research at Georgia Institute of Technology. The study was born out of a stimulating 2019 cyberterrorism symposium at the University of Haifa. We appreciate the generous input of the article reviewers and journal editors.

Data Availability

Replication data and documentation are available at <https://doi.org/10.7910/DVN/FU62PS>.

References

- Ackerman, Spencer. 2012. "DHS Crushed This Analyst for Warning About Far-Right Terror." *Wired*, August 7. <https://www.wired.com/2012/08/dhs/>
- Almond, Gabriel A. 1950. *The American People and Foreign Policy*. New York: Harcourt, Brace and Company.
- Backhaus, Sophia, Michael L. Gross, Israel Waismel-Manor, Hagit Cohen, and Daphna Canetti. 2020. "A Cyberterrorism Effect? Emotional Reactions to Lethal Attacks on Critical Infrastructure." *Cyberpsychology, Behavior and Social Networking* 23:595–603.
- Bada, Maria, and Jason R. C. Nurse. 2020. "The Social and Psychological Impact of Cyberattacks." In *Emerging Cyber Threats and Cognitive Vulnerabilities*, edited by Vladlena Benson and John McAlaney, 73–92. London: Academic Press.
- Barari, Soubhik, Elissa Berwick, Jens Hainmueller, Daniel Hopkins, Sean Liu, Anton Strezhnev, and Teppei Yamamoto. 2018. "Cjoint: AMCE Estimator for Conjoint Experiments." R Package Version 2. <https://cran.r-project.org/web/packages/cjoint/cjoint.pdf>.
- Baum, Matthew A., and Tim Groeling. 2010. "Reality Asserts Itself: Public Opinion on Iraq and the Elasticity of Reality." *International Organization* 64:443–79.
- Baum, Matthew A., and Philip B. K. Potter. 2015. *War and Democratic Constraint: How the Public Influences Foreign Policy*. New Jersey: Princeton University Press.
- Branch, Jordan. 2021. "What's in a Name? Metaphors and Cybersecurity." *International Organization* 75:39–70.
- Brenan, Megan. 2021. "Cyberterrorism Tops List of 11 Potential Threats to U.S. Gallup." Gallup, March 22. <https://news.gallup.com/poll/339974/cyberterrorism-tops-list-potential-threats.aspx>.
- Canetti, Daphna, Joshua R. Gubler, and Thomas Zeitzoff. 2021. "Motives Don't Matter? Motive Attribution and Counter-Terror Policy." *Political Psychology* 42:483–99.
- Canetti-Nisim, Daphna, Eran Halperin, Keren Sharvit, and Stevan E. Hobfoll. 2009. "A New Stress-Based Model of Political Extremism: Personal Exposure to Terrorism, Psychological Distress, and Exclusionist Political Attitudes." *Journal of Conflict Resolution* 53:363–89.
- Canfil, Justin K. 2022. "The Illogic of Plausible Deniability: Why Proxy Conflict in Cyberspace May No Longer Pay." *Journal of Cybersecurity* 8:tyac007.
- Chamberlain, Samuel. 2021. "Lindsey Graham Rips Biden's 'Naive,' 'Weak' Response to Colonial Pipeline Cyberattack." *New York Post*, 13 May. <https://nypost.com/2021/05/13/lindsey-graham-rips-bidens-weak-response-to-colonial-pipeline-cyberattack/>.
- Critifence. 2018. "2018 Critical Infrastructure Cyber Attack Timeline." *Critifence*, September 18. <http://www.critifence.com/blog/2018-critical-infrastructure-cyber-attack-timeline/>
- Denning, Dorothy. 2000. "Cyberterrorism: Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Services, U House of Representatives." <http://www.stealth-iss.com/documents/pdf/cyberterrorism.pdf>
- D'Orazio, Vito, and Idean Salehyan. 2018. "Who Is a Terrorist? Ethnicity, Group Affiliation, and Understandings of Political Violence." *International Interactions* 44:1017–39.
- Dunn Cavelty, Myriam. 2019. "The Materiality of Cyberthreats: Securitization Logics in Popular Visual Culture." *Critical Studies on Security* 7:138–51.
- Egloff, Florian J. 2020. "Public Attribution of Cyber Intrusions." *Journal of Cybersecurity* 6: 1–12.

- Enders, Walter, and Todd Sandler. 2011. *The Political Economy of Terrorism*. Cambridge: Cambridge University Press.
- Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38:41–73.
- Geis, Anna, and Carmen Wunderlich. 2014. "The Good, the Bad, and the Ugly: Comparing the Notions of 'Rogue' and 'Evil' in International Politics." *International Politics* 51:458–74.
- Getmansky, Anna, and Thomas Zeitzoff. 2014. "Terrorism and Voting: The Effect of Rocket Threat on Voting in Israeli Elections." *American Political Science Review* 108:588–604.
- Gomez, Miguel Alberto, and Christopher Whyte. 2021. "Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats." *International Studies Quarterly* 65: 1137–50.
- Greszki, Robert, Marco Meyer, and Harald Schoen. 2015. "Exploring the Effects of Removing 'Too Fast' Responses and Respondents from Web Surveys." *Public Opinion Quarterly* 79: 471–503.
- Groeling, Tim, and Matthew A. Baum. 2008. "Crossing the Water's Edge: Elite Rhetoric, Media Coverage, and the Rally-Round-the-Flag Phenomenon." *Journal of Politics* 70:1065–85.
- Gross, Michael L. 2018. "Moral Dilemmas of Asymmetric Conflict." In *The Oxford Handbook of International Political Theory*, edited by Chris Brown and Robyn Eckersley, 233–46. Oxford: Oxford University Press.
- Gross, Michael L, Daphna Canetti, and Dana R. Vashdi. 2016. "The Psychological Effects of Cyber Terrorism." *The Bulletin of the Atomic Scientists* 72:284–91.
- Gross, Michael L., Daphna Canetti, and Dana R. Vashdi. 2017. "Cyberterrorism: Its Effects on Psychological Well-Being, Public Confidence and Political Attitudes." *Journal of Cybersecurity* 3:49–58.
- Hainmueller, Jens, and Daniel J. Hopkins. 2015. "The Hidden American Immigration Consensus: A Conjoint Analysis of Attitudes Toward Immigrants." *American Journal of Political Science* 59:529–48.
- Hainmueller, Jens, Daniel J. Hopkins, and Teppei Yamamoto. 2014. "Causal Inference in Conjoint Analysis: Understanding Multidimensional Choices via Stated Preference Experiments." *Political Analysis* 22:1–30.
- Henschke, Adam. 2021. "Terrorism and the Internet of Things: Cyberterrorism as an Emergent Threat." In *Counter-Terrorism, Ethics and Technology*, edited by Adam Henschke, Alastair Reed, Scott Robbins, and Seumas Miller, 71–87. Cham: Springer.
- Hoffman, Bruce. 2006. *Inside Terrorism*. New York: Columbia University Press.
- Huddy, Leonie, Stanley Feldman, Charles Taber, and Gallya Lahav. 2005. "Threat, Anxiety, and Support of Antiterrorism Policies." *American Journal of Political Science* 49:593–608.
- Huff, Connor, and Joshua D. Kertzer. 2018. "How the Public Defines Terrorism." *American Journal of Political Science* 62:55–71.
- Jarvis, Lee, and Stuart Macdonald. 2015. "What Is Cyberterrorism? Findings from a Survey of Researchers." *Terrorism and Political Violence* 27:657–78.
- Jarvis, Lee, Stuart Macdonald, and Andrew Whiting. 2017. "Unpacking Cyberterrorism Discourse: Specificity, Status, and Scale in News Media Constructions of Threat." *European Journal of International Security* 2:64–87.
- Jarvis, Lee, Lella Nouri, and Andrew Whiting. 2014. "Understanding, Locating and Constructing Cyberterrorism." In *Cyberterrorism*, edited by Thomas M. Chen, Lee Jarvis, and Stuart Macdonald, 25–41. New York: Springer.
- Kertzer, Joshua D., and Thomas Zeitzoff. 2017. "A Bottom-Up Theory of Public Opinion about Foreign Policy." *American Journal of Political Science* 61:543–58.
- Kimhi, Shaul, Daphna Canetti-Nisim, and Gilad Hirschberger. 2009. "Terrorism in the Eyes of the Beholder: The Impact of Causal Attributions on Perceptions of Violence." *Peace and Conflict: journal of Peace Psychology* 15:75–95.

- Konow-Lund, Maria, and Eva-Karin Olsson. 2017. "Social Media's Challenge to Journalistic Norms and Values during a Terror Attack." *Digital Journalism* 5:1192–204.
- Kostyuk, Nadiya, and Carly Wayne. 2021. "The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public." *Journal of Global Security Studies* 6:1–25.
- Kreps, Sarah, and Debak Das. 2017. "Warring from the Virtual to the Real: Assessing the Public's Threshold for War Over Cyber Security." *Research & Politics* 4:1–8.
- Lawson, Sean T. 2019. *Cybersecurity Discourse in the United States: Cyber-Doom Rhetoric and Beyond*. Abingdon: Routledge.
- Leeper, Thomas J. 2020. "Cregg: Simple Conjoint Analyses and Visualization." R Package Version 0.4.0. <https://cran.r-project.org/web/packages/cregg/cregg.pdf>.
- Leeper, Thomas J., Sara B. Hobolt, and James Tilley. 2020. "Measuring Subgroup Preferences in Conjoint Experiments." *Political Analysis* 28:207–21.
- Lin-Greenberg, Erik. 2021. "Soldiers, Pollsters, and International Crises: Public Opinion and the Military's Advice on the Use of Force." *Foreign Policy Analysis* 17:orab009.
- Liu, Mingnan, and Laura Wronski. 2018. "Examining Completion Rates in Web Surveys via Over 25,000 Real-World Surveys." *Social Science Computer Review* 36:116–24.
- Luijijf, Eric. 2014. "Definitions of Cyber Terrorism." In *Cyber Crime and Cyber Terrorism Investigator's Handbook*, edited by Babak Akhgar, Andrew Staniforth, and Francesca Bosco, 11–7. Waltham: Elsevier.
- Montalvo, Jose G. 2011. "Voting After the Bombings: A Natural Experiment on the Effect of Terrorist Attacks on Democratic Elections." *Review of Economics and Statistics* 93:1146–54.
- Murray, Gregg R., Craig Douglas Albert, Kim Davies, Candace Griffith, John Heslen, Lance Y. Hunter, Nadia Jilani-Hyler, and Sudha Ratan. 2019. "Toward Creating a New Research Tool: Operationally Defining Cyberterrorism." <https://osf.io/uk3z7>.
- R Core Team. 2022. *R: A Language and Environment for Statistical Computing*. Vienna: R Foundation for Statistical Computing. <https://www.R-project.org/>
- Rid, Thomas. 2013. *Cyber War Will Not Take Place*. Oxford: Oxford University Press.
- Rid, Thomas, and Ben Buchanan. 2015. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38:4–37.
- Sanger, David E. and Nicole Perlroth. 2021. "Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity." *New York Times*, May 14. <https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html>.
- Sevenans, Julie. 2021. "How Public Opinion Information Changes Politicians' Opinions and Behavior." *Political Behavior* 43:1801–23.
- Shandler, Ryan, Michael L. Gross, and Daphna Canetti. 2023. "Cyberattacks, Psychological Distress, and Military Escalation: An Internal Meta-Analysis." *Journal of Global Security Studies* 8. <https://doi.org/10.1093/jogss/ogac042>.
- Shandler, Ryan, and Miguel Alberto Gomez. 2022. "The Hidden Threat of Cyber-Attacks—Undermining Public Confidence in Government." *Journal of Information Technology & Politics* 1–16.
- Shandler, Ryan, Michael L. Gross, Sophia Backhaus, and Daphna Canetti. 2022. "Cyber Terrorism and Public Support for Retaliation—A Multi-Country Survey Experiment." *British Journal of Political Science* 52:850–68.
- Shandler, Ryan, Michael L. Gross, and Daphna Canetti. 2021. "A Fragile Public Preference for Cyber Strikes: Evidence from Survey Experiments in the United States, United Kingdom, and Israel." *Contemporary Security Policy* 42:135–62.
- Shandler, Ryan, Keren L. G. Snider, and Daphna Canetti. 2022. "The Political Psychology of Cyberterrorism." In *Cambridge Handbooks in Psychology*, edited by Danny Osborne and Chris G. Sibley, 565–81. Cambridge: Cambridge University Press.

- Shechory-Bitton, Mally, and Keren Cohen-Louck. 2018. "Does Fear of Terrorism Differ from Fear of Crime and Sexual Assault: A Question of Geographical Location and Residential Area." *International Journal of Offender Therapy and Comparative Criminology* 62:806–26.
- Snider, Keren L. G., Ryan Shandler, Sharon Matzkin, and Daphna Canetti. 2022. "The Political Psychology of Terrorism." In *The Oxford Handbook of Political Psychology*, edited by Leonie Huddy, David Sears, Jack Levy, and Jennifer Jerit. Oxford: Oxford University Press.
- Snider, Keren L. G., Ryan Shandler, Shay Zandani, and Daphna Canetti. 2021. "Cyberattacks, Cyber Threats, and Attitudes Toward Cybersecurity Policies." *Journal of Cybersecurity* 7: tyab019.
- Stroobants, Serge. 2018. "Cyberterrorism Is the New Frontier." *Global Terrorism Index 2018*. <http://visionofhumanity.org/app/uploads/2018/12/Cyberterrorism-is-the-new-frontier-1.pdf>.
- U.S. Congress, House of Representatives, Committee on Environment and Public Works. 2016. *Foreign Cyber Threats: Small Businesses, Big Target, 114th Cong., 2nd Sess., 1–2*.
- Valeriano, Brandon, and Ryan C. Maness. 2015. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press.
- Weimann, Gabriel. 2012. "Lone Wolves in Cyberspace." *Journal of Terrorism Research* 3: 75–90.
- Wheeler, Tarah, and Bruce Schneier. 2021. "Hacked Drones and Busted Logistics Are the Cyber Future of Warfare." Brookings. <https://www.brookings.edu/techstream/hacked-drones-and-busted-logistics-are-the-cyber-future-of-warfare/>.
- Young, Joseph K., and Michael G. Findley. 2011. "Promise and Pitfalls of Terrorism Research." *International Studies Review* 13:411–31.
- Zeitoff, Thomas. 2014. "Anger, Exposure to Violence, and Intragroup Conflict: A 'Lab in the Field' Experiment in Southern Israel." *Political Psychology* 35:309–35.
- Zeri, Norshahida Noor, and Noor Nirwandy Mat Noordin. 2017. "Framing Cyberterrorism: A Content Analysis of the *New York Times*." *Journal of Media and Information Warfare* 9: 179–200.
- Zubiaga, Arkaitz, Rob Procter, and Carsten Maple. 2018. "A Longitudinal Analysis of the Public Perception of the Opportunities and Challenges of the Internet of Things." *PLoS One* 13:1–18.