Original Manuscript

Journal of Conflict Resolution
2023, Vol. 0(0) 1–31

DOI: 10.1177/00220027231153580
journals.sagepub.com/home/jcr

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

Kathryn Hedgecock[1] **and Lauren Sukin**[2]

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. 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.

Keywords

Cyber, Escalation, Deterrence, Attribution, Covert Action

[1]United States Military Academy, West Point, NY
[2]London School of Economics and Political Science, London, UK

Corresponding Author:
Lauren Sukin, London School of Economics and Political Science, Houghton St., London WC2A 2AE, UK.
Email: l.sukin@lse.ac.uk

Introduction

The vulnerability of critical infrastructure and financial systems to cyber operations remains a primary concern for national security. Protecting the state from cyber operations requires active deterrent measures through intelligence gathering, monitoring, and public-private cooperation in defense. However, when deterrence fails and malicious cyber activity occurs, questions arise about the 'approprate' response that balances escalation and deterrence (Borghard and Lonergan 2019). In seeking to understand how states choose to respond to cyber attacks,[1] one important consideration is the significant public debate surrounding them.

Scholars have suggested public support for conflict may encourage governments to engage, while public opposition to conflict can restrain government behavior (Haesebrouck 2019; Kertzer and Brutger 2016; Kertzer et al. 2020; Levendusky and Horowitz 2012; Tomz and Weeks 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 is 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 with 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. While some existing research has found attitudes about cyber and kinetic conflicts differ, many existing surveys do not address the *mechanisms* by which these differences arise. One exception is Snider et al. 2021 which finds threat perception to be an important moderator for retaliation support.

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 underpinning attitudes about cyber attacks. In particular, we find the clandestine nature of attacks common in the cyber domain, with long discovery times and uncertain attribution, dampen retaliatory support. We find physical attacks that are similarly covert are also less likely to prompt retaliatory support. This previously understudied feature of attacks can help us understand when and why cyber incidents lead to public calls for retaliation.

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 (Borghard and Lonergan 2019; Fischerkeller and Harknett 2017; Libicki 2012; Lin 2012). Theoretical literature on escalation in the cyber domain includes studies of coercion via cyber-means, the operational elements of hybrid warfare (Kostyuk and Zhukov 2017; Maschmeyer 2021), the entanglement of command and control systems, the intersection of cyber and nuclear systems (Acton 2018; Gartzke and Lindsay 2017), and different cross-domain escalation pathways (Healy and Jervis 2020).[2] Empirical research on these topics, however, is often 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 explore the microfoundations of escalation, or when and why support for escalation might arise. Some literature has taken this approach, assessing public support for retaliation in the cyber domain. 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 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). Public opinion can influence policy through retrospective voting, political parties, lobbies, or direct influence on political and bureaucratic actors (Dalton 2013; Risse-Kappen 1991) Key elements of the U.S. foreign policy apparatus are especially sensitive to public opinion. For example, Erik Lin-Greenberg finds “public opposition makes military leaders less likely to recommend the use of force.”(Lin-Greenberg 2021, 1)

Large scale military operations, especially, can be highly visible and costly. Because the public is sensitive to the optics, casualties, outcomes, and economic costs of conflict, leaders often proactively anticipate the public’s response to military initiatives and reactively make foreign policy decisions once public views are known (Chu and Recchia 2021; Eichenberg 2005; Gartner 2008; Grieco et al. 2011; Reiter and Stam 2010). The public holds opinions not only on whether military force is justified, but also on the types of weapons or strategies that are acceptable to apply. As the highly-publicized debate over the use of drones exemplifies, such views can have significant political costs (Kreps and Wallace 2016; Shah 2018)

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, while a few surveys have sought to understand the mechanisms underlying the public response to cyber attacks (Gomez and Whyte 2021; Snider et al. 2021), surveys have generally not examined mechanisms distinguishing the response to cyber and kinetic attacks (Shandler et al. 2021). 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 the covert nature of attacks is essential to understanding the response.

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 the public displays greater reluctance to retaliate against cyber than kinetic attacks (Kreps and Schneider 2019; Schneider 2017; Shandler et al. 2021). This suggests the following hypothesis:

> **H1.** *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 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 distinguishing 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 (Brantly 2018b; Borghard and Lonergan 2019; Gartzke and Lindsay 2019).

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 retaliatory support, while attacks causing 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. This approach, in turn, expects 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).

> **H2.** *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 (Gartzke 2013; Kello 2013; Rid 2012). 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 (Buchan 2012; Fidler 2016).

Existing survey research focuses principally on testing the means and effects-based theories. Kreps and Schneider (2019) and Kreps and Das (2017) find retaliatory support 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. (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 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.

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 (Gartzke and 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 (Maurer 2018; Poznansky and Perkoski 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; Poznansky and Perkoski 2018). The covert nature of cyber operations lends itself to two distinct technical 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; Gartzke and Lindsay 2015; Lindsay 2015; Rid and Buchanan 2015). Although cybersecurity experts note that attribution challenges are becoming less acute in the cyber domain (Canfil 2022), governments still often have opportunities to strategically withhold attribution from the public. Moreover, the extended timelines associated with attribution—even when certain attribution is possible—still disproportionately impact cyber operations relative to the kinetic realm.

While the presence of physical weaponry or combatants often makes the origin of kinetic attacks easier and faster to identify, there are also 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 (Cormac and Aldrich 2018; Johnson 2020; Mumford 2013). 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 underexplored in previous empirical work. As attribution challenges in the cyber domain persist and attribution problems in kinetic conflict become more common, understanding the implications of the attribution process is increasingly politically pressing. Meanwhile, militaries increasingly rely on contractors and non-state actors, while emerging technologies make fast attribution more important and more difficult. Indeed, only about 3 in 1000 cybercrimes are ever prosecuted (Garcia and Eoyang 2020).

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 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 attribution certainty will increase public support for retaliation to both cyber and kinetic attacks, attribution is empirically 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:

H3a. *As the attribution certainty of an attack increases, retaliatory support increases.*

A related challenge is the timing of attribution. Despite the adage 'revenge is a dish best served cold,' retaliation is often believed to be most appropriate served hot (Brantly 2018b). A more recently attributed attack should elicit greater retaliatory support. When attacks are discovered or attributed months or years later, their salience will be lower, as will the perceived costs of not responding.[3] 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 now have new actors who do 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, suggesting that:

H3b. *As the time since an attack becomes more distant, retaliatory support 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 that complicate and increase the need for effective attribution (Johnson 2020). Like with attribution certainty, if attribution delays reduce retaliatory support, 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 potentially distinguishing 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 the most influential features of attacks relate to their covertness.

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.[4] Each 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[5], 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 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 parallel to a cyber attack that would be highly similar in every way except the means of delivery: a terrorist attack.[6] We selected a terrorist attack as our comparison in order to control for two common features of cyber attacks: they can be conducted by non-state actors and they usually cause little damage. Terrorist attacks cause less damage than other types of conventional attacks, making them a more plausible comparison than attacks by a military. Gross et al. (2016) found respondents perceive attacks by cyberterrorists and terrorists as similarly threatening.[7] Because the "terrorism" label is

Table 1. Factorial Treatments for the Scale of an Attack.

	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.**

applied to both the cyber and kinetic attacks, the attacks are highly comparable.[8] To be sure cyberterrorists and terrorists were viewed similarly, we assessed perceptions of these actors in pre-treatment questions. While there are some differences, respondents show 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." This suggests pre-existing conceptions about these actors should not explain any differences in 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. A loss of life treatment is included to dialogue with existing literature that finds the importance of a lethality threshold for support of cyber retaliation (Shandler et al. 2021). 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 with minimal inflicted damage, we bias against our argument that cyber and kinetic attacks will be seen differently. Like other surveys, we provide a treatment with a lethal attack. To account for the possibility respondents primarily respond to whether damage is physical (Gartzke 2013; Libicki 2012; Rid 2012), we include both physical and non-physical effects.

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).[10] Attribution certainty is one way to proxy the 'secrecy' dimension of an attack.[11] The simplicity of our terminology prevents respondents from introducing alternative interpretations. We anticipate certainty 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

Table 2. Treatments by Factor.

Type	Scale	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		

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

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

The attack is conducted by a non-state actor with a state sponsor, Russia. Kreps and Schneider (2019, 6) opted to anonymize the state actor in their survey, but they found 57% of respondents had a particular country in mind while responding to their vignette. To guard against this, and to be able to more precisely control for respondents' pre-existing attitudes about the state initiating the attack, we designated Russia as the state sponsor for our experiment. Russia is a highly active state actor in the cyber domain and may naturally arise in the mind of respondents. This element of the vignette is both plausible and politically relevant. Designating Russia as the sponsor may help reduce the effect of identity biases associated with terrorism. Finally, Russia is a near-peer competitor, so our treatment presents a hard case for escalation. We also include controls on respondents' pre-treatment perceptions of Russia.

The dependent variable is public support for retaliation, captured by affirmative answers to the question: "Should the U.S. military retaliate against the attack?" We construct a binary indicator of retaliatory support. The binary choice allows us to assess respondents' initial preferences and allows for clear interpretability of results. Building on this response, we ask respondents several more detailed questions regarding their preferences for how to respond to the attack. These compose several alternative dependent variables, and our results are robust whether we use our primary, binary measure or these alternate specifications. 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.[12] 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.[13] 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 (Gomez and Whyte 2021; Gregory et al. 1995; McDermott 2019; Snider et al. 2021). 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 retaliatory support and attitudes about deterrence and escalation. Additionally, respondents answer questions on demographics and report attitudes about vengeance, nationalism, globalism, international law, trust in government, international security issues, and perceptions of cyberterrorists, terrorists, and Russia.

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 retaliatory support (66%). This is largely consistent across the type of attack, with 64% supporting a military response to a cyber attack and 68% 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 causes is not significantly related to retaliatory support 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. Note that this finding is not due to inattention, as the findings are robust to dropping respondents who failed attention checks. In addition, high retaliatory support, regardless of an attack's effects, is linked to hawkishness among the U.S. public, but the nationally representative sample should display similar hawkishness as the U.S. public writ large. Moreover, our results hold with the inclusion of multiple controls for hawkishness. This surprising result contradicts the effects-based approach.

Regression analysis also provides insight into a number of factors potentially associated with support for escalation. In Models 3 and 4, we include respondents' demographics, 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. This finding is contrary to existing literature which finds cyber vulnerability and threat to be important mechanisms for cyber attitudes (Gross et al. 2016; Kostyuk and Wayne 2020; Snider et al. 2021). The results also hold while

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

	Base (1)	Interactions (2)	Demographic controls (3)	Full model (4)	Post treatment (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)

(continued)

Table 3. (continued)

	Base (1)	Interactions (2)	Demographic controls (3)	Full model (4)	Post treatment (5)
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	2797	2797	2486	2476	2476
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: $^{*}p < 0.05$; $^{**}p < 0.01$; $^{***}p < 0.001$.

controlling for threat perceptions of Russia.[15] We find attitudes about vengeance are strongly and consistently correlated with retaliatory support, and attitudes on international law and on trust in government are inconsistently related to retaliation. These results are unsurprising. Vengeful individuals seek a 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.

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' retaliatory support by four percentage points, statistically significant at the $p < 0.05$ level. This effect is nearly four times smaller than the estimated effect of certain attribution at the $p < 0.001$ level. 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' retaliatory support 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 provide some evidence for the means-based approach, they also suggest previous work may have overestimated the importance of means.

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; Borghard and Lonergan 2019; Fischerkeller and Harknett 2017; Libicki 2012; Lin 2012; Lindsay 2015). However, we find that respondents have the same views on deterrence and escalation in the cyber and physical domains.[17] Belief in the efficacy of response is an important predictor of retaliatory support. Respondents who believed their most preferred response 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 would lead to subsequent escalation, were 54 percentage points more likely to support retaliation initially than those who believe the United States should not have retaliated if doing so would have escalated.[18]

Across all models, we find that attribution certainty and timing are the greatest and most significant predictors of respondents' retaliatory support. As indicated in Figure 1, 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% of those told the government had "low confidence" supported the same response. Change from "low confidence" to "high confidence" is associated with an 15% increase in retaliatory support, 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

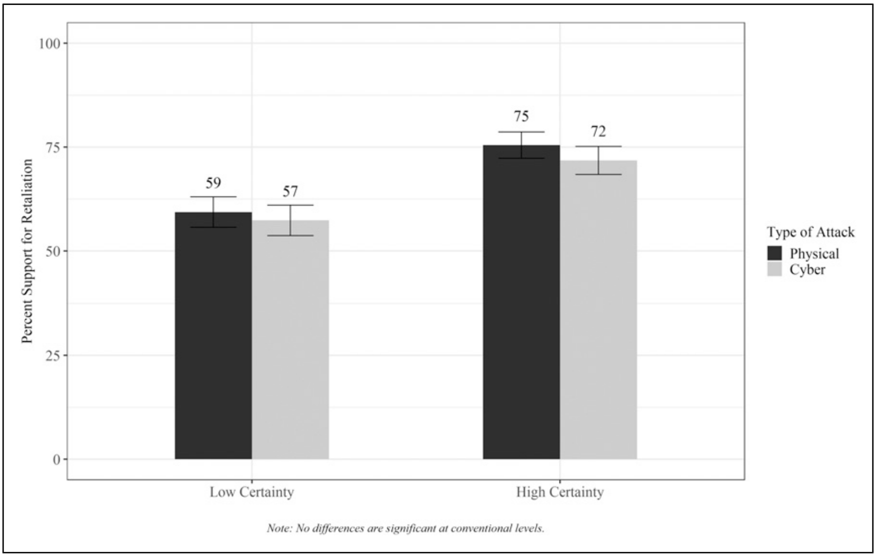


Figure 1. Support for retaliation by certainty treatment.

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 retaliatory support. Yet ‘grey zone’ warfare and other types of covert kinetic attacks may experience similar public resistance to retaliation.

Many respondents explicitly referenced attribution as an important component of their retaliatory support. These comments are illustrative of the aforementioned significance of attribution in respondents’ 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.” Many respondents suggested attributed attacks should be met with a strong response. For example, one respondent 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.” While these quotations certainly do not constitute a comprehensive test of our hypothesis about the importance of attribution, the prevalence of references to attribution in respondents' open-ended comments further substantiates our argument that respondents pay attention to and care about this issue.

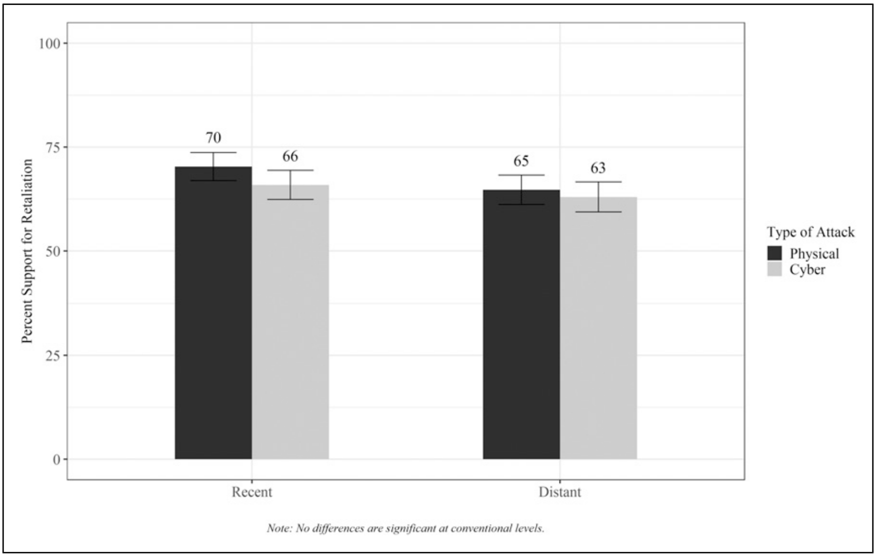
The second largest treatment effect is from timing. Among respondents who were told the attack occurred "more than a year ago," 64% supported retaliation, while among those who were told that the attack occurred "recently," 68% supported retaliation. Attacks that occurred in the year prior experienced a three to five percentage point decline in retaliatory support, compared to those that were described as having occurred "recently." This is significant at $p < 0.05$ across all model specifications. Figure 2 further illustrates the effects of a recent or distant treatment. Once again, there is no statistically significant difference between cyber and kinetic attacks. Regardless of the means, receiving a more distant treatment is associated with depressed support for retaliation. 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.

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 retaliatory support, we find no evidence for the effects-based theory. The scale of an attack's damage does not affect respondents' retaliatory support. 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.

Assessing Within- and Cross-Domain Response Preferences

In addition to asking about willingness to retaliate, we also examined respondents' most preferred policy response. Again, we find majority support for military options such as kinetic and cyber retaliation. Figure 3 breaks down respondents' most preferred response by whether they received a cyber or physical vignette. Figure 3 indicates some support for cross-domain retaliation and some support for a "notion of equivalence." 31% of respondents receiving a cyber treatment preferred to respond with a cyber attack; similarly, 34% of respondents who received a kinetic treatment preferred to respond kinetically.[19]

When we group respondents by their most preferred response, we find those receiving the cyber treatment were less likely to support physical retaliation (significant at $p < 0.001$), although no less likely to support retaliation overall.[20] Individuals receiving the 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 those with 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



Note: No differences are significant at conventional levels.

Figure 2. Support for retaliation by attack timing.

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.*[21]

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% of respondents support the use of drones; 33% support sending in Special Operations forces; 21% support a "boots on the ground" approach; and 17% support a bombing campaign.[22] This represents notable public support for disproportionate responses to both cyber and kinetic attacks that impose relatively minimal damage.

Explaining High Retaliatory Support

We find high 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

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, retaliatory support will increase, regardless of the means of delivery.	No
Covertness	**H3a (Attribution certainty):** As the attribution certainty of an attack increases, retaliatory support will increase, regardless of means of delivery.	Yes
	H3b (Timing): As the time since an attack becomes more distant, retaliatory support will decrease, regardless of means of delivery.	Yes

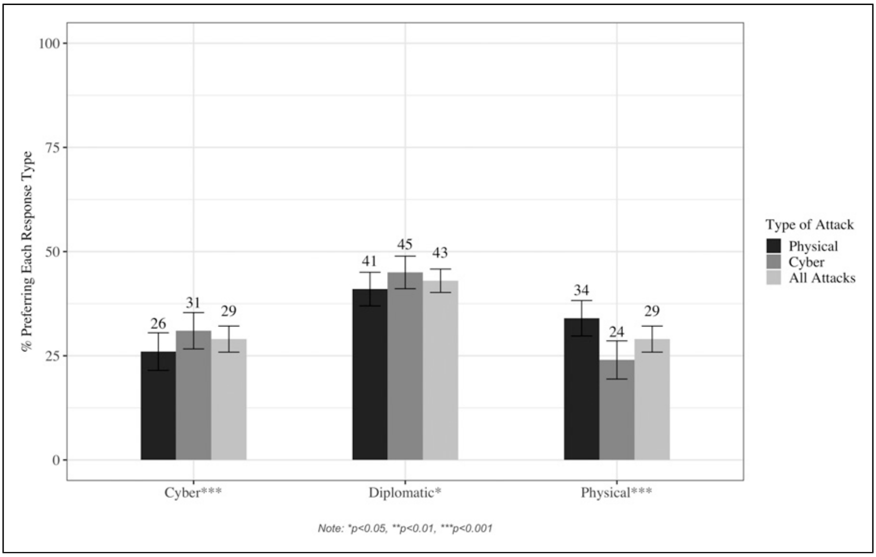


Figure 3. Most preferred type of response.

this phenomenon? To answer this question, we examine a battery of controls that could contribute to high public support for retaliation.

Few attitudes about international politics consistently contribute to retaliatory support. Table 3 shows that neither respondents' knowledge about cybersecurity nor their perceived personal vulnerability to cyber operations are correlated with retaliatory support; nor are these variables linked to higher likelihoods of support for retaliation to cyber attacks relative to kinetic attacks.[23] Additionally, neither nationalism nor globalism is associated with retaliatory support, 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, although these variables do not distinguish between respondents' reactions to cyber and kinetic attacks.[24] The effectiveness 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% of respondents who supported retaliation, compared to 52% of respondents who opposed it, thought attacks would be effective. This suggests retaliatory support leverages a consequentialist logic; respondents may support retaliation because they believe it will effectively deter.

The escalation variable references a post-treatment question telling 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% of respondents support retaliation in this situation, compared to 66% supporting retaliation in the original experiment. It could be that when respondents know retaliation will escalate, they interpret that as evidence of the malintentions or capabilities of the adversary, making retaliation—even if it is costly—more critical. This suggests retaliatory support is "sticky." It may consequently be difficult to dissuade a hawkish public from demanding retaliation in response to attacks. Additionally, retaliatory support may not be diminished, or could actually increase, with a highly capable adversary.

Attitudes about vengeance are also linked to retaliatory support. A majority of respondents were highly vengeful and therefore may have be more focused on punishing fictional attackers than on determining an appropriate response by other measures. 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 (Liberman and Skitka 2019; McDermott et al. 2017; Sagan and Valentino 2019a; Stein 2015).[25] We confirm previous work associating vengefulness with increased retaliatory support, although the effect of vengefulness has not previously been explored in the cyber domain.

Figure 4 shows retaliatory support 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. Vengeance is the control variable with the single greatest impact on respondents' likelihood to support retaliation. Table 3 shows that 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 complements research by Shandler et al. (2021) arguing anger is a primary mechanism of support for cyber retaliation.

We find high public support for retaliation; this finding is politically significant, as it may indicate the public will not act as a stopgap against—and may, in fact, encourage—escalation after even low-damage attacks. High approval for retaliation may be influenced by a combination of factors, including consequentialist logic about the usefulness of retaliation as well as a more emotive logic related to attitudes about vengeance.

Challenging the Effects-Based Theory

Contrary to previous empirical literature (Kreps and Das 2017; Kreps and Schneider 2019; Shandler et al. 2021), we find no evidence of an effects-based mechanism.[26] We find the scale of damage has almost no measurable effect on willingness to retaliate. This holds true across a wide range of model specifications, including alternate dependent variables.[27]

There are several potential explanations for this result. 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 shaping the results of previous studies. Second, we intentionally chose outcomes respondents would find believable and which are largely consistent with attacks familiar to casual news consumers. This departs from existing work, which uses more severe outcomes, 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 since previous surveys were fielded.[28]

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 effects of an attack are not a significant predictor of retaliatory support.

Respondents do not dismiss the attacks in our scenario, despite the low amounts of damage they inflict. Instead, there is significant support for retaliation, including highly disproportionate responses. Retaliatory support is largely consistent across damage-levels, as shown in Figure 5.[29] 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 suggests cyber attacks do not need to reach a high ‘threshold’ of damage to

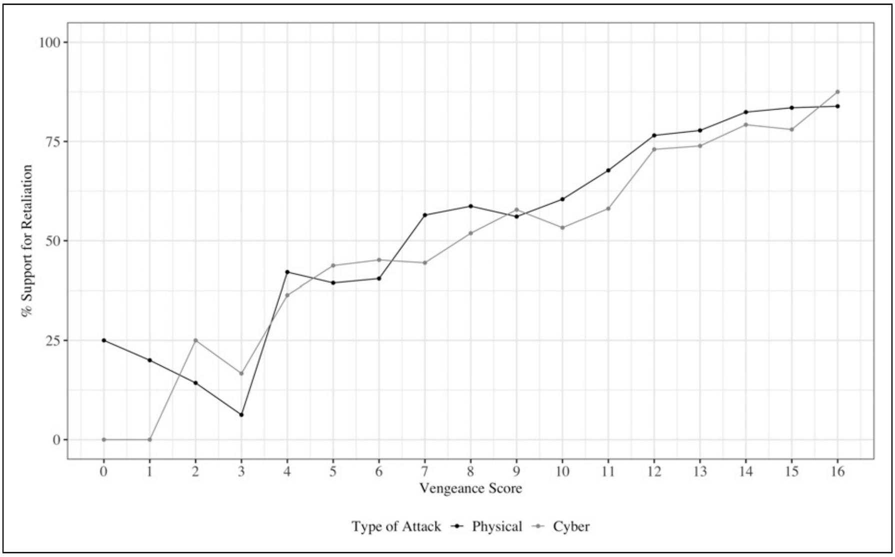


Figure 4. Retaliatory support by vengeance score and type treatment.

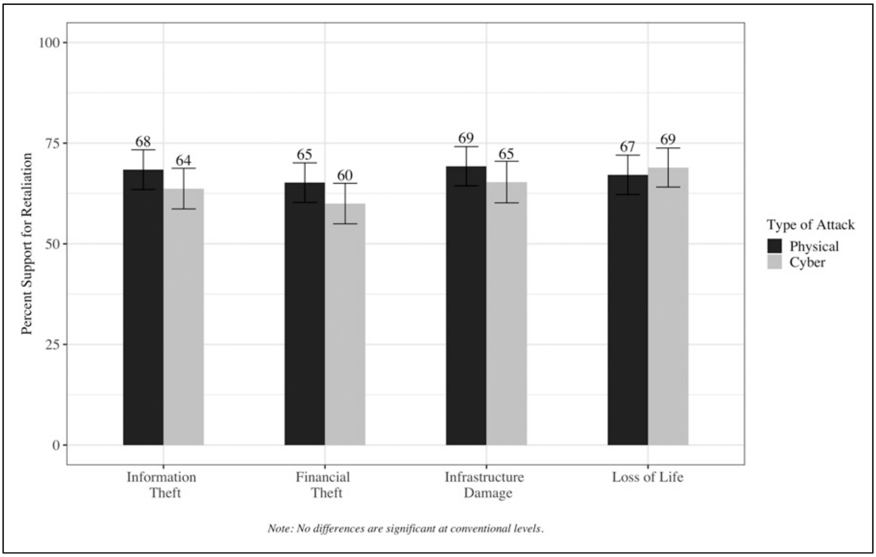


Figure 5. Percent support for retaliation by scale treatment.

generate retaliatory support. 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 States. When asked how respondents would “most prefer” the United States respond to this theft, 26% selected that they preferred a “physical attack”. An additional 30% supported a cyber attack. Overall, we find a high baseline level of retaliatory support 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.[30]

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 retaliatory support against low-damage attacks, but also that the amount of damage an attack causes has no effect on retaliatory support. We also challenge the lethality threshold hypothesis, finding no effect of lethality on respondents’ overall retaliatory support.

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 retaliatory support 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 retaliatory support, we varied four treatments in a 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' retaliatory support. 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 retaliatory support. 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 less generate public support for retaliation.

Additionally, we find the timing of the attack has a significant impact on public support for 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' retaliatory support. 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 retaliatory support. 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.[31]

Second, our results suggest the current focus on how much damage or what type of damage a cyber attack causes may be misplaced. This article 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. If this finding is generalizable to other states' publics, then the current U.S. strategy of 'persistent engagement' may be founded on shaky assumptions of non-escalation for cyber operations. It is plausible that a competitor may choose to rally public support to exploit operations that are short of force.

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 retaliatory support 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 retaliatory support.

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. Some of the dynamics we explore in this paper may not persist in other settings, such as in states where cyber infrastructure is significantly more or less developed, in states facing different adversaries in cyberspace than the United States, or where important, underlying cultural attitudes, such as a sense of justice as a retributive process, differ from American sensibilities. Despite these potential limitations to generalizability, however, our findings represent a step forward for understanding the dynamics of adverse cyber events in the politically important context of U.S. policy, and further research should explore the extent to which the arguments we advance and test here provide similar insights into public preferences elsewhere.

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.

Acknowledgements

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

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the Stanford Center for American Democracy.

ORCID iD

Lauren Sukin https://orcid.org/0000-0002-5775-8790

Supplemental Material

Supplemental material for this article is available online.

Notes

1. 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.
2. Because we focus on public support for escalation, the technical and operational elements of cyber warfare, including entanglement with other systems, are beyond our scope. Although these elements should influence the actual probability of escalation, the public is unlikely to understand the details of U.S. cyber capabilities or to be able to adequately assess feasibility.
3. Attackers can also make calculated choices with regards to attribution timing.
4. See Appendix A. We had 4,444 total respondents; respondents were dropped if they did not consent to participate, failed an attention check, or could not correctly identify the target of the attack. Robustness tests in Appendix C include those who incorrectly answered the mechanism and attention checks and affirm our main results. Lucid aggregates respondents across multiple panels, making their respondent pool more representative than some competitors' (Coppock and McClellan 2019). For example, Lucid has greater numbers of older respondents, who are typically underrepresented in online surveys (Munger et al. 2021).

[5] “Red Square” was always prefaced with “the [cyber]terrorist organization” or respondents were asked about the group’s Headquarters. No individuals appear to have mistaken “Red Square” for the location.

[6] Kreps and Das (2017) do not use a non-cyber control. Kreps and Schneider (2019) do vary means. They offer a conventional alternative to a cyber attack but their scenario involves a state actor rather than a state-sponsored proxy. They also include a nuclear attack.

[7] They also find cyberterrorism provokes a similar anxiety response regardless of lethality, while anxiety varies differs between conventional lethal and non-lethal terrorist attacks.

[8] There is legal precedent for states to retaliate to terrorist attacks, but the role of cyberterrorism under international law is more uncertain (Sukin and Weiner 2022).

[9] See Appendix I.

[10] Low confidence does not mean 0% certainty; high confidence does not imply 100% certainty. Real-world attribution may include more variety than we are able to test.

[11] There are strategic considerations for both the initiator and target in the use and revelation of cyber capabilities. However, we examine only one type of strategy for obscuring attribution: the use of a proxy. We choose this because it is a quite common strategy. This approach allows us to vary attribution in a simple way that can be clearly communicated to the public. For more on strategic considerations of attribution, see Egloff 2020; Egloff and Wenger 2019; Poznansky and Perkoski 2018.

[12] See Appendix E.

[13] See Appendix F.

[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?” Neither variable effects willingness to respond to cyber attacks, suggesting neither explains differences in public attitudes about cyber versus kinetic attacks. See Appendix H.

[15] See Appendix H.

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

[17] These post-treatment variables are included because they had a significant effect on the dependent variable but were not affected by the treatment. See Appendix B.

[18] 39% of respondents opposing retaliation initially later supported retaliation after learning it resulted in escalation, suggesting escalation does not deter but justifies retaliation. For details, see Appendices B and H.

[19] There is no significant difference between support for cross-domain retaliation to cyber and kinetic attacks. In a robustness test including only respondents who received high damage treatments—infrastructure damage or loss of life—the results hold. See Appendix F.

[20] See Appendix F.

[21] Scale had no effect on most preferred response, except in the loss of the life treatment. Respondents with lethal attacks were marginally more likely to support physical retaliation. See Appendix F.

22. Relative to cyber attacks, kinetic attacks are associated with higher support for all of these types except the "boots on the ground" response.
23. See Appendix H.
24. See Appendix B.
25. 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.
26. Kreps and Schneider (2019) find support for the means-based theory, but their results also show a positive relationship between attack scale and willingness to retaliate. Shandler et al. (2021) find no means-based distinction at lower effects thresholds, but they do identify one when attacks cause loss of life.
27. For more, including additional operationalizations of scale, see Appendix D.
28. 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 support the effects-based theory. Finally, we mitigate the effects of respondents' attitudes about Russia by controlling for them in our design.
29. When the attack targeted financial institutions, respondents were between 4 and 5 percentage points less likely to support retaliation. This could be related to a specific dislike of the financial sector. Retaliatory support does not significantly differ for any other scale treatments.
30. We tested other elements theorized to distinguish between cyber and kinetic means, such as expectations about escalation, the consequences of inaction, the novelty of cyber operations, and perceived vulnerability to cyber operations. These do not lead to significant differences in public support for retaliation by attack means. See Appendix H.
31. For further discussion of how policymakers can shift the public's perceptions of cyber attack attribution, see Hedgecock 2021.

References

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

Acton, James M. 2018. "Escalation Through Entanglement: How the Vulnerability of Commandand-Control Systems Raises the Risks on an Inadvertent Nuclear War." *International Security* 43 (1): 56-99.

Borghard, Erica D., and Shawn W. Lonergan. 2019. "Cyber Operations as Imperfect Tools of Escalation." *Strategic Studies Quarterly* 13 (3): 122-145.

Brantly, Aaron. 2016. "Aesop's Wolves: The Deceptive Appearance of Espionage and Attacks in Cyberspace." *Intelligence and National Security* 31 (5): 674-685.

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

Brantly, Aaron. 2018b. “The Cyber Deterrence Problem.” In *2018 10th International Conference on Cyber Conflict (CyCon)*, 31-54. 2018 10th International Conference on Cyber Conflict (CyCon).

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

Canfil, Justin. 2022. “Outsourcing Cyber Power: Why Proxy Conflict in Cyberspace May No Longer Pay.” *Journal of Cybersecurity* 8: 50.

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

Carson, Austin, and Keren Yarhi-Milo. 2017. “Covert Communication: The Intelligibility and Credibility of Signaling in Secret.” *Security Studies* 26 (1): 124-156.

Chu, Jonathan, and Stefano Recchia. 2021. “Does Public Opinion Affect the Preferences of Foreign Policy Leaders? Experimental Evidence from the U.K. parliament.” *Journal of Politics*.

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

Coppock, Alexander, and Oliver McClellan. 2019. “Validating the Demographic, Political, Psychological, and Experimental Results Obtained from a New Source of Online Survey Respondents.” *Research and Politics* 6 (1): 205316801882217.

Cormac, Rory, and Richard J. Aldrich. 2018. “Grey is the New Black: Covert Action and Implausible Deniability.” *International Affairs* 94 (3): 477-494.

Dalton, Russell. 2013. *Citizen Politics: Public Opinion and Political Parties in Advanced Industrial Democracies*. University of California, Irvine, CA: CQ Press.

Egloff, Florian, and Andreas Wenger. 2019. “Public Attribution of Cyber Incidents.” *CSS Analyses in Security Policy* 244 (May): 1-4.

Egloff, Florian J. 2020. “Public Attribution of Cyber Intrusions.” *Journal of Cybersecurity* 6 (1): 1-12.

Eichenberg, Richard. 2005. “Victory Has Many Friends: U.S. Public Opinion and the Use of Military Force, 1981–2005.” *International Security* 30 (1): 140-177.

Farrell, Henry, and Charles Glaser. 2017. “The Role of Effects, Saliencies and Norms in US Cyberwar Doctrine.” *Journal of Cybersecurity* 3 (1): 7-17.

Fearon, James. 1994. “Domestic Political Audiences and the Escalation of International Disputes.” *American Political Science Review* 88 (3): 577-592.

Fidler, David. 2016. “Just and Unjust War, Uses of Force and Coercion: An Ethical Inquiry with Cyber Illustrations.” *Daedalus* 145: 37-49.

Fischerkeller, Michael, and Richard Harknett. 2017. “Deterrence is Not a Credible Strategy for Cyberspace.” *Orbis* 61 (3): 381-393.

Garcia, Michael, and Mieke Eoyang. 2020. “A Road Map for Tackling Cybercrime.” *Lawfare*.

Gartner, Scott Sigmund. 2008. “The Multiple Effects of Casualties on Public Support for War: An experimental approach.” *American Political Science Review* 102 (1): 95-106.

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 (2): 316-348.

Gartzke, Erik, and Jon Lindsay. 2017. “Thermonuclear Cyberwar.” *Journal of Cybersecurity* 1: 37-48.

Gartzke, Erik, and Jon Lindsay. 2019. *Cross-Domain Deterrence: Strategy in an Era of Complexity*. New York, NY: Oxford University Press.

Gomez, Miguel Alberto, and Christopher Whyte. 2021. “Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats.” *International Studies Quarterly* 65: 1137-1150.

Gregory, Robin, James Flynn, and Paul Slovic. 1995. “Technological Stigma.” *American Scientist* 83 (3): 220-224.

Grieco, Joseph, Christopher Gelpi, Jason Reifler, and Peter Feaver. 2011. “Let’s get a Second Opinion: International institutions and American public support for war.” *International Studies Quarterly* 55 (2): 563-583.

Gross, Michael, Daphna Canetti, and Dana R. Vashdi. 2016. “The Psychological Effects of Cyber Terrorism.” *Bulletin of the Atomic Scientists* 72 (5): 284-291.

Haesebrouck, Tim. 2019. “Who Follows Whom? A Coincidence Analysis of Military Action, Public Opinion and Threats.” *Journal of Peace Research* 56 (6): 753-766.

Healy, Jason, and Robert Jervis. 2020. “The Escalation Inversion and Other Oddities of Situational Cyber Stability.” *Texas National Security Review* 3 (1): 31-53.

Hedgecock, Kathryn. 2021. “Strategic Attribution.” *Working Paper.*

Johnson, James. 2020. “Delegating Strategic Decision-Making to Machines: Dr. Strangelove Redux?” *Journal of Strategic Studies* 45: 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*.

Kostyuk, Nadiya, and Yuri M. Zhukov. 2017. “Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events?” *Journal of Conflict Resolution* 63 (2): 317-347.

Kreps, Sarah, and Debak Das. 2017. “Warring From the Virtual to the Real: Assessing the Public’s Threshold for War Over Cyber Security.” *Research and Politics* 4 (2): 205316801771593.

Kreps, Sarah, and Jacquelyn Schneider. 2019. “Escalation Firebreaks in the Cyber, Conventional, and Nuclear Domains: Moving Beyond Effects-Based Logics.” *Journal of Cybersecurity* 5 (1): tyz007.

Kreps, Sarah, and Geoffrey Wallace. 2016. "International Law, Military Effectiveness, and Public Support for Drone Strikes." *Journal of Peace Research* 53 (6): 830-844.

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 (2): 189-215.

Libicki, Martin. 2012. *Crisis and Escalation in Cyberspace*. Santa Monica, CA: Rand Corporation.

Lieber, Keir, and Daryl Press. 2013. "Why States Won't Give Nuclear Weapons to Terrorists." *International Security* 38 (1): 80-104.

Lin, Herbert. 2012. "Escalation Dynamics and Conflict Termination in Cyberspace." *Strategic Studies Quarterly* 25: 46-70.

Lin-Greenberg, Erik. 2021. "Soldiers, Pollsters, and International Crises: Public Opinion and the Military's Advice on the Use of Force." *Foreign Policy Analysis* 17 (3): orab009.

Lindsay, Jon. 2015. "Tipping the Scales: The Attribution Problem and the Feasibility of Deterrence Against Cyberattack." *Journal of Cybersecurity* 1 (1): 53-67.

Maschmeyer, Lennart. 2021. "The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations." *International Security* 46 (2): 51-90.

Maurer, Tim. 2018. *Cyber Mercenaries*. Cambridge, UK: Cambridge University Press.

McDermott, Rose. 2019. "Some Emotional Considerations in Cyber Conflict." *Journal of Cyber Policy* 4 (3): 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 (1): 68-89.

Miller, Michael. 2007. "Nuclear Attribution as Deterrence." *The Nonproliferation Review* 14 (1): 33-60.

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

Munger, Kevin, Ishita Gopal, Jonathan Nagler, and Joshua A Tucker. 2021. "Accessibility and Generalizability: Are Social Media Effects Moderated by Age or Digital Literacy?" *Research and Politics* 8 (2): 20531680211016968.

Nye, Joseph. 2017. "Deterrence and Dissuasion in Cyberspace." *International Security* 41 (3): 44-71.

Poznansky, Michael, and Evan Perkoski. 2018. "Rethinking Secrecy in Cyberspace: The Politics of Voluntary Attribution." *Journal of Global Security Studies* 3 (4): 402-416.

Reiter, Dan, and Allan Stam. 2010. *Democracies at War*. Princeton, NJ: Princeton University Press.

Rid, Thomas. 2012. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35 (1): 5-32.

Rid, Thomas, and Ben Buchanan. 2015. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38 (1): 4-37.

Risse-Kappen, Thomas. 1991. "Public Opinion, Domestic Structure, and Foreign Policy in Liberal Democracies." *World Politics* 43 (4): 479-512.

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

Sagan, Scott, and Benjamin Valentino. 2019b. "On Reciprocity, Revenge, and Replication: A Rejoinder to Walzer, McMahan, and Keohane." *Ethics and International Affairs* 33 (4): 473-479.

Schneider, Jacquelyn. 2017. "Cyber and Crisis Escalation: Insights from Wargaming." *USASOC Futures Forum*: 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 U.S. 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* 52: 1-19.

Snider, Keren, Ryan Shandler, Shay Zandani, and Daphna Canetti. 2021. "Cyberattacks, Cyber Threats, and Attitudes Toward Cybersecurity Policies." *Journal of Cybersecurity* 7 (1): 1-11.

Stein, Rachel. 2015. "War and Revenge: Explaining Conflict Initiation by Democracies." *American Political Science Review* 109 (3): 556-573.

Sukin, Lauren, and Allen Weiner. 2022. "War and Words: The International Use of Force in the United Nations Charter." Chap. 5 In *Is the International Legal Order Unraveling?*, edited by David Sloss, 143-184. New York, NY: Oxford University Press.

Tomz, Michael. 2007. "Domestic Audience Costs in International Relations: An Experimental Approach." *International Organization* 61 (4): 821-840.

Tomz, Michael, and Jessica Weeks. 2020. "Public Opinion and Foreign Electoral Intervention." *American Political Science Review* 114 (3): 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.