Responding to Uncertainty: The Importance of Covertness in Support for Retaliation to Cyber and Kinetic Attacks

Kathryn Hedgecock and Lauren Sukin *†

February 26, 2022

Abstract

This paper investigates the escalation dynamics of cyber attacks. Two main theories have been advanced. First, "means-based" theory argues attack type determines response; cyber attacks are less likely to escalate than kinetic attacks. Second, "effects-based" theory argues an attack's material consequences determine the likelihood of retaliation. We advance a third perspective, arguing that the covertness of an attack has the largest effect on its propensity towards escalation. We identify two characteristics of covertness that affect support for retaliation: the certainty of attribution and its timing. We use a survey experiment to assess public support for retaliation, while varying the means, effects, timing, and attribution certainty of attacks.[1] We find no evidence for the effects-based approach, instead finding high levels of support for retaliation regardless of an attack's scale. We find that the most significant contributor to support for retaliation is an attack's covertness.

*Kathryn Hedgecock holds a Ph.D. in Political Science from Stanford University and serves as an Assistant Professor in International Affairs at the United States Military Academy at West Point. Lauren Sukin is a Stanford University Political Science Ph.D. Candidate and Pre-Doctoral Fellow at the Center for International Security and Cooperation. Contact: 616 Jane Stanford Way, Stanford CA 94305, (650) 723-1806.

†**Acknowledgements:** For comments and suggestions, the authors thank: Leah Matchett, Joshua Goldstein, Scott Sagan, Jacquelyn Schneider, Kenneth Schultz, and Michael Tomz. The authors thank the Stanford Center for American Democracy for their funding and support.

1. This survey experiment was pre-registered and was conducted in compliance with human subject research laws. The survey experiment was deemed exempt and approved by the institutional review board.

1 Introduction

In December 2020, the prestigious cybersecurity firm FireEye revealed they were the victim of a state-sponsored hack (Sanger and Perlroth 2020). Soon, the extent of the exploit began to unfold; universities, hospitals, and federal government agencies announced that they, too, had been hacked. Government officials publicly attributed the exploit to Russia, and support for retaliation swiftly followed. Bipartisan calls for retaliation sounded from figures as diverse as then President-elect Joe Biden and Senator Marco Rubio (R-FL). This cyber operation, colloquially referred to as SolarWinds,[2] is considered one of the largest hacks in history by a state actor (Heath 2021). The sharp bipartisan calls for retaliation against the attack challenge a commonly held idea that cyber attacks are non-escalatory (Kreps and Schneider 2019; Tomz et al. 2020; Kostyuk and Wayne 2020).

The SolarWinds hack highlighted the need to better understand the consequences of cyber attacks in the public domain, including when and how pressures towards escalation emerge. Ultimately, the Biden Administration leveled sanctions against Russia, promised additional "seen" and "unseen" actions, and designed an executive order to enhance domestic cybersecurity (Temple-Raston 2021). In seeking to understand how states choose to respond to cyber attacks like SolarWinds,[3] one important consideration is the significant public debate that surrounds them.

Scholars have suggested public support for conflict may encourage governments to engage, while public opposition to conflict can restrain government behavior (Tomz and Weeks

2. The hack is named for the Texas-based software company that was the source of the exploit.

3. Some scholars have argued cyber operations do not rise to the threshold of an attack until they cause damage equivalent to that produced by a kinetic attack (Fidler 2016; Gartzke 2013; Rid 2012). While we use the term attack to broadly refer to hostile cyber operations, including those whose aim is espionage, we recognize the distinction between different types of cyber operations.

2020; Kertzer and Brutger 2016; Levendusky and Horowitz 2012; Haesebrouck 2019; Kertzer et al. 2020). Currently, there is only a nascent literature on how the public reacts to cyber attacks. Survey work has found the public is less likely to support retaliation against cyber operations than against kinetic operations that produce the same effects (Kreps and Schneider 2019). It is not particularly clear why this is: psychological responses to cyber and conventional terrorism are similar (Gross et al. 2016); and individual concern about cybersecurity issues to be low and resistant to change (Kostyuk and Wayne 2020). At least the scale of the cyber attack does seem to matter: scholars have found support for retaliation against cyber attacks that produce casualties (Kreps and Das 2017; Shandler et al. 2021), but a preference for restraint in response to electoral interference (Tomz et al. 2020). Existing experimental surveys provide an important foundation, but they leave many questions unanswered. Most essentially, while some existing research has found that attitudes about cyber and kinetic conflicts differ, existing surveys generally do not address the *mechanisms* by which these differences arise.

We use a vignette survey experiment to better understand public attitudes about cyber attacks. We identify the conditions under which the public supports retaliation against such operations, and we delineate the differences between public perceptions of cyber and kinetic attacks. In doing so, we depart from existing work by seeking to understand the specific mechanisms that underpin attitudes about cyber attacks. In particular, we find that the clandestine nature of attacks common in the cyber domain, with long discovery times and uncertain attribution, dampen support for retaliation. We find that physical attacks that are similarly covert are also less likely to prompt support for retaliation. This previously understudied feature of attacks can help us understand cases like SolarWinds, where a high certainty cyber attack led to public calls for retaliation, while shedding light on why many other instances of hostile cyber operations do not result in such calls.

2 Attitudes on Cyber and Kinetic Conflict

Despite its increasing prevalence in the world, research on the cyber domain has yet to reach a conclusion on whether retaliation for a cyber operation is more likely to lead to deterrence or escalation (Fischerkeller and Harknett 2017; Lin 2012; Libicki 2012). Empirical research is hindered by the challenges of accurately capturing cases of cyber operations. Great variation among cyber attacks, coupled with the difficulties of gathering data on covert actions, makes it challenging to advance and test theoretical claims.

One approach to negotiate this uncertainty is to better understand how the public reacts to cyber (versus kinetic) attacks. Public opinion surveys circumvent the operational challenges of collecting empirical data on often-classified responses to often-covert cyber operations, while lending insight into the micro-foundations of how these operations are understood. In doing so, public opinion surveys provide insight into the dynamics policymakers may consider when facing offensive cyber operations. Survey research has been shown to effectively predict policymaker attitudes on foreign policy topics (Kertzer et al. 2020; Tomz et al. 2020). In addition, public opinion surveys present information about the conditions that policymakers might face when evaluating a cyber attack, since policymakers, particularly in democracies, must take into account public support or opposition when designing security policies (Fearon 1994; Schultz 1999; Tomz 2007).

In the small number of existing surveys on cyber operations, scholars have found public support for retaliation to cyber attacks is distinct from support for retaliation to kinetic attacks. However, surveys have generally not examined the mechanisms behind this distinction. We investigate three theorized mechanisms to identify which differences between cyber and kinetic attacks underpin public attitudes: the type of attack, the means of attack, and the covertness of the attack. We argue that the covert nature of attacks is essential to understanding the response.

2.1 Type of Attack

Even when cyber and kinetic attacks result in similar outcomes, they can be distinguished by their means of delivery. Cyber attacks are delivered via information and communication technologies (ICTs), while kinetic attacks are delivered in the physical domains of land, air, or sea. Through these distinct methods, cyber and kinetic attacks can produce analogous effects. For example, in 2014, a cyber attack on an industrial control system at a German steel mill led to the physical destruction of a blast furnace. These same effects could have been achieved utilizing a kinetic method, such as bombing.

In order to study cyber and kinetic attacks as unique 'types' of attacks, it is important to hold constant the effects of an attack and to focus solely on the means of delivery. The idea that an attack being delivered by cyber means would change the perception of the attack relative to one that caused the same effects kinetically is referred to as the "means-based" theory (Farrell and Glaser 2017). Previous survey and wargame research supports means-based theory, finding that the public displays greater reluctance to retaliate against cyber than kinetic attacks (Kreps and Schneider 2019; Kreps and Das 2017; Schneider 2017; Tomz and Weeks 2020; Shandler et al. 2021). This suggests the following hypothesis:

H_1 : *The public will be more likely to support retaliation against kinetic attacks than cyber attacks with effects of the same magnitude.*

Our survey experiment is designed to understand *what features* of cyber attacks drive differential attitudes about these attacks relative to their kinetic counterparts. If we identify the features by which cyber and kinetic attacks differ, then we should expect that the independent effect of an attack's means—beyond these elements—would be negligible. As a result, we expect only a small, residual difference between cyber attacks and kinetic attacks once we control for key features that distinguish these methods of attack.

However, attitudes about *how* retaliation should occur could vary; respondents may be more likely to prefer within-domain retaliation (e.g. to respond to cyber attacks with cyber means) than cross-domain retaliation (e.g. to respond to cyber attacks with kinetic means). While tit-for-tat reciprocity may be perceived as proportionate or fair among respondents, public opinion research has often demonstrated preferences for disproportionate responses to attacks, perhaps driven by vengeful attitudes (Sagan and Valentino 2019b, 2019a). The current U.S. doctrine supports cross-domain deterrence. But, in practice, determining a proportionate, within-domain response for a cyber operation can be difficult (E. Gartzke and J.R. Lindsay 2019; Brantly 2018b).

2.2 Magnitude of Effects

Regardless of an attack's means, the consensus states desire for retaliation should vary in response to the magnitude of an attack's effects. Smaller, less consequential attacks should generate less support for retaliation, while attacks that cause massive damage or loss of life should evoke greater support (Kreps and Das 2017; Shandler et al. 2021). This logic should hold for both cyber and kinetic attacks. We, in turn, expect demand for retaliation to increase as the scale of the damage caused by an attack increases, irrespective of its means. This constitutes the "effects-based" theory (Farrell and Glaser 2017).

H_2 : *Regardless of the means of delivery, public support for retaliation will increase as the effects of the attack increase in scale.*

While it is possible for a cyber attack to cause physical damage, some scholars point out the implausibility of cyber attacks rising to a level that would constitute an act of war (Rid 2012; Gartzke 2013; Kello 2013). Instead, cyber operations are often viewed as a complement to force, due to their generally limited effects. Some scholars have argued cyber attacks must

impose equivalent physical consequences as a kinetic attack in order to legally 'count' as a use of force and, in turn, enable the attacked state to execute on its right to self-defense (Fidler 2016; Buchan 2012).

Existing survey research focuses principally on testing the means and effects-based theories. Kreps and Schneider (2019) and Kreps and Das (2017) find support for retaliation generally increases as the magnitude of an attack's effects increases. Kreps and Schneider also find support for the means-based theory, suggesting there are domain distinctions beyond attacks' effects that influence public attitudes. In contrast, Shandler et al.(Shandler et al. 2021) find support for means-based theory until cyber attacks cross a *lethality threshold*, at which point the public does not distinguish by means. Little empirical work has investigated how cyber and kinetic means may differ beyond questions of the likely magnitude of each type of attack. In this paper, we suggest that a primary difference between cyber and kinetic attacks is the often-covert nature of cyber operations, which results in uncertain attribution. The following section explores this major feature of cyber operations and argues it may play an important role in distinguishing how cyber operations are perceived relative to their kinetic counterparts.

2.3 Covertness

Cyber operations are often clandestine and covert. With the exception of ransomware, distributed denial of service (DDoS), and defacement, a majority of state-sponsored cyber operations must remain hidden in order to achieve their objectives (Erik Gartzke and Jon Lindsay 2015). Even in cases where secrecy cannot be achieved, virtually all cyber operations are designed to conceal the identity of the sponsor, and states usually do not claim credit for cyber operations against other states (Poznansky and Perkoski 2018; Maurer 2018). Together, the covert nature of cyber operations and the absence of credit-claiming create an 'attribution problem' in cyberspace (Clark and Landau 2011; Kello 2013; Nye 2017; Poznan-

sky and Perkoski 2018). The covert nature of cyber operations lends itself to two distinct attribution problems: one posed by the degree of certainty associated with attributing the perpetrator's identity and another posed by delays caused by difficulties in detection and attribution (Brantly 2016; Lindsay 2015; Rid and Buchanan 2015; Erik Gartzke and Jon Lindsay 2015).

In contrast, the presence of physical weaponry or combatants often makes the origin of kinetic attacks easier to identify. Although there are cases of physical operations where attribution is not certain—such as when actors deny involvement in 'grey zone conflict' or use proxies—this situation is relatively rare compared to the cyber domain. In addition, the physical evidence involved in kinetic operations usually makes attribution possible (Cormac and Aldrich 2018), even in 'tough' cases (consider, for example, Russia's "little green men" in the 2014 Ukraine crisis). Attribution of kinetic attacks is often achieved either through human intelligence or credit-claiming (Carson 2018; Carson and Yarhi-Milo 2017; Lieber and Press 2013; Miller 2007). There are fewer incentives to credit-claim in the cyber domain and significantly more challenges for human intelligence. However, this key difference between the domains has been under-explored in previous empirical work.

As attribution challenges in the cyber domain abound and attribution problems in kinetic conflict become more common, understanding the implications of the attribution process is increasingly politically pressing. Indeed, only about 3 in 1,000 cybercrimes are ever prosecuted (Garcia and Eoyang 2020). Meanwhile, militaries increasingly rely on contractors and non-state actors while emerging technologies make fast attribution more important and more difficult (Johnson 2020; Cormac and Aldrich 2018; Mumford 2013).

Attribution problems are important because they raise serious barriers to deterrence by punishment as the threat of reciprocal actions can only be taken when it is clear upon whom punishment should be leveled (Nye 2017). In cases where states can establish attribution, there may still be skepticism about the reliability of attribution claims due to denials by

the attack's sponsor and an incentive on behalf of the victim state to withhold technical details of how attribution was determined (Egloff and Wenger 2019). Retaliation to uncertainly attributed attacks is therefore difficult; retaliation against the wrong actor could have significant adverse consequences, and retaliation against the right actor may still draw condemnation if there is ambiguity or deniability. If this insight is understood by the public, then covert attacks should be less likely to lead to calls for retaliation. While we expect that attribution certainty will increase public support for retaliation to both cyber and kinetic attacks, attribution is empirically much more difficult for cyber than kinetic operations, meaning an attribution certainty effect would disproportionately impact cyber operations in the real world. We predict the following:

H_{3a} : *As the attribution certainty of an attack increases, support for retaliation increases.*

A related challenge is the timing of attribution. Despite the adage that 'revenge is a dish best served cold,' retaliation is often believed to be most appropriate when served hot (Brantly 2018b). A more recently attributed attack should elicit greater support for retaliation. When attacks are discovered or attributed months or years later, their salience will be lower, as will the perceived costs of not responding.[4] Policymakers and the public may be less willing to devote resources towards responding to an 'old' attack; they may also assume more distant attacks were more low-impact, since their depth and breadth were not immediately evident. Additionally, responding to attacks after a significant delay may have less utility. The organization that conducted the attack may have a new set of actors who may not feel accountable for the original attack. Technologies and techniques may have evolved such that an in-kind response would be difficult, outdated, or ineffective, such that:

4. Governments and third-party actors can also make calculated choices with regards to attribution timing.

H_{3b} : *As the time since an attack becomes more distant, support for retaliation will decrease.*

These dynamics appear in both cyber and kinetic operations, although attribution is usually more challenging for cyber operations. Attribution could, however, become an increasingly important problem in the kinetic domain as the use of proxies increases and militaries integrate emerging technologies, such as AI decision-making systems, that complicate and increase the need for effective attribution (Johnson 2020). Like with attribution certainty, if attribution delays reduce support for retaliation, both covert physical and covert cyber attacks would be affected by this dynamic, but it would be disproportionately relevant in the cyber domain.

Attribution dynamics have featured in various theoretical studies, particularly in the cyber domain. However, there have been few empirical tests to this end. Thus, this research provides novel insight into a critical and understudied feature of attacks. We also test a number of other features that may distinguish cyber and kinetic means, including the novelty of cyber operations, the public's exposure to cybersecurity threats, and attitudes about deterrence and escalation in the cyber and kinetic domains. However, we theorize and find that the most influential features of attacks relate to their covertness.

3 Experimental Design

We design and implement a vignette survey experiment on a representative sample of 2,797 Americans using Lucid's Marketplace platform, which leverages online survey panels. The sample is balanced through the use of quotas on age, gender, income, and education.[5] Each

5. See Appendix A. 4,444 total respondents were sampled. Respondents were dropped if they did not consent to participate, failed the attention check, or did not receive the treatment and could not correctly identify the target of the attack described in the vignette. Robustness tests in Appendix C include respondents who incorrectly answered the mechanism check and attention check questions and affirm our main

participant was given a scenario describing an attack against New York City. Respondents were asked about their support for U.S. military retaliation. Characteristics of the attack were randomized across four main parameters: *type*, *scale*, *attribution certainty*, and *timing*. The language of the treatment is provided below with each randomized factor in italics.

> "Imagine that terrorist operatives conducted a [*type*] against the United States [*timing*]. The operatives targeted the [*scale*]. Government officials have [*attribution certainty*] that the attack was perpetrated by an organization of [*type*] terrorists, called Red Square[6], that is sponsored by the Russian government."

Type compares terrorist attacks conducted via two distinct means, cyber or kinetic. Each respondent received one of two characterizations: *"terrorist operatives have conducted a cyber attack"* or *"terrorist operatives have conducted a physical, in person attack'*. Respondents who were assigned the cyber attack treatment were also told that the attack was *"perpetrated by an organization of cyberterrorists,"* while respondents who were assigned the kinetic attack treatment were told the attack was *"perpetrated by an organization of terrorists."*

Our survey holds constant the effects of cyber and physical attacks. We chose a conventional parallel to a cyber attack that would be highly similar in every way except the means of delivery: a terrorist attack.[7] We selected a terrorist attack as our comparison in order to control for two common features of cyber attacks: that they can be conducted by non-state actors and that they usually cause low-scale damage. Terrorist attacks cause less damage than other types of conventional attacks, making them a more plausible comparison

results hold.

6. The authors acknowledge that the organization's name is a location in Russia. To prevent confusion for the respondents, Red Square it was prefaced with "the terrorist organization" or asked about the group's Headquarters. A review of open-ended questions find no support that individuals mistook Red Square for the location.

7. Kreps and Das' (2017) foundational survey does not use a non-cyber control. Kreps and Schneider (2019) do vary means as a feature of their experiment. They offer a conventional attack as an alternative to a cyber attack, but their conventional scenario involves a state actor, rather than a state-sponsored proxy. Kreps and Schneider (2019) also include a nuclear attack treatment.

to a cyber attack than a state's military attacking the United States. Moreover, Gross et al. (2016) found that respondents perceive attacks by cyberterrorist and terrorists to be similarly threatening.[8] Because the"terrorism" label is applied to both the cyber and kinetic attacks, the attacks are highly comparable. To be sure that cyberterrorists and terrorists were viewed similarly by respondents, we randomly assessed respondents' perceptions of these actors in a pre-treatment question battery. While there are some differences in views about these groups, our findings suggest respondents have similar baseline perceptions of cyberterrorists and terrorists.[9] For example, cyberterrorists are not seen as any more or less likely to be "white," "dangerous," "evil," "rational," or "predictable."[10] This suggests that pre-existing conceptions about these actors should not explain any differences between respondents' reactions to their attacks.

The scale of the damage caused by the attack is randomized among four outcomes: information theft, financial theft, infrastructure destruction, and loss of life. Table 1 outlines these treatments. These four treatments were selected to mirror plausible cyber capabilities familiar to a casual news consumer. The treatments are intentionally less catastrophic than those used in previous surveys in order to enable better understanding of likely real-world reactions to cyber attacks. By using attack scenarios in which there is low or minimal damage inflicted, we bias against our argument that cyber and kinetic attacks will be treated differently in the public eye. Like other surveys, we provide a treatment in which the attack is lethal. To account for the possibility that respondents primarily respond to whether damage is physical (Rid 2012; Gartzke 2013; Libicki 2012), we include both physical and non-physical attacks.

8. They also find that cyberterrorism provokes a similar anxiety among respondents whether lethal or not, while the level of anxiety among conventional terrorism differs between lethal and non-lethal attacks.

9. See Appendix I.

10. The significant differences are generally substantively small. For example, cyberterrorists are 4 percentage points more likely to be seen as operating alone, 8 percentage points more likely to be "ideological," and 10 percentage points less likely to be "well-funded."

	Physical	**Non-Physical**
High Cost	The operatives targeted the **electrical grid** in New York City, resulting in **extensive power outages that caused a large number of deaths.**	The operatives targeted **financial institutions** in New York City, resulting in the **theft of large amounts of money.**
Low Cost	The operatives targeted the **electrical grid** in New York City, resulting in **widespread power outages.**	The operatives targeted the **municipal archives** in New York City, resulting in the **theft of large amounts of personally identifiable information.**

Table 1: Factorial Treatments for the Scale of an Attack

The attribution certainty variable has two levels: *"low confidence"* and *"high confidence."* This language was chosen to reflect intelligence estimates from the United States National Intelligence Agency when categorizing cyber attribution (*A Guide to Cyber Attribution* 2018).[11] The simplicity of the terminology prevents respondents from introducing alternative interpretations that may be associated with percentages or additional adjectives. This allows us to test how attribution certainty—a core challenge in cyber operations—affects attitudes about retaliation. We anticipate this will be a critical feature shaping public perceptions.

The timing parameter has two factors reflecting the date of the attack: *"more than a year ago"* and *"recently"*. We include attack date to assess how the passage of time may influence the desire to retaliate or respond. Slow discovery and attribution processes make timing a critical factor for cyber operations. In this sense, timing is another feature of covertness, as covert attacks may suffer from attribution problems—or enable governments to strategically obscure and reveal attribution. Thus timing is not an independent feature of attacks but a secondary test of the effects of attribution dynamics. Note that we can only proxy for the

11. Low confidence does not mean that there 0% certainty and high confidence does not imply 100% certainty. We explicitly compare low- and high-certainty attacks to more precisely assess the impact of certainty given our sample size, but real-world attribution may include more variety than we are able to test here.

passage of time by asking respondents to imagine attacks on different time scales. This biases against our hypothesis predicting higher support for retaliation to more recent attacks, as we cannot necessarily pick up respondents' actual emotive reactions to time. Instead, we are effectively measuring the importance that respondents cognitively assign to timing.

In all, the experiment uses a 2 x 4 x 2 x 2 factorial design, with 32 total treatment groups. Each respondent received a single randomized treatment. Table 2 depicts the treatments.

Table 2: Treatments by Factor

Type	**Scale**[12]	**Attribution Certainty**	**Timing**
Cyber attack	Information Theft	High Confidence	Recently
Physical attack	Financial Theft	Low Confidence	More than a year ago
	Infrastructure Destruction		
	Loss of Life		

The attack is conducted by a non-state actor with a state sponsor (Russia).[13] Russia is a highly active state actor in the cyber domain and may naturally arise in the mind of respondents. State-sponsorship mirrors the empirical reality of advanced persistent threats (APTs). APTs are likely to cause high-level, widespread consequences, because they conduct operations that are resource- and intelligence-intensive. This element of the vignette is therefore plausible and politically relevant. There is a possibility priors on terrorism would associate terrorism with individuals of Middle Eastern descent. Designating Russia as the sponsor may help reduce the effect of identity biases. Finally, Russia is a near-peer competitor, so our treatment may present a hard case. Respondents may be reluctant to retaliate against Russia. In order to guard against the influence of pre-existing respondent attitudes toward Russia, we include a control for respondents' perceptions of Russia as a threat within the model.

The dependent variable is public support for retaliation, captured by affirmative an-

12. See Table 1 for full text of scale treatment.
13. This differs from Kreps & Schneider (2019), which does not identify the attacker.

swers to the question: **"Should the U.S. military retaliate against the attack?"** We construct a binary indicator of support for retaliation. In addition, we capture several alternative dependent variables. First, respondents were asked to rate their confidence in their support for or opposition to retaliation; we use this to construct an ordinal scale from very confident opposition to very confident support for retaliation. Next, each respondent was asked to select their most preferred response from a list of seven possible responses: physical attack against Russia, cyber attack against Russia, physical attack against Red Square's headquarters, cyber attack against Red Square's headquarters, economic sanctions against Russia, publicly denounce the attack, or do not acknowledge the attack. Finally, respondents were asked to indicate approval for each of the seven possible responses on a five-point scale from strongly disapprove to strongly approve.

Beyond the experimentally manipulated treatments, it is possible respondents' attitudes about cyber attacks are distinguished by the relative novelty of and perceived individual vulnerability to cyber attacks (Gregory et al. 1995; McDermott 2019). In pre-treatment questions, respondents were asked about their self-reported knowledge of cyberterrorism and terrorism. Respondents were also asked four questions designed to capture perceived vulnerability to cyber attacks. These are included in the regression models as the controls *Cyber Knowledge* and *Cyber Vulnerability*.[14] We also assess the relationship between respondents' support for retaliation and various attitudes about deterrence and escalation in the cyber and kinetic realms.

Respondents are presented with a battery of controls including questions on demographics—such as age, gender, veteran status, political affiliation, and parenthood—as well as attitudes

14. *Cyber Vulnerability* uses the following questions: "How likely do you think it is that there will be a cyberterrorist attack against the United States next year?" "How likely do you think it is that you or someone you know will be the victim of a cyberterrorist attack next year?" "Have you or someone you know ever been the victim of a cyberterrorist attack?" and "How concerned are you about protecting personally identifiable information such as your address or social security number?" We did not find a unique effect of cyber knowledge or vulnerability on willingness to respond to cyber attacks, suggesting neither explains differences in public attitudes about cyber versus kinetic attacks. See Appendix H.

about vengeance, nationalism, globalism, international law, trust in government, international security issues, and perceptions of cyberterrorists, terrorists, and Russia.[15]

4 Main Results

We find that the traditional distinction between "effects-based" and "means-based" models is insufficient to adequately describe respondents' perceptions of attacks. Rather, we argue there are certain characteristics more prevalent in cyber operations that make respondents perceive this method of attack as distinct from kinetic alternatives. In particular, we find the certainty of attribution has a previously underestimated, but central, role in determining public support for retaliation. This suggests support for retaliation is not so much means-based as it is shaped by specific features such as attribution and timing.

Overall, we find strong support for retaliation (66 percent). This is largely consistent across the type of attack, with 64 percent supporting a military response to a cyber attack and 68 percent supporting a military response to a physical attack. Although this difference is statistically significant, it is substantively small. Table 3 shows the results of a linear probability model on support for responding to an attack "with military force." There is a notable absence of interaction effects between the cyber attack treatment and the other experimentally manipulated treatments. The absence of interactions suggests cyber attacks are not uniquely vulnerable to changes in the certainty, timing, or scale of an attack's damage (although certain values of these parameters may be more common for cyber attacks.) This undermines the means-based theory. Strikingly, the scale of damage that the attack

15. Respondent's attitudes about the United States and its role in the international environment may predispose retaliation support. To control for these attitudes, we use three variables: *Nationalism*, *Int'l Law*, and *Globalism*. *Nationalism* is a binary indicator recording if the respondent selected that being an American was somewhat or very important to their identity. *Int'l Law* is a binary indicator for whether respondents somewhat or strongly agree that it is important for states to comply with international law. *Globalism* reflects the average score of three statements designed to assess beliefs about the U.S. role in the international environment. Respondents were also asked: "How much do you trust the U.S. government as a whole to manage crises?" This constitutes the *Trust in Gov't* variable.

causes is not significantly related to support for retaliation in any of the models in Table 3. Respondents support retaliation against attacks that produce stolen information at the same rate as attacks that resulted in large numbers of deaths. This surprising result contradicts the effects-based approach.

Across all models, we find that attribution certainty and timing are the greatest and most significant predictors of respondents' support for retaliation. Almost three-quarters of respondents who were told that the government had "high confidence" in the attribution of the attack supported retaliation, while just under 60 percent of those told the government had "low confidence" supported the same response. Change from "low confidence" to "high confidence" is associated with an increase in support for retaliation between 11 and 16 percentage points, an effect larger than for almost any other variable examined. This effect is significant at $p < 0.001$ across specifications. Attribution challenges are not unique to cyber attacks. However, cyber attacks empirically face much greater difficulties in attribution than kinetic attacks. This explains why cyber attacks may often be thought of as less likely to escalate—these attacks may be difficult to attribute, depressing support for retaliation. Yet 'grey zone' warfare and other types of covert kinetic attacks may experience similar public resistance to retaliation.

There are two plausible reasons for the differences between our and previous studies' findings. First, the language associated with attribution varies. While we opted to use "high confidence" and "low confidence" in keeping with the United States' Director of National Intelligence *Cyber Attribution Guide*, Kreps and Das (2017) use "probably" and "almost certainly," while Tomz and Weeks (2020) use percentage certainty (50%, 75%, 95%, 100%). Respondents may have different associations with each phrasing. Additionally, these studies include partisanship in their experiments. Elite signaling and party politics may have subsumed the effects of attribution, or respondents may have interpreted attribution certainty as a partisan measure. However, political polarization does not necessarily reflect real politics

in this instance. Defense is one of few bipartisan issues. Analyses of attribution that center partisanship might underestimate attribution's effect by overestimating the importance of cross-partisan cues.

To illustrate, some respondents explicitly referenced attribution as an important component of their support for retaliation. Respondents wrote retaliation should happen because "the Americans know who is responsible," and, "since the government knows for sure it was the Russians, shouldn't we show Russia that we won't let them get away with the attack?" Several respondents specified retaliation should be conditional, occurring only "if they know who did it," "if they can prove who did it," or "once they find out exactly who did it." Respondents suggested attributed attacks should be met with a strong response. For example, one wrote: "If the government has high confidence and has the named group's information, I would believe they have enough to make a strong move." Another wrote: "If it is known who did it, surely the military should get involved." Attribution was also linked to accountability, with respondents writing: "If they have actual proof that Russia sponsored a terrorist attack towards the U.S., they should be held accountable" and "I believe if there's a strong evidence that they did it...then it's logical that [the United States would] retaliate back and let them know no one can mess with the country."

The second largest treatment effect is from timing. Among respondents who were told the attack occurred "more than a year ago," 64 percent supported retaliation, while among those who were told that the attack occurred "recently," 68 percent supported retaliation. Attacks that occurred in the year prior experienced a 4 to 6 percentage point decline in support for retaliation, compared to those that were described as having occurred "recently." Indeed, some respondents recognize the importance of timing, writing that "a quick response is necessary," "response time is important before another attack," and "the earlier you try to solve a problem, the earlier it's no longer a problem." Previous researchers have suggested delays in attribution make it harder to respond to cyber attacks (Brantly 2018a; Kello 2013).

These delays can be the result of attribution challenges or intentional decisions by actors making attribution claims. We find support for this phenomenon.

We find that an attack's means has a smaller effect than attribution certainty and is subject to variation in size and significance with the inclusion of controls. For example, in Model 4, the effect of an attack occurring with cyber, rather than physical, means decreased respondents' support for retaliation by four percentage points. This effect is nearly four times smaller than the estimated effect of certain attribution. Yet the attack's means has no significant effect in the majority of models in Table 3.[16] When accounting for other features of attacks—e.g. effect size, attribution certainty, and timing—the residual, uniquely "cyber" nature of cyber attacks has only a marginal dampening effect on respondents' support for retaliation that is sensitive to the inclusion of controls. This suggests attribution certainty and timing explain a significant portion of *why* cyber and kinetic operations are usually perceived in distinct ways. While these findings provides some evidence for the means-based approach, they also suggest previous work may have overestimated the importance of means.

Regression analysis also provides insight into a number of control variables associated with support for retaliation. Because the treatments are randomized and the sample balanced, we should expect treatment effects to hold regardless of the inclusion of controls. However, including control variables provides a more comprehensive understanding of public attitudes by showing how particular groups of respondents react to attacks. In Model 3, we include respondents' demographics, such as age and gender. In Models 4 and 5, we add additional control variables, such as measures of respondents' normative attitudes about governance and international politics, perceptions about and knowledge of cyberterrorism, and views on deterrence. Of note, the novelty of cyber operations and respondents' perceived susceptibility appear to have no effect on retaliation. The results also hold while controlling

16. This is similarly true when using the scaled dependent variable. See Appendix E.

Table 3: Linear Regression Support for Retaliation (Binary DV)

	Binary Support for Retaliation				
	Base	Interactions	Demographic Controls	Full Model	Post Treatment
	(1)	(2)	(3)	(4)	(5)
Cyber	−0.028 (0.018)	−0.085 (0.050)	−0.036* (0.018)	−0.043* (0.018)	−0.026 (0.016)
Distant	−0.043* (0.018)	−0.056* (0.025)	−0.052** (0.018)	−0.041* (0.018)	−0.038* (0.016)
Certain	0.153*** (0.018)	0.161*** (0.025)	0.152*** (0.018)	0.150*** (0.018)	0.106*** (0.016)
Scale	0.011 (0.008)	0.001 (0.011)	0.015 (0.008)	0.015 (0.008)	0.009 (0.007)
Cyber:Distant		0.026 (0.035)			
Cyber:Certain		−0.016 (0.035)			
Cyber:Scale		0.021 (0.016)			
Age			0.004*** (0.001)	0.004*** (0.001)	0.002** (0.001)
Education			−0.003 (0.007)	−0.007 (0.007)	−0.002 (0.006)
Female			−0.104*** (0.019)	−0.043* (0.020)	−0.030 (0.018)
White			0.029 (0.033)	0.009 (0.032)	−0.014 (0.029)
Black			−0.013 (0.039)	−0.030 (0.038)	−0.053 (0.034)
Hispanic			−0.025 (0.030)	−0.020 (0.029)	−0.014 (0.026)
Parent			0.147*** (0.021)	0.085*** (0.021)	0.058** (0.019)
Veteran			0.006 (0.020)	−0.005 (0.019)	−0.011 (0.017)
Household Income			−0.001 (0.003)	−0.006 (0.003)	−0.006* (0.003)
Citizen			0.182* (0.071)	0.124 (0.069)	0.123* (0.061)
Republican			0.072*** (0.021)	0.022 (0.021)	0.0003 (0.019)
Russia Threat				0.030** (0.011)	0.018 (0.010)
Vengeance				0.031*** (0.003)	0.014*** (0.003)
Nationalism				0.053 (0.029)	0.009 (0.026)
Globalism				−0.014 (0.012)	−0.010 (0.010)
Int'l Law				−0.011 (0.014)	−0.026* (0.013)
Trust in Gov't				0.026** (0.009)	0.005 (0.008)
Cyber Knowledge				0.011 (0.012)	−0.003 (0.010)
Cyber Vulnerability				0.004 (0.010)	−0.002 (0.009)
Effective Deterrent					0.077*** (0.010)
Escalation					0.430*** (0.019)
Constant	0.591*** (0.026)	0.619*** (0.035)	−7.649*** (1.153)	−7.399*** (1.263)	−3.300** (1.139)
Observations	2,797	2,797	2,486	2,476	2,476
R^2	0.030	0.031	0.089	0.151	0.331
Adjusted R^2	0.028	0.028	0.084	0.143	0.324
Residual Std. Error	0.467 (df = 2792)	0.467 (df = 2789)	0.451 (df = 2470)	0.436 (df = 2452)	0.388 (df = 2450)
F Statistic	21.422*** (df = 4; 2792)	12.603*** (df = 7; 2789)	16.113*** (df = 15; 2470)	19.000*** (df = 23; 2452)	48.404*** (df = 25; 2450)

Note: *p<0.05; **p<0.01; ***p<0.001

for respondents' perceptions of Russia as a threat.[17] We find that attitudes about vengeance are strongly and consistently correlated with support for retaliation, and attitudes on international law and on trust in government are inconsistently related to retaliation. These results are unsurprising. Vengeful individuals seek response to infringements, and trust in international law and government may make respondents more confident in their government's ability to effectively retaliate as well as more sensitive to incursions. Several demographic variables also were significant. For example, older respondents were more likely to support retaliation, as were parents.

Model 5 includes two post-treatment policy controls: *Effective Deterrent* and *Escalation*. Existing literature on public support for retaliation often attributes public attitudes to deterrence and escalation dynamics. Attitudes about deterrence and escalation have been theorized to differ between cyber and kinetic operations (Brantly 2018a; Lin 2012; Lindsay 2015; Libicki 2012). However, we find that respondents have the same views on deterrence and escalation in the cyber and physical domains. We test these dynamics using two variables. *Effective Deterrent* derives from a post-treatment question that asked respondents how effective they believed their most preferred response to the attack would be in preventing future attacks. *Escalation* derives from a post-treatment question that tells respondents, regardless of their choice to retaliate or not, to "imagine that the U.S. decided to retaliate against the attack by targeting Red Square. In response to the U.S. military retaliation, Red Square carries out an attack against the U.S. This new attack is similar to the first attack. Knowing this, do you think that the U.S. military should have retaliated against the original attack?"[18] As indicated by Model 4, belief in the efficacy of response is an important predictor of support for retaliation. Respondents who believed their most preferred response

17. See Appendix H.

18. *Effective Deterrent* was assessed on a five-point scale from very ineffective to very effective. *Escalation* was a binary indicator. These variables were included as a post-treatment controls because they had a significant, independent effect on the dependent variable but were not affected by the attack type treatment. See Appendix B.

would be 'somewhat' or 'very' effective at deterring future attacks were 31 percentage points more likely to support retaliation. Respondents who agreed the United States should have retaliated, knowing that it led to subsequent escalation, were 54 percentage points more likely to support retaliation initially than those who believe the United States should not have retaliated.[19]

Table 4 outlines the four treatments, identifying how they relate to theories about cyber and kinetic conflict. While we find evidence that the type, attribution certainty, and timing of an attack influence support for retaliation, we find no evidence for the effects-based theory. The scale of an attack's damage does not affect respondents' support for retaliation. Respondents largely favor retaliation, even to very low-level exploits. After controlling for features theorized to vary between cyber and kinetic attacks, we find limited evidence for the means-based approach. Instead, our results indicate key features that can relate to the means of attack—namely, attribution certainty and timing—play a significant role.

Table 4: Summary of Hypotheses and Findings, H1-H3

Characteristic	**Hypotheses**	**Evidence?**
Means	**H1 (Type):** The public will be more likely to support retaliation against kinetic attacks than cyber attacks with effects of same magnitude.	Mixed
Effects	**H2 (Scale):**As the effects of the attack increase in scale, public support for retaliation will increase, regardless of the means of delivery.	No
Covertness	**H3a: (Attribution Certainty):** As the attribution certainty of an attack increases, support for retaliation will increase, regardless of means of delivery.	Yes
	H3b (Timing): As the time since an attack becomes more distant, support for retaliation will decrease, regardless of means of delivery.	Yes

4.1 Assessing Within- and Cross-Domain Response Preferences

In addition to asking about willingness to retaliate, we also examined each respondent's most preferred policy. Again, we find majority support for military options such as kinetic and

19. 39% of respondents opposing retaliation initially later supported retaliation after learning it resulted in escalation. This suggests escalation does not deter but or justifies retaliation. For a more detailed exploration of deterrence and escalation, see Appendices B and H.

cyber retaliation. Figure 1 shows a breakdown of respondents' most preferred response by whether they received a cyber or physical vignette. Figure 1 indicates some support for cross-domain retaliation and some support for a "notion of equivalence." 31 percent of respondents who received a cyber attack treatment preferred to respond with a cyber attack; similarly, 34 percent of respondents who received a kinetic attack preferred to respond kinetically. Of respondents who received the cyber treatment, 24 percent preferred to respond kinetically, while 45 percent opted for a diplomatic solution, such as economic sanctions. This breakdown is similar for respondents who received the kinetic treatment: 26 percent preferred retaliation in the form of a cyber operation, while 41 percent preferred a diplomatic option.[20]

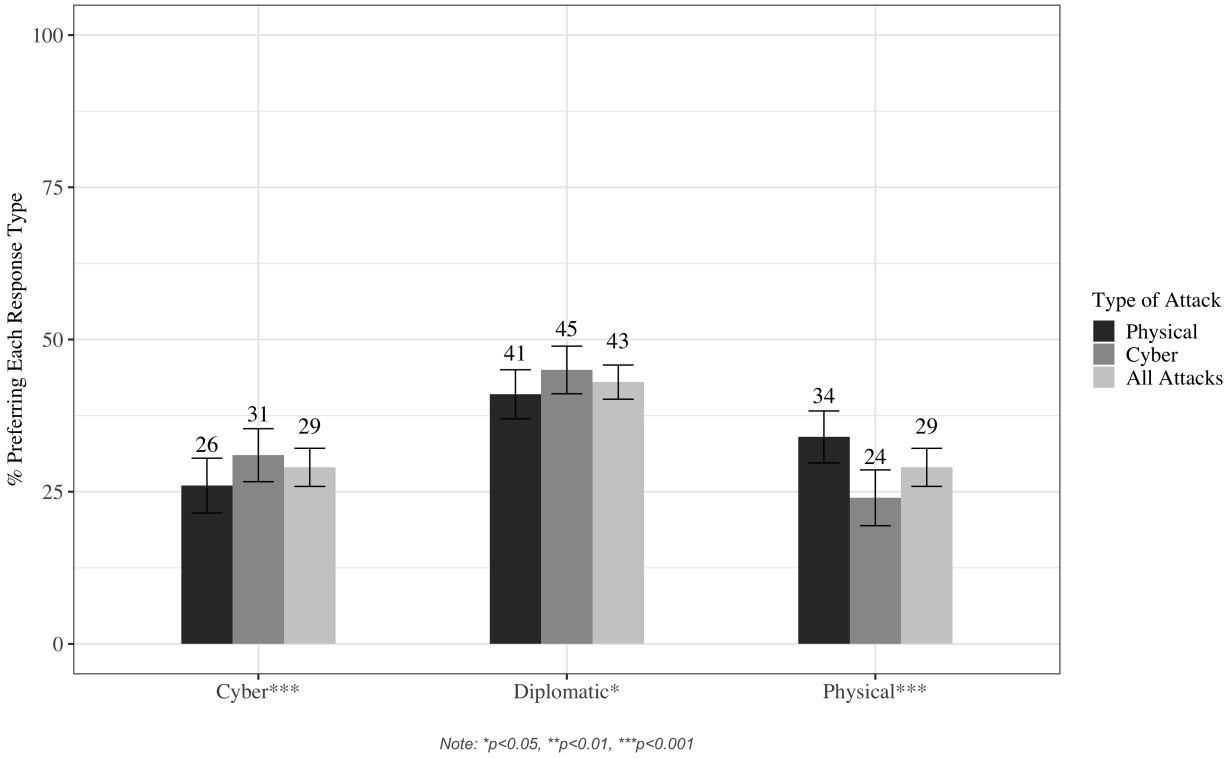


Figure 1: Most Preferred Type of Response

When we group respondents by their most preferred response, we find that those who

20. There is no significant difference between support for cross-domain retaliation to cyber and kinetic attacks. When only including respondents who were given a high damage treatment—infrastructure damage or loss of life—the results are similar. See Appendix F.

receive a cyber treatment are less likely to support physical retaliation, although generally no less likely to support retaliation overall.[21] Individuals who received a cyber treatment were 10 percentage points less likely to select a physical attack as their most preferred response, 5 percentage points more likely to select a cyber-based response, and 4 percentage points more likely to prefer a diplomatic response relative to individuals who received the kinetic treatment. This suggests that, while the type of attack may not affect respondents' overall willingness to respond, it may have an important role in the preferred response type. While empirical studies of means-based theory have largely focused on how the means of an attack influences attitudes about responding, our results suggest the means of an attack may have less influence on *whether* to respond and more influence on *how*.[22] While these effects are small, attitudes about how attacks might occur can influence politics. The public can hold opinions on the types of weapons or strategies that are acceptable to apply. As the highly-publicized debate over the use of drones exemplifies, these views can impose significant political costs.[23]

A large subset of respondents support highly disproportionate militarized action in response to the treatments. While the most severe treatment causes a loss of life, this is still limited to a single attack on a single city, and the least severe treatment reflects the kind of information-gathering hacks occurring regularly against U.S. targets. Nonetheless, when we ask respondents what kinds of physical attacks they would support against Russia—even if those attacks were not respondents' first-choice preferences—we find high levels of support for aggressive options. 35 percent of respondents support the use of drones; 33 percent support sending in Special Operations forces; 21 percent support a "boots on the ground" approach; and 17 percent support a bombing campaign.[24] These results show notable public support

21. See Appendix F.

22. The scale of an attack had no effect on respondents' most preferred response, except in the loss of the life treatment. Respondents who were told an attack was lethal were marginally more likely to support physical retaliation. See Appendix F.

23. Kreps and Wallace 2016; Krieg 2016; Shah 2018.

24. Relative to cyber attacks, kinetic attacks are associated with higher support for all of these attack types

for disproportionate responses to both cyber and kinetic attacks that imposed relatively minimal damage. These results are comparable across the cyber and kinetic treatments.

4.2 Explaining High Baseline Support for Retaliation

We find high baseline levels of public support for military retaliation—including in the form of large-scale conventional attacks—in response to even low-level instances of aggression, where non-state actors steal money or data from U.S. citizens. What might explain this phenomenon? To answer this question, we examine a battery of controls that could contribute to high public support for retaliation. We find several respondent characteristics and beliefs that may drive support for retaliation. For example, in Table 3, respondents' age and parental status are consistently correlated with support for retaliation.[25] This reiterates the findings of previous work linking parenthood and support for the use of force (Brooks and Valentino 2011).

Few attitudes about international politics consistently contribute to support for retaliation. Table 3 shows that neither respondents' knowledge about cybersecurity nor their perceived personal vulnerability to cyber operations are correlated with support for retaliation; nor are these variables linked to higher likelihoods of support for retaliation to cyber attacks relative to kinetic attacks.[26] Additionally, neither nationalism nor globalism is associated with support for retaliation, while views on international law and trust in government are inconsistently correlated with support.

In contrast, respondents' expectations about the escalation potential and effectiveness of retaliation play a critical role in retaliation support, although these variables do not distinguish between respondents' reactions to cyber and kinetic attacks.[27] The effectiveness

except the "boots on the ground" approach.

25. Both are positively correlated with support; no other demographics are consistently correlated with support. Gender, income, citizenship, and political party are inconsistently related to retaliation support.

26. See Appendix H.

27. See Appendix B.

variable measures responses to the question: "How effective do you think this response would be at preventing future attacks against the U.S. in the next year?" 80 percent of respondents who supported retaliation, compared to 52 percent of respondents who opposed it, thought attacks would be effective. This suggests support for retaliation sometimes leverages a consequentialist logic; respondents may support retaliation because they believe it will effectively deter.

The escalation variable references a post-treatment question that tells respondents that, regardless of their choice to retaliate or not to: "Imagine that the U.S. decided to retaliate against the attack by targeting Red Square. In response to the U.S. military retaliation, Red Square carries out an attack against the U.S. This new attack is similar to the first attack. Knowing this, do you think that the U.S. military should have retaliated against the original attack?" Even when respondents are explicitly told retaliation will have escalatory consequences, they do not back down. 71 percent of respondents support retaliation in this situation, compared to 66 percent that supported retaliation in the original experiment. It could be that when respondents know retaliation will escalate, they interpret that information as evidence of the malintentions or capabilities of the adversary, making retaliation—even if it is costly—more critical. This finding suggests support for retaliation is "sticky." It may consequently be difficult to dissuade a hawkish public from demanding retaliation in response to attacks. Additionally, support for retaliation may not be diminished, or could actually increase, when the adversary is highly capable.

The final variable consistently related to retaliatory support in Table 3 measures attitudes about vengeance. A majority of respondents were highly vengeful and, therefore, may have be more focused on punishing fictional attackers than on determining an appropriate response. Previous research has suggested the importance of vengefulness as an explanatory factor in public support for military actions. These studies suggest that, beyond a strategic or consequentialist logic, respondents that support retaliatory policies—such as the death

penalty—are much more likely to support the use of force (Stein 2015; Liberman and Skitka 2019; McDermott et al. 2017; Sagan and Valentino 2019a).[28] We confirm previous work associating vengefulness with increased support for retaliation, even in the cyber domain, where the effect of vengeance has not previously been explored.

Figure 2 shows support for retaliation by score on a vengeance scale. Respondents scored a '0' if they strongly disagreed with all four vengeful statements and a '16' if they strongly agreed. The graph indicates a near-linear relationship, supporting existing literature that suggests revenge motives are an important predictor of support for the use of force. Vengeance is the control variable with the single greatest impact on respondents' likelihood to support retaliation. In Model 4 of Table 3, a one-point increase in vengeance is associated with a 3 percentage point increase in the likelihood of supporting retaliation (significant at $p < 0.001$.) In other words, moving from "somewhat" to "strongly" agreeing with just one of the four vengeful statements is associated with a similar magnitude of effect as receiving the delayed attribution treatment. Our finding complement research by Shandler et al. (2021) arguing anger is a primary mechanism of support for cyber retaliation.

Several open-ended comments illustrate the importance of vengeance in some respondents' support for retaliation. For example, respondents wrote the attack "is wrong and deserves to be punished" and explained retaliation would be "fair" and "an eye for an eye." They wrote: "We should take...revenge," "give them a taste of their own medicine," and "teach them a lesson." Respondents wrote the perpetrators "deserve it" and retaliation would be a form of "justice" for "a crime against America," since "crime needs consequences no matter who commits it" and attackers "need to be punished." We also find that vengeful respondents are far less susceptible to the effects of low attribution certainty. Among respon-

28. To measure vengefulness, we ask: "Do you support or oppose the death penalty for convicted murders?;" "Do you support or oppose the U.S. using 'enhanced interrogation' techniques (such as waterboarding) on terrorists?;" "How much do you agree with the following statement: An eye for an eye is never enough;" and "How much do you agree with the following statement: Anyone that kills Americans deserves to be punished." See Appendix G.

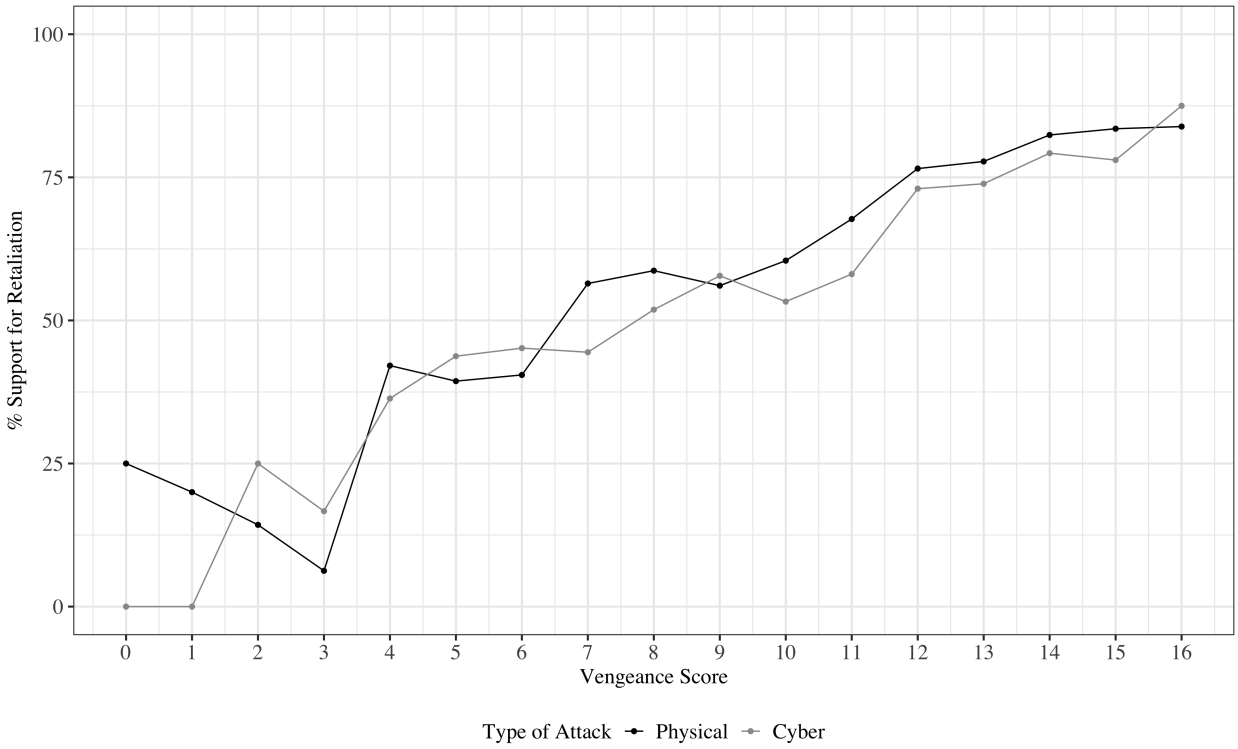


Figure 2: Support for Retaliation by Vengeance Score and Type Treatment

dents who received a low certainty treatment, 79 percent of respondents with a vengeance score above the mean (11 or greater) supported retaliation, while just 53 percent of those with scores below the mean supported retaliation. Among those who received a high certainty treatment, 83 percent with a higher-than-average vengeance score supported retaliation, while 64 percent of below-average respondents supported retaliation.[29]

We find high baseline levels of support for retaliation; this finding is politically significant, as it may indicate the public will not act as a stop-gap against—and may, in fact, encourage—escalation after even low-damage cyber or kinetic attacks. High public approval of retaliation may be influenced by a combination of factors. Consequentialist logic about the usefulness of retaliation may play a role in public support for the use of force, as might a more emotive logic related to attitudes about vengeance. In addition, some demographic features—specifically, respondents' age and parenthood status—may contribute to support for retaliation.

4.3 Challenging the Effects-Based Theory

Contrary to previous literature (Kreps and Schneider 2019; Kreps and Das 2017; Tomz and Weeks 2020; Shandler et al. 2021), we find no evidence of an effects-based mechanism.[30] We find that the scale of the attack's damage has almost no measurable effect on respondents' willingness to retaliate. This finding holds true across a wide range of model specifications, including alternate dependent variables.[31]

There are several potential explanations. First, we control for a broader range of differences between cyber and kinetic attacks than previous studies. The inclusion of factors like attribution certainty and timing may remove implicit associations that shaped results in

29. These differences are significant at $p < 0.001$.

30. Even when Kreps and Schneider (2019) find support for the means-based theory, their results also show a positive relationship between the scale of an attack and respondents' willingness to retaliate. Likewise, Shandler et al. (2021) find no means-based distinction at lower effects thresholds but identify one when attacks cause loss of life.

31. For further analysis of scale variable, including additional operationalizations of scale, see Appendix D

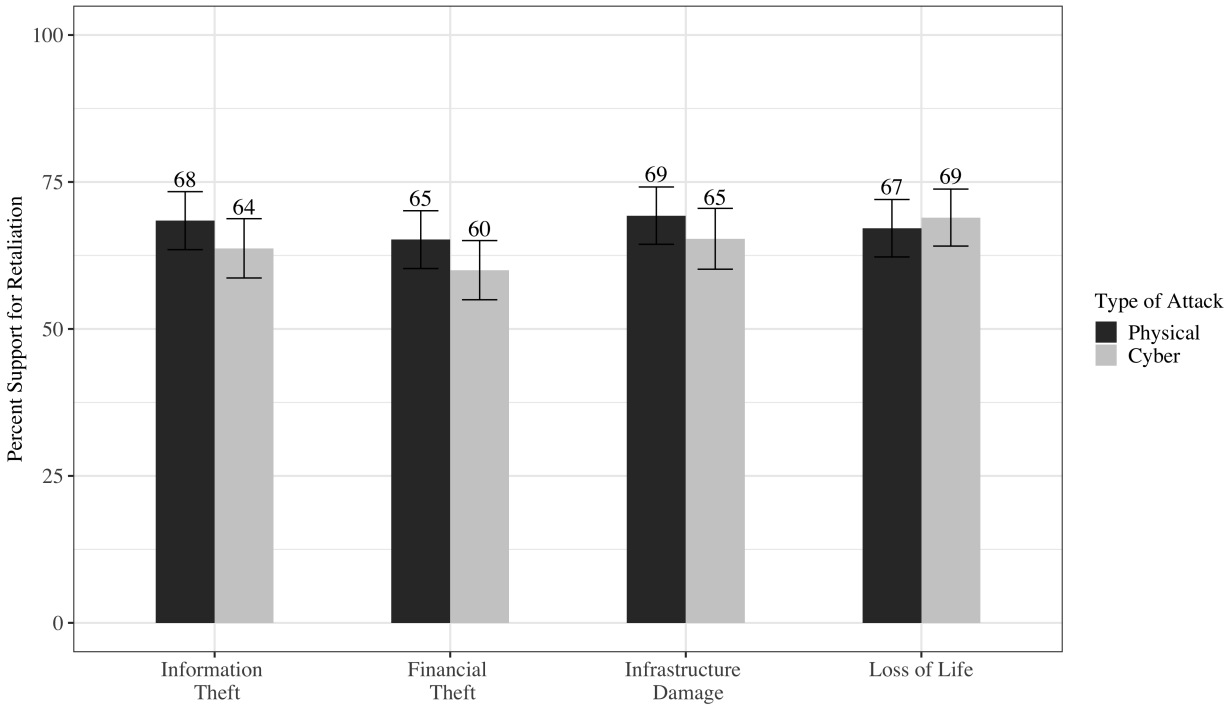
previous studies. Second, we intentionally chose outcomes respondents would find believable and that were largely consistent with cyber attacks familiar to casual news consumers. This departs from existing work, which uses severe outcomes for attacks, such as a nuclear meltdown (Kreps and Das 2017; Kreps and Schneider 2019). As a result, our work presents a hard test of the effects-based theory. Third, it is possible the public has learned more about cybersecurity and has evolved since some previous surveys were fielded.[32]

While we cannot point to precisely why we fail to find evidence for the effects-based theory, we do provide an important and reliable test. We show that at common levels of damage associated with cyber attacks, the effect of the attack is not a significant predictor of support for retaliation. We also find respondents do not dismiss the attacks in our scenario, despite the low amounts of damage they inflict. Instead, even with low damage, there is still significant support for retaliation, including highly disproportionate responses. However, support for retaliation is largely consistent across damage-levels, as shown in Figure 3.[33] Given the emphasis on effects in the current literature and U.S. cyber strategy, this finding should be deeply puzzling.

Our findings suggest support for military retaliation is strong and enduring. This contradicts scholars who have advocated for an effects-based framework, and it suggests cyber attacks do not need to reach a high 'threshold' of damage to generate support for retaliation. We find two-thirds support for military retaliation against a cyber attack with no effect other than information theft—an event that occurs regularly throughout the United

32. The inclusion of Russia and terrorism could have encouraged a stronger retaliatory response than in previous surveys, although this would not explain the lack of an effects-based result. In addition, Shandler et al. (2021) used terrorism and Kreps and Das (2017) included Russia in their designs. Both found support for the effects-based theory.Finally, we attempted to mitigate the effect of perceptions toward Russia by controlling for pre-treatment attitudes of Russia.

33. When the attack targeted financial institutions, respondents were between 4 and 5 percentage points less likely to support retaliation than with the loss of life treatment, the higher-damage treatments combined, the information theft and loss of life treatments combined, and all other treatment groups combined. This could be related to a specific dislike of the financial sector. The level of support for retaliation does not significantly differ across any other set of scale treatments.



Note: No differences are significant at conventional levels.

Figure 3: Percent Support for Retaliation by Scale Treatment

States. When asked how respondents would "most prefer" the United States respond to this theft, 26 percent selected that they preferred a "physical attack". An additional 30 percent supported a cyber attack. Overall, we find a high baseline level of support for retaliation that is independent of the damage caused.

Our results suggest previous work has overestimated the importance of effects-based models. We find little evidence that the immediate effects of attacks influence respondents' attitudes about retaliation. Our findings also raise questions, however, for the utility of the traditional "means-based" approach. While we do find that attacks that use cyber, as compared to kinetic, methods might result in lower levels of public support for retaliation, a large part of the usual 'dampening' effect of cyber attacks is due to specific features that can be common to both cyber and kinetic attacks. Attribution certainty and timing may in part produce the 'dampening' effect generally associated with cyber attacks. That is, because cyber attacks tend to be both difficult to attribute and to have longer discovery and attribution times, it makes sense we would often see lower support for military responses to cyber attacks.[34]

5 Conclusion

We challenge the common effects-based theory of the public response to cyber attacks. While much of the literature and policy conversations on cyber attacks have focused on questions about what attacks must do or cause to warrant retaliation in kind with physical attacks, we find not only high rates of support for retaliation against low-damage attacks, but also that the amount of damage an attack causes has no effect on public support for retaliation. We also challenge the lethality threshold hypothesis, finding no effect of lethality on respondents'

34. We tested other elements theorized to distinguish between cyber and kinetic means, such as expectations about escalation or the consequences of inaction, the novelty of cyber operations, and the public's perceived vulnerability to cyber operations. These do not lead to significant differences in public support for retaliation to cyber versus kinetic attacks. See Appendix H.

overall support for retaliation.

Additionally, our findings raise questions for the focus on simple versions of means-based theories, which argue that how attacks are delivered has important effects on how they are understood. Instead, we find the American public reacts to cyber and physical attacks in similar ways. Some respondents explicitly note they consider cyber attacks to be no different than their kinetic counterparts. One respondent wrote: "We should be able to protect the American people, either if it's a cyber attack or a[n] actual terrorist attacking America." Another explained: "even though a cyber attack isn't aimed at something tangible, it's still an attack against us nonetheless." These respondent comments illustrate a perceived similarity between cyber and kinetic attacks.

Instead, we find that other features of attacks—such as attribution certainty and timing—influence respondents' preferences both for cyber and physical attacks. However, these features more commonly manifest in the cyber domain. In contrast to the frequently used means- and effects-focused frameworks, our results suggest support for retaliation will be determined by specific characteristics of an attack. However, we do find limited evidence that respondents prefer in-kind responses to attacks, such that cyber attacks may be more likely to generate cyber responses and vice versa.

To identify the effects of different attack characteristics on support for retaliation, we varied four treatments in the survey experiment: the attack's means, timing, attribution certainty, and the scale of its damage. Of these treatments, attribution certainty had the greatest effect on respondents' support for retaliation. A shift from "low confidence" that the attack was attributed to a Russian-sponsored non-state organization to "high confidence" was associated with up to a 15 percentage point increase in support for retaliation. While this effect persists irrespective of the attack's means of delivery, attribution problems are empirically more common for cyber operations than their kinetic counterparts. This suggests the attribution problem has implications for the political feasibility of deterrence by

punishment in the cyber domain. It also suggests that covert kinetic attacks, such as those that use proxy actors, may be more difficult to retaliate against.

Additionally, we find the timing of the attack has a significant impact on retaliation. An attack that happened "more than a year ago," relative to an attack that happened "recently," was associated with a 4 percentage point decrease in respondents' support for retaliation. Timing issues are generally more salient in the cyber domain. It has often taken governments more time to be prepared to respond to hostile cyber operations than kinetic operations. This is because cyber operations can take a long time to discover, and difficulties with attribution in the cyber realm may contribute lead time before retaliation is possible. Governments may also choose if and when to attribute attacks. One reason, then, that cyber operations may prompt retaliation less often is because retaliation often cannot be immediate. These dynamics, however, can also complicate strategy in response to kinetic attacks that have long discovery or attribution periods.

This research has implications for policymakers crafting responses to hostile operations. First, our findings suggest the public is responsive to characteristics of attacks that are not often the focus of policy discussions, such as attribution certainty and attack timing. Given the nature of the attribution problem in the cyber domain, it may be harder to rally support in response to a cyber attack until attribution confidence is high. Unfortunately, waiting to obtain high confidence in attribution may create a temporal delay that has a countervailing dampening effect on support for retaliation. Policymakers may also approach attacks similarly to the public, highly valuing information about attribution certainty and responding to the temporal dynamics of attacks and retaliation.

Second, our results suggest the current focus on how much damage or what type of damage a cyber attack causes may be misplaced. This paper finds high levels of support for retaliation against cyber and kinetic attacks, even when they only cause minimal and non-physical damage. Cyber attacks with these effects are already very common. We find

significant levels of support for very disproportionate responses to low-level attacks. Our findings suggest the public is not likely to serve as restraining force on hawkish leadership in the event the United States is targeted by an attack. Indeed, policymakers may be able to rally significant support for large-scale retaliation against even minor attacks, or they may experience public pressure to retaliate. In addition, while we find slight preferences for within-domain retaliation, we also find high levels of support for cross-domain retaliation, retaliation even when subsequent escalation is likely, and severe tactics such as drone strikes or "boots on the ground" attacks against states that sponsor attacks.

Third, our findings suggest public support for retaliation is generally intractable. Not only is the public unlikely to counteract a leader's retaliatory ambitions, but policymakers may actually face enduring political pressure to respond to both cyber and kinetic attacks, especially those that are well-attributed. We not only find that respondents support retaliation at high rates, but also that support for retaliation endures even when respondents are told retaliation will have high costs and consequences. Vengeful attitudes among the public contribute further to high levels of intractable support for retaliation.

Future research could explore the effects of differently sized delays between attacks and responses, assess how attribution certainty can be manipulated by political actors, or examine public attitudes about different actors that may engage in or sponsor hostile cyber operations. While we have focused on cyber operations in this paper, our results have potentially valuable implications for kinetic operations as well. Further studies on how covertness influences perceptions of attacks in the kinetic domain could enhance our understanding of retaliation dynamics. In addition, while much scholarship has largely focused on the American public, further studies examining attitudes about cybersecurity in other contexts could supplement existing theories of cyber operations.

As cyber operations continue to feature as a regular component of international politics, enhanced understanding of how these attacks are perceived will be critical for developing

policies in the cyber domain. This research offers a new perspective, departing from existing frameworks that have privileged the effects and means of attacks. Our results suggest the need for an expanded approach, which would consider more specific characteristics as key determinants of how these attacks might be perceived by both the public and policymakers.

References

A Guide to Cyber Attribution. 2018. Office of the Director of National Intelligence, September 14, 2018.

Brantly, Aaron. 2016. "Aesop's Wolves: the deceptive appearance of espionage and attacks in cyberspace." *Intelligence and National Security* 31, no. 5 (July 28, 2016): 674–685.

———. 2018a. *Conceptualizing Cyber Deterrence by Entanglement.* SSRN Scholarly Paper ID 2624926. Rochester, NY: Social Science Research Network, April 5, 2018.

———. 2018b. "The Cyber Deterrence Problem." In *2018 10th International Conference on Cyber Conflict (CyCon),* 31–54. May.

Brooks, Deborah Jordan, and Benjamin A Valentino. 2011. "A war of one's own: Understanding the gender gap in support for war." *Public Opinion Quarterly* 75 (2): 270–286.

Buchan, Russell. 2012. "Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?" *Journal of Conflict and Security Law* 17 (2): 211–227.

Carson, Austin. 2018. *Secret Wars: Covert Conflict in International Politics.* Princeton University Press, September 25, 2018.

Carson, Austin, and Keren Yarhi-Milo. 2017. "Covert Communication: The Intelligibility and Credibility of Signaling in Secret." *Security Studies* 26, no. 1 (January 2, 2017): 124–156.

Clark, David, and Susan Landau. 2011. "Untangling Attribution Essay." *Harvard National Security Journal* 2 (2): 323–352.

Cormac, Rory, and Richard J. Aldrich. 2018. "Grey is the new black: covert action and implausible deniability." *International Affairs* 94, no. 3 (May 1, 2018): 477–494.

Egloff, Florian, and Andreas Wenger. 2019. "Public Attribution of Cyber Incidents." *CSS Analyses in Security Policy* 244 (May).

Farrell, Henry, and Charles Glaser. 2017. "The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine." *Journal of Cybersecurity* 3, no. 1 (March 1, 2017): 7–17.

Fearon, James. 1994. "Domestic Political Audiences and the Escalation of International Disputes." *American Political Science Review* 88, no. 3 (September): 577–592.

Fidler, David. 2016. "Just & Unjust War, Uses of Force & Coercion: An Ethical Inquiry with Cyber Illustrations." *Daedalus* 145 (September 1, 2016): 37–49.

Fischerkeller, Michael, and Richard Harknett. 2017. "Deterrence is Not a Credible Strategy for Cyberspace." *Orbis* 61, no. 3 (January 1, 2017): 381–393.

Garcia, Michael, and Mieke Eoyang. 2020. "A Road Map for Tackling Cybercrime." *Lawfare* (December).

Gartzke, E., and J.R. Lindsay. 2019. *Cross-Domain Deterrence: Strategy in an Era of Complexity.* Oxford University Press.

Gartzke, Erik. 2013. "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth." *International Security* 38 (2): 41–73.

Gartzke, Erik, and Jon Lindsay. 2015. "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace." *Security Studies* 24, no. 2 (April 3, 2015): 316–348.

Gregory, Robin, James Flynn, and Paul Slovic. 1995. "Technological Stigma." *American Scientist* 83, no. 3 (May 1, 1995): 220–224.

Gross, Michael, Daphna Canetti, and Dana R. Vashdi. 2016. "The Psychological Effects of Cyber Terrorism." *Bulletin of the Atomic Scientists* 72, no. 5 (September): 284–291.

Haesebrouck, Tim. 2019. "Who Follows Whom? A coincidence analysis of military action, public opinion and threats." *Journal of Peace Research* 56, no. 6 (November 1, 2019): 753–766.

Heath, Brad. 2021. "SolarWinds hack was 'largest and most sophisticated attack' ever: Microsoft president." *Reuters* (February 15, 2021).

Johnson, James. 2020. "Delegating strategic decision-making to machines: Dr. Strangelove redux?" *Journal of Strategic Studies,* 1–39.

Kello, Lucas. 2013. "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft." *International Security* 38 (2): 7–40.

Kertzer, Joshua, and Ryan Brutger. 2016. "Decomposing Audience Costs: Bringing the Audience Back into Audience Cost Theory." *American Journal of Political Science* 60 (1): 234–249.

Kertzer, Joshua, Brian Rathbun, and Nina Srinivasan Rathbun. 2020. "The Price of Peace: Motivated Reasoning and Costly Signaling in International Relations." *International Organization* 74 (1): 95–118.

Kostyuk, Nadiya, and Carly Wayne. 2020. "The Microfoundations of State Cybersecurity: Cyber Risk Perceptions and the Mass Public." *Journal of Global Security Studies* (March 12, 2020).

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, no. 2 (April 1, 2017): 2053168017715930.

Kreps, Sarah, and Jacquelyn Schneider. 2019. "Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving beyond effects-based logics." *Journal of Cybersecurity* 5, no. 1 (January 1, 2019).

Kreps, Sarah E, and Geoffrey PR Wallace. 2016. "International law, military effectiveness, and public support for drone strikes." *Journal of Peace Research* 53 (6): 830–844.

Krieg, Andreas. 2016. "Externalizing the burden of war: the Obama Doctrine and US foreign policy in the Middle East." *International Affairs* 92 (1): 97–113.

Levendusky, Matthew, and Michael Horowitz. 2012. "When Backing Down Is the Right Decision: Partisanship, New Information, and Audience Costs." *The Journal of Politics* 74 (2): 323–338.

Liberman, Peter, and Linda Skitka. 2019. "Vicarious Retribution in US Public Support for War Against Iraq." *Security Studies* 28, no. 2 (March 15, 2019): 189–215.

Libicki, Martin. 2012. *Crisis and Escalation in Cyberspace.* Rand Corporation.

Lieber, Keir, and Daryl Press. 2013. "Why States Won't Give Nuclear Weapons to Terrorists." *International Security* 38, no. 1 (July 1, 2013): 80–104.

Lin, Herbert. 2012. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly,* 25.

Lindsay, Jon. 2015. "Tipping the Scales: The attribution problem and the feasibility of deterrence against cyberattack." *Journal of Cybersecurity* 1, no. 1 (September 1, 2015): 53–67.

Maurer, Tim. 2018. *Cyber Mercenaries.* Cambridge University Press, January 18, 2018.

McDermott, Rose. 2019. "Some Emotional Considerations in Cyber Conflict." *Journal of Cyber Policy* 4, no. 3 (September 2, 2019): 309–325.

McDermott, Rose, Anthony Lopez, and Peter Hatemi. 2017. "'Blunt Not the Heart, Enrage It': The Psychology of Revenge and Deterrence." *Texas National Security Review* 1, no. 1 (November 24, 2017).

Miller, Michael. 2007. "Nuclear Attribution as Deterrence." *The Nonproliferation Review* 14, no. 1 (March 1, 2007): 33–60.

Mumford, Andrew. 2013. "Proxy Warfare and the Future of Conflict." *The RUSI Journal* 158 (2): 40–46.

Nye, Joseph. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (January): 44–71.

Poznansky, Michael, and Evan Perkoski. 2018. "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution." *Journal of Global Security Studies* 3, no. 4 (October 1, 2018): 402–416.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (February): 5–32.

Rid, Thomas, and Ben Buchanan. 2015. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1 (January 2, 2015): 4–37.

Sagan, Scott, and Benjamin Valentino. 2019a. "Just War and Unjust Soldiers: American Public Opinion on the Moral Equality of Combatants." *Ethics & International Affairs* 33 (4): 411–444.

———. 2019b. "On Reciprocity, Revenge, and Replication: A Rejoinder to Walzer, McMahan, and Keohane." *Ethics & International Affairs* 33 (4): 473–479.

Sanger, David, and Nicole Perlroth. 2020. "FireEye, a Top Cybersecurity Firm, Says It Was Hacked by a Nation-State." *The New York Times* (December 8, 2020).

Schneider, Jacquelyn. 2017. "Cyber and Crisis Escalation: Insights from Wargaming." *US-ASOC Futures Forum* (March): 43.

Schultz, Kenneth. 1999. "Do Democratic Institutions Constrain or Inform? Contrasting Two Institutional Perspectives on Democracy and War." *International Organization* 53 (2): 233–266.

Shah, Aqil. 2018. "Do US drone strikes cause blowback? Evidence from Pakistan and beyond." *International Security* 42 (4): 47–84.

Shandler, Ryan, Michael Gross, Sophia Backhaus, and Daphna Canetti. 2021. "Cyber Terrorism and Public Support for Retaliation – A Multi-Country Survey Experiment." *British Journal of Political Science,* 1–19.

Stein, Rachel. 2015. "War and Revenge: Explaining Conflict Initiation by Democracies." *American Political Science Review* 109, no. 3 (August): 556–573.

Temple-Raston, Dina. 2021. "Biden Order Will Require New Cybersecurity Standards In Response To SolarWinds Attack." *NPR* (April 19, 2021).

Tomz, Michael. 2007. "Domestic Audience Costs in International Relations: An Experimental Approach." *International Organization* 61, no. 4 (October): 821–840.

Tomz, Michael, and Jessica Weeks. 2020. "Public Opinion and Foreign Electoral Intervention." *American Political Science Review* 114, no. 3 (August): 856–873.

Tomz, Michael, Jessica Weeks, and Keren Yarhi-Milo. 2020. "Public Opinion and Decisions About Military Force in Democracies." *International Organization* 74 (1): 119–143.

Supplemental Appendix

Table of Contents

A Balance Table **A2**

B Post-Treatment Policy Controls **A2**

C Robustness Checks for Main Results **A4**

D Scale Analysis **A6**

E Scaled Measure of Retaliation **A7**

F Most Preferred Response **A8**

G Vengeance **A11**

H Alternative Explanations **A12**

I Terrorism and Cyberterrorism **A14**

J Pre-Analysis Plan **A16**

K Survey Text **17**

A Balance Table

Table A1: Balance Table

Variable	Balance Type	Unadjusted Difference
Age	Contin.	0.00
Education	Contin.	0.01
Female	Binary	-0.01
White	Binary	0.00
Black	Binary	-0.01
Hispanic	Binary	0.00
Parent	Binary	0.00
Veteran	Binary	-0.02
Household Income	Contin.	0.02
Citizen	Binary	-0.01
Republican	Binary	0.00

B Post-Treatment Policy Controls

We are able to include the escalation and effectiveness post-treatment controls in the main regression models because there is no effect of the cyber attack treatment on either variable, but both variables are correlated with a higher level of support for retaliation. See Table A2. This section discusses those variables in more detail.

Table A2: Two-Stage Regression of Escalation and Effective Deterrent

	Treatment on Escalation	Escalation on Retaliation	Treatment on Effective Deterrent	Effective Deterrent on Retaliation
	(1)	(2)	(3)	(4)
Cyber	−0.027 (0.017)		−0.008 (0.037)	
Distant	−0.011 (0.017)		−0.046 (0.037)	
Certain	0.075*** (0.017)		0.198*** (0.037)	
Scale	0.009 (0.008)		−0.005 (0.016)	
Escalation		0.540*** (0.017)		
Effective Response				0.165*** (0.009)
Constant	0.673*** (0.025)	0.274*** (0.014)	2.876*** (0.055)	0.175*** (0.027)
Observations	2,797	2,797	2,797	2,797
R^2	0.008	0.266	0.011	0.115
Adjusted R^2	0.007	0.265	0.010	0.114
Residual Std. Error	0.450	0.406	0.967	0.446
	(df = 2792)	(df = 2795)	(df = 2792)	(df = 2795)

Note: *p<0.05; **p<0.01; ***p<0.001

C Robustness Checks for Main Results

Table A3 reproduces Table 3 without excluding respondents who failed the mechanism check asking them to correctly identify the target of the attack. Respondents who failed the attention check are still excluded. Table A4 includes both individuals who failed the attention check and individuals who failed the manipulation check. In each of robustness check, the main results hold.

Table A3: Support for Retaliation Including Mechanism Check Failures

	Binary Support for Retaliation				
	Base	Interactions	retal Demographic Controls	Full Model	Post Treatment
	(1)	(2)	(3)	(4)	(5)
Cyber	−0.020 (0.016)	−0.091* (0.046)	−0.023 (0.017)	−0.030 (0.016)	−0.017 (0.015)
Distant	−0.045** (0.016)	−0.070** (0.023)	−0.054** (0.017)	−0.045** (0.016)	−0.041** (0.015)
Certain	0.137*** (0.016)	0.144*** (0.023)	0.135*** (0.017)	0.134*** (0.016)	0.098*** (0.015)
Scale	0.007 (0.007)	−0.004 (0.010)	0.008 (0.007)	0.007 (0.007)	0.003 (0.007)
Cyber:Distant		0.050 (0.032)			
Cyber:Certain		−0.013 (0.032)			
Cyber:Scale		0.021 (0.014)			
Age			0.003*** (0.001)	0.003*** (0.001)	0.001* (0.001)
Education			−0.002 (0.006)	−0.006 (0.006)	−0.002 (0.006)
Female			−0.095*** (0.018)	−0.041* (0.018)	−0.028 (0.016)
White			0.028 (0.030)	0.013 (0.030)	0.002 (0.026)
Black			−0.013 (0.035)	−0.019 (0.034)	−0.028 (0.031)
Hispanic			−0.012 (0.027)	−0.010 (0.026)	−0.007 (0.024)
Parent			0.123*** (0.019)	0.063** (0.019)	0.040* (0.017)
Veteran			0.007 (0.018)	−0.010 (0.018)	−0.015 (0.016)
Household Income			0.0003 (0.003)	−0.005 (0.003)	−0.005* (0.003)
Citizen			0.209*** (0.060)	0.157** (0.059)	0.130* (0.052)
Republican			0.068*** (0.019)	0.020 (0.019)	0.0002 (0.017)
Russia Threat				0.024* (0.010)	0.012 (0.009)
Vengeance				0.027*** (0.003)	0.012*** (0.003)
Nationalism				0.072** (0.027)	0.026 (0.024)
Globalism				−0.018 (0.011)	−0.014 (0.010)
Int'l Law				−0.011 (0.012)	−0.027* (0.011)
Trust in Gov't				0.029*** (0.008)	0.009 (0.007)
Cyber Knowledge				0.012 (0.011)	0.001 (0.009)
Cyber Vulnerability				0.006 (0.009)	−0.004 (0.008)
Effective Deterrent					0.071*** (0.009)
Escalation					0.429*** (0.017)
Constant	0.614*** (0.024)	0.649*** (0.032)	−5.881*** (1.071)	−5.938*** (1.174)	−2.105* (1.059)
Observations	3,311	3,311	2,946	2,932	2,932
R^2	0.024	0.026	0.071	0.130	0.310
Adjusted R^2	0.023	0.023	0.066	0.123	0.304
Residual Std. Error	0.466 (df = 3306)	0.466 (df = 3303)	0.454 (df = 2930)	0.440 (df = 2908)	0.392 (df = 2906)
F Statistic	20.453*** (df = 4; 3306)	12.370*** (df = 7; 3303)	14.942*** (df = 15; 2930)	18.885*** (df = 23; 2908)	52.317*** (df = 25; 2906)

Note: *p<0.05; **p<0.01; ***p<0.001

Table A4: Support for Retaliation Including Attention and Manipulation Check Failures

	Binary Support for Retaliation				
	Base	Interactions	retal Demographic Controls	Full Model	Post Treatment
	(1)	(2)	(3)	(4)	(5)
Cyber	−0.020 (0.015)	−0.094* (0.042)	−0.028 (0.016)	−0.033* (0.015)	−0.021 (0.014)
Distant	−0.044** (0.015)	−0.070** (0.021)	−0.044** (0.016)	−0.035* (0.015)	−0.035** (0.014)
Certain	0.125*** (0.015)	0.132*** (0.021)	0.120*** (0.016)	0.120*** (0.015)	0.090*** (0.014)
Scale	0.003 (0.007)	−0.008 (0.009)	0.005 (0.007)	0.005 (0.007)	0.002 (0.006)
Cyber:Distant		0.051 (0.030)			
Cyber:Certain		−0.013 (0.030)			
Cyber:Scale		0.022 (0.013)			
Age			0.003*** (0.001)	0.003*** (0.001)	0.001* (0.0005)
Education			−0.004 (0.006)	−0.007 (0.006)	−0.003 (0.005)
Female			−0.101*** (0.017)	−0.049** (0.017)	−0.038* (0.015)
White			0.046 (0.028)	0.026 (0.027)	0.015 (0.024)
Black			−0.005 (0.032)	−0.012 (0.031)	−0.023 (0.028)
Hispanic			−0.023 (0.025)	−0.018 (0.024)	−0.023 (0.021)
Parent			0.109*** (0.018)	0.056** (0.018)	0.035* (0.016)
Veteran			0.024 (0.017)	0.005 (0.017)	−0.009 (0.015)
Household Income			0.002 (0.003)	−0.003 (0.003)	−0.004 (0.002)
Citizen			0.189*** (0.047)	0.141** (0.047)	0.124** (0.042)
Republican			0.071*** (0.018)	0.025 (0.018)	0.001 (0.016)
Russia Threat				0.021* (0.009)	0.010 (0.008)
Vengeance				0.026*** (0.003)	0.013*** (0.003)
Nationalism				0.085*** (0.024)	0.032 (0.022)
Globalism				−0.020 (0.010)	−0.013 (0.009)
Int'l Law				−0.018 (0.011)	−0.032** (0.010)
Trust in Gov't				0.029*** (0.007)	0.010 (0.007)
Cyber Knowledge				0.003 (0.010)	−0.007 (0.009)
Cyber Vulnerability				0.011 (0.008)	−0.0004 (0.007)
Effective Deterrent					0.067*** (0.008)
Escalation					0.419*** (0.016)
Constant	0.637*** (0.022)	0.673*** (0.030)	−5.374*** (1.005)	−5.595*** (1.095)	−2.331* (0.989)
Observations	3,837	3,837	3,375	3,361	3,361
R^2	0.021	0.022	0.070	0.127	0.303
Adjusted R^2	0.020	0.020	0.066	0.121	0.298
Residual Std. Error	0.464 (df = 3832)	0.464 (df = 3829)	0.451 (df = 3359)	0.438 (df = 3337)	0.392 (df = 3335)
F Statistic	20.134*** (df = 4; 3832)	12.339*** (df = 7; 3829)	16.978*** (df = 15; 3359)	21.135*** (df = 23; 3337)	57.928*** (df = 25; 3335)

Note: *p<0.05; **p<0.01; ***p<0.001

D Scale Analysis

In light of our findings which suggest a rejection of effects-based theory, a deeper analysis of the scale variable is warranted. Table A5 includes four additional operationalizations of the scale variable. In Model 2, scale is treated as a factor with the base level of information theft. There is no statistically significant difference in support for retaliation among any scale treatments. In Model 3, scale is once again treated as a factor, but the factor is re-leveled to provide a clear comparison to loss of life. Individuals who received a financial theft scale treatment are the only individuals with a statistically significant difference in support for retaliation relative to loss of life. Due to the finding that respondents see financial theft as unique to other scale treatments, Model 4 re-orders information theft and financial theft scale with financial theft as the lowest scale. This reinforces the unique nature of financial theft relative to other scales. Finally, Model 5 provides a binary indicator of high scale treatment (loss of life and infrastructure damage) compared to a low scale treatment (financial theft and information theft). The statistical significance in this specification is likely driven by the unique perception of financial theft.

Table A5: Linear Regression Support for Retaliation (Binary DV)

	Binary Support for Retaliation				
	Base	Scale as Factor	Re-level to Loss of Life	Reorder Scale Finance Level 1	High Scale Binary
	(1)	(2)	(3)	(4)	(5)
Cyber	−0.028 (0.018)	−0.028 (0.018)	−0.028 (0.018)	−0.028 (0.018)	−0.028 (0.018)
Distant	−0.043* (0.018)	−0.044* (0.018)	−0.044* (0.018)	−0.044* (0.018)	−0.044* (0.018)
Certain	0.153*** (0.018)	0.153*** (0.018)	0.153*** (0.018)	0.153*** (0.018)	0.153*** (0.018)
Scale	0.011 (0.008)				
Scale 2		−0.033 (0.025)			
Scale 3		0.018 (0.025)			
Scale 4		0.020 (0.025)			
Scale 1			−0.020 (0.025)		
Scale 2			−0.053* (0.025)		
Scale 3			−0.002 (0.025)		
Re-scale Information				0.033 (0.025)	
Re-scale Infrastructure				0.051* (0.025)	
Re-scale Loss of Life				0.053* (0.025)	
High Scale					0.036* (0.018)
Constant	0.591*** (0.026)	0.618*** (0.023)	0.638*** (0.024)	0.585*** (0.023)	0.601*** (0.020)
Observations	2,797	2,797	2,797	2,797	2,797
R^2	0.030	0.031	0.031	0.031	0.031
Adjusted R^2	0.028	0.029	0.029	0.029	0.029
Residual Std. Error	0.467 (df = 2792)	0.467 (df = 2790)	0.467 (df = 2790)	0.467 (df = 2790)	0.467 (df = 2792)
F Statistic	21.422*** (df = 4; 2792)	14.943*** (df = 6; 2790)	14.943*** (df = 6; 2790)	14.943*** (df = 6; 2790)	21.974*** (df = 4; 2792)

Note: *p<0.05; **p<0.01; ***p<0.001

E Scaled Measure of Retaliation

This appendix uses an alternate measure of support for retaliation. It combines a binary measure indicating whether respondents support military retaliation with a question measuring the strength of that preference on a five-point Likert scale. The resulting variable is a ten-point measure from very strong support for retaliation to very strong opposition. Our main results hold.

Table A6: Support for Retaliation (Scaled)

	Scaled Support for Retaliation				
	Base	Interactions	Demographic Controls	Full Model	Post Treatment
	(1)	(2)	(3)	(4)	(5)
Cyber	−0.243 (0.128)	−0.588 (0.358)	−0.296* (0.130)	−0.346** (0.125)	−0.227* (0.111)
Distant	−0.326* (0.128)	−0.452* (0.180)	−0.386** (0.130)	−0.307* (0.125)	−0.284* (0.111)
Certain	1.102*** (0.128)	1.191*** (0.180)	1.124*** (0.130)	1.105*** (0.125)	0.776*** (0.113)
Scale	0.103 (0.057)	0.042 (0.081)	0.131* (0.058)	0.135* (0.056)	0.097 (0.050)
Cyber:Distant		0.256 (0.255)			
Cyber:Certain		−0.177 (0.255)			
Cyber:Scale		0.122 (0.114)			
Age			0.033*** (0.004)	0.030*** (0.005)	0.014*** (0.004)
Education			−0.014 (0.048)	−0.049 (0.048)	−0.018 (0.042)
Female			−0.821*** (0.138)	−0.317* (0.142)	−0.223 (0.126)
White			0.152 (0.238)	−0.016 (0.230)	−0.188 (0.205)
Black			−0.210 (0.279)	−0.342 (0.269)	−0.523* (0.239)
Hispanic			−0.203 (0.215)	−0.156 (0.207)	−0.130 (0.184)
Parent			1.163*** (0.149)	0.663*** (0.148)	0.464*** (0.132)
Veteran			−0.026 (0.142)	−0.103 (0.137)	−0.137 (0.122)
Household Income			0.001 (0.023)	−0.040 (0.023)	−0.043* (0.020)
Citizen			1.278* (0.509)	0.839 (0.492)	0.827 (0.437)
Republican			0.583*** (0.148)	0.212 (0.148)	0.053 (0.132)
Russia Threat				0.215** (0.076)	0.129 (0.068)
Vengeance				0.240*** (0.023)	0.119*** (0.021)
Nationalism				0.270 (0.208)	−0.043 (0.185)
Globalism				−0.072 (0.083)	−0.054 (0.074)
Int'l Law				0.029 (0.101)	−0.093 (0.090)
Trust in Gov't				0.250*** (0.063)	0.095 (0.056)
Cyber Knowledge				0.079 (0.082)	−0.024 (0.073)
Cyber Vulnerability				0.007 (0.068)	−0.037 (0.061)
Effective Deterrent					0.628*** (0.069)
Escalation					2.975*** (0.133)
Constant	6.431*** (0.191)	6.602*** (0.254)	−60.731*** (8.270)	−57.456*** (8.980)	−27.356*** (8.098)
Observations	2,795	2,795	2,484	2,474	2,474
R^2	0.031	0.032	0.105	0.180	0.353
Adjusted R^2	0.029	0.029	0.099	0.172	0.346
Residual Std. Error	3.373 (df = 2790)	3.373 (df = 2787)	3.236 (df = 2468)	3.102 (df = 2450)	2.756 (df = 2448)
F Statistic	22.028*** (df = 4; 2790)	12.968*** (df = 7; 2787)	19.287*** (df = 15; 2468)	23.309*** (df = 23; 2450)	53.377*** (df = 25; 2448)

Note: *p<0.05; **p<0.01; ***p<0.001

F Most Preferred Response

Figure A1 shows the coefficients for each treatment on the three types of preferred responses: kinetic responses, cyber responses, and diplomatic responses. The coefficients on the left reflect the "Full Model" specification, which includes demographic and policy control variables. The coefficients on the right reflect the same specification, but they omit from analysis any respondents who were assigned to the "loss of life" treatment for the scale of the attack. Attribution certainty increases support physical responses and decreases support for diplomatic responses in both sets of models. Cyber attacks are associated with increased support for cyber responses and decreased support for kinetic responses. The same is true for attacks that occurred more than one year prior. In the models that do not omit the loss of life treatment, increases in the scale of the damage caused by an attack result in a small but significant increase in support for a physical response to the attack. This could provide suggestive evidence for the lethality thesis advanced by Shandler et al. (2021), which argues that the scale of an attack influences retaliation when attacks are lethal. However, we do not find that lethal attacks increase the overall level of support for retaliation, even if they affect the preferred form of retaliation.

Figure A2 recreates Figure 1 using only respondents who were given the two highest-value treatments for the scale of an attack's damage, i.e. the treatments involving damage to infrastructure that do and do not result in large losses of life. There remains support for both cross-domain and within-domain retaliation.

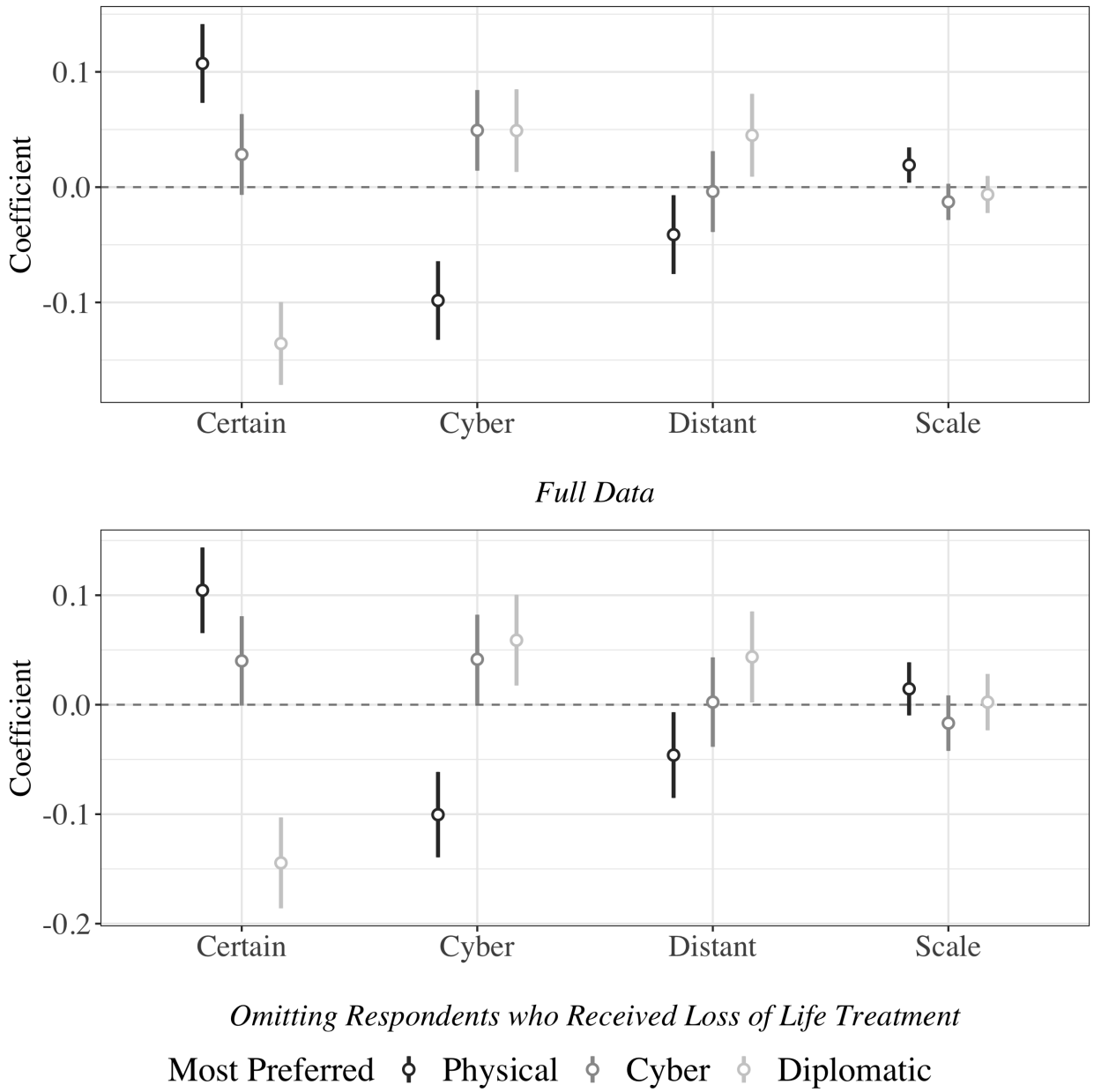


Figure A1: Coefficient Plot of Most Preferred Response by Type With and Without Respondents in "Loss of Life" Treatment Group

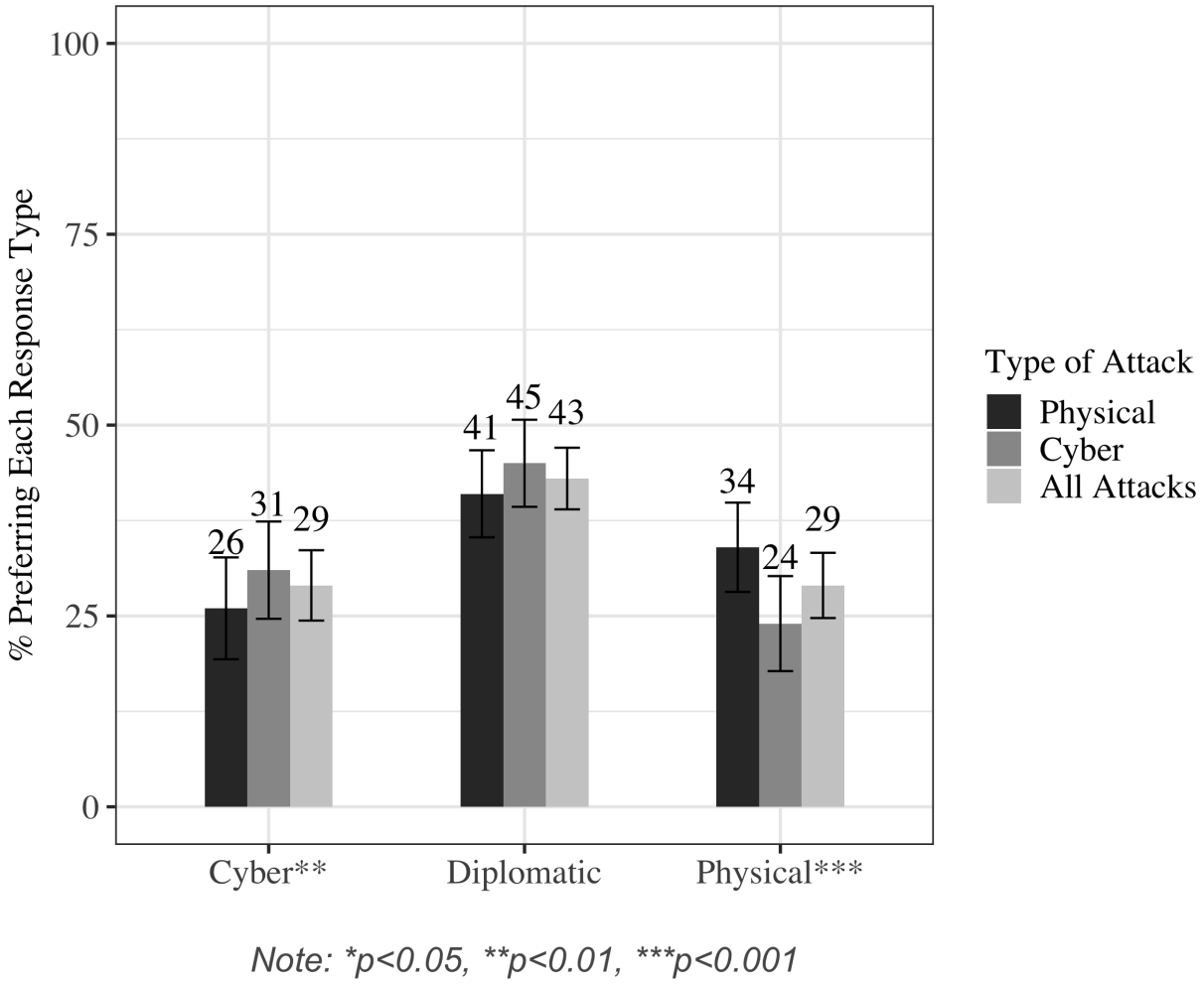


Figure A2: Most Preferred Response Type Using Highest Scale Treatments Only

G Vengeance

This figure supplements Figure 2. It shows the number of respondents per vengeance score by whether respondents were assigned to a cyber or kinetic attack treatment. To measure vengefulness, we ask: "Do you support or oppose the death penalty for convicted murders?;" "Do you support or oppose the U.S. using 'enhanced interrogation' techniques (such as waterboarding) on terrorists?;" "How much do you agree with the following statement: An eye for an eye is never enough;" and "How much do you agree with the following statement: Anyone that kills Americans deserves to be punished." Respondents react to each statement with a five-point scale from strong agreement to strong disagreement. Respondents' scores for each statement are then added to create the overall vengeance score. Respondents scored a '0' if they strongly disagreed with all four vengeful statements and a '16' if they strongly agreed. The mean score is 11, with a standard deviation of 3.3.

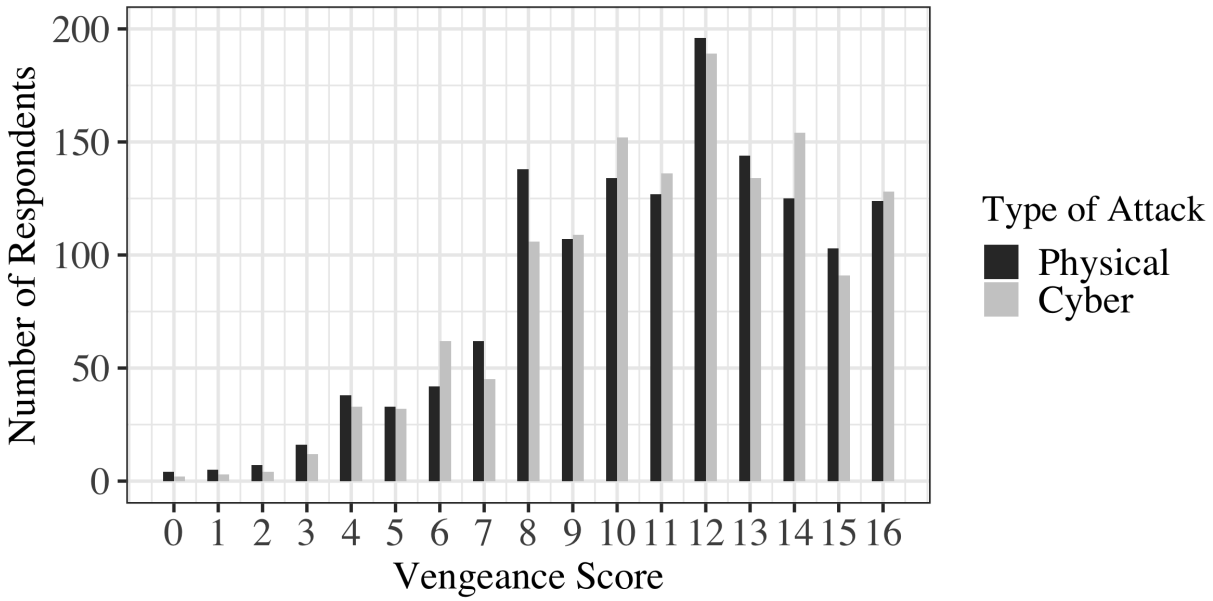


Figure A3: Number of Respondents by Vengeance Score within Treatment Group

H Alternative Explanations

This appendix explores additional characteristics that have been theorized to vary between cyber and physical attacks. As with the clandestine nature of cyber operations, the novelty of the cyber domain is a potentially important distinguishing factor between cyber and kinetic operations, yet the effect of this feature has not been robustly assessed in the empirical literature. We find that the perceived novelty of cyber operations does not have an effect on respondents' support for retaliation to cyber attacks relative to kinetic attacks. Respondents who report knowing more about cyberterrorism and terrorism are more supportive of retaliation, but these results are not specific to the type of attack. Those that indicate they know "a lot" or "a fair amount" about cyberterrorism were, on average, more supportive of retaliation than those who indicated they knew "a little" or "almost nothing" (73 as compared to 59 percent in favor). However, respondents who had more self-reported knowledge on cyberterrorism did not respond to cyber attacks any differently than physical attacks. This suggests newness or unfamiliarity with cyber attacks is not a key reason why respondents react differently to these attacks than to physical attacks.

We also find respondents' perceived vulnerability to cyber operations is not linked to higher likelihoods of support for retaliation to cyber attacks relative to kinetic attacks. Respondents who scored the highest on measures of perceived vulnerability to cyber attacks were more likely to support retaliation to any attack, but they were no more likely to support retaliation to cyber attacks than to kinetic attacks. Yet perceptions of vulnerability are high. 28 percent of respondents had personally been the victim of a cyber attack, and over half judged that they would be likely to be victims in the next year. More than three-quarters expected that the United States would face a cyber attack in the next year. Vulnerability to cyber operations, however, does not uniquely contribute to support for retaliation to cyber attacks. Instead, perceptions of vulnerability may reflect more general attitudes that

contribute to views about retaliation to any attack, regardless of means. Although the vulnerability of cyber infrastructure used by private citizens has had a central place in scholarly theories about cyber operations, it does not appear to be central to public attitudes about responding to hostile cyber operations in particular.

In Appendix B, we showed that there is no relationship between the attack type treatment and respondents' beliefs in the effectiveness of retaliation or their support for retaliation after being told that retaliation will necessarily lead to conflict escalation. This suggests that respondents do not perceive these central elements of deterrence as operating differently in the cyber and physical domains. Both elements, however, are related to respondents' support for retaliation. That is, respondents are more likely to support retaliation if they believe it will be effective. Respondents are also more likely to support retaliation initially if they would also support retaliation even knowing it would result in conflict escalation.

We find some evidence of a negative relationship between perceived costs of inaction after an attack and support for retaliation. 58 percent of respondents suggested more attacks were "very likely" if the United States did not retaliate, and 28 percent thought more attacks were "somewhat likely." If we compare these respondents to all others, they were were significantly more likely to support retaliation. An average of 68 percent of these respondents support retaliation, compared to 42 percent among the remaining respondents. This suggests that, at least for the subset of people most concerned about future attacks, deterrence was an important part of their calculation about the need to retaliate.

We find respondents had similar concerns about the ability to deter both cyber and kinetic attacks. Similar percentages of respondents (86 and 85 percent) thought continued attacks were very or somewhat likely absent retaliation, regardless of whether they were told about a cyber or kinetic attack, respectively.

I Terrorism and Cyberterrorism

How do respondents think about terrorism and cyberterrorism? These labels could influence public attitudes about the attacks described in our vignettes. Overall, we find that the perception of threat from cyber attacks is very high. 93 percent of respondents considered cyberterrorism "somewhat" or "very" threatening. However, this is not unique to the cyber domain. 92 percent of respondents considered terrorism threatening. Respondents' perceptions of whether cyberterrorism and terrorism were threatening were highly correlated ($p < 0.001$). This comparability suggests that the use of terrorism makes our cyber attack and kinetic attack vignettes highly comparable.

The public may also have different expectations about who conducts these two types of operations. If respondents have deeply different beliefs about who is carrying out an attack, they may respond differently to that type of attack. To investigate this possibility, we asked respondents to select characteristics that they believed were associated with cyberterrorists, terrorists, or Russian military officials in order to compare between them. The Russian military offers a comparison point that lets us assess the difference between perceptions of state and non-state adversaries.

There is greater consistency in perceptions between cyberterrorists and terrorists than between cyberterrorists and Russian Military Officials. Cyberterrorists are perceived to be smarter, less well-funded and less ideological than terrorists. Cyberterrorists and terrorists are not perceived statistically different in their evilness, race, danger, rationality, or predictability. Overall, this analysis confirms that terrorism was a more appropriate control group for our experimental design than a conventional military.

Table A7: Characterization of Actors, Percent of Randomized Respondents

	Evil	Radical	Smart	Operates Alone	White	Dangerous	Rational	Well-funded	Ideological	Predictable
Cyberterrorists	67.69	52.06	51.32	13.41	14.26	85.53	11.93	34.42	25.77	8.13
Russian Military Officers	33.87	37.74	45.48	10.65	25.38	70.43	11.61	46.02	28.49	10.97
Terrorists	75.76	62.5	34.02	9.46	12.39	87.17	11.63	44.02	34.46	9.67
T.Test (Russian Mil v. Cyberterror)	***	***	*		***	***		***		
T.Test (Terror v. Cyberterror)		*	***	*				***	***	
Note:								*p<0.05; **p<0.01; ***p<0.001		

J Pre-Analysis Plan

The following pages include the pre-analysis plan as registered.

K Survey Text

The following pages include the full text of the survey experiment. The survey was designed on Qualtrics and fielded on Lucid Marketplace.